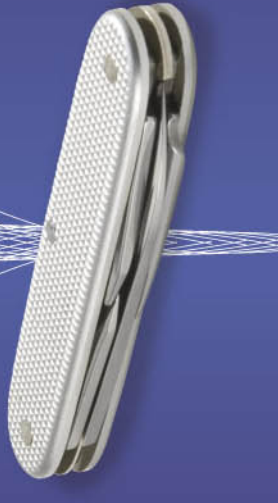
Microsoft

Microsoft Windows® 8

Уильям Р. Станек



Справочник администратора

РУССКАЯ РЕДАКЦИЯ Microsoft bhv®

Microsoft

Microsoft Windows® 8 Administration

Pocket Consultant

William R. Stanek

Microsoft Windows® 8

Справочник администратора

Уильям Р. Станек

РУССКАЯ РЕДАКЦИЯ

bhv

2014

УДК 004.451
ББК 32.973.26-018.2
С76

Станек У. Р.

С76 Microsoft Windows® 8. Справочник администратора: Пер. с англ. — М.: Издательство «Русская редакция»; СПб.: «БХВ-Петербург», 2014. — 688 с.: ил. — (Справочник администратора)

ISBN 978-5-7502-0426-7 («Русская редакция»)
ISBN 978-5-9775-0927-5 («БХВ-Петербург»)

Данная книга — краткий и исчерпывающий справочник по администрированию Windows 8. Здесь описаны настройка рабочего стола и нового пользовательского интерфейса, профилей пользователей, управление устройствами, приложениями и виртуализацией, автоматизация конфигурирования Windows 8, оптимизация системы, выполнение задач обслуживания и поддержки, технологии TPM и BitLocker, управление дисковыми приводами и файловыми системами, управление защитой файлов и общими ресурсами, настройка параметров TCP/IP, мобильные сети и удаленный доступ. Также углубленно рассматривается вопрос поиска и устранения неполадок.

Для квалифицированных пользователей и системных администраторов

УДК 004.451
ББК 32.973.26-018.2

Уильям Р. Станек

Microsoft Windows® 8. Справочник администратора

Перевод с английского языка Сергея Таранушенко

Совместный проект издательства «Русская редакция» и издательства «БХВ-Петербург»

РУССКАЯ РЕДАКЦИЯ bhv®

Подписано в печать 28.06.13.
Формат 70×100 1/16. Печать офсетная. Усл. печ. л. 55,47.
Тираж 1000 экз. Заказ №

Первая Академическая типография "Наука"
199034, Санкт-Петербург, 9 линия, 12/28

ISBN 978-0-7356-6613-9 (англ.)
ISBN 978-5-7502-0426-7 («Русская редакция»)
ISBN 978-5-9775-0927-5 («БХВ-Петербург»)

Оглавление

Эта книга посвящается моей жене, которая на протяжении многих книг, многих миллионов слов и многих тысяч страниц была рядом со мной, предоставляя помощь и поддержку и создавая домашний уют в каждом месте, в котором мы жили.

Я также посвящаю эту книгу моим детям, за их помощь видеть мир по-новому, за их исключительное терпение и безграничную любовь, а также за то, что они делают каждый день приключением.

Также посвящается Карене, Мартину, Луанде, Джулиане и многим другим людям, которые помогали мне как в малом, так и в большом.

Уильям Р. Станек

Об авторе

Уильям Р. Станек (William R. Stanek, **http://www.williamstanek.com**) имеет за плечами более 20 лет практического опыта работы в области продвинутого программирования и разработки. Он один из ведущих экспертов по компьютерным технологиям, автор отмеченных наградами книг, и довольно-таки хороший обучающий инструктор. На протяжении многих лет он своими практическими советами помогал миллионам программистов, разработчиков и сетевых инженеров по всему миру.

Уильям участвует в разработке коммерческих интернет-проектов с 1991 г. Свой основной опыт в бизнесе и изучении технологий он накопил за 11 с лишним лет службы в армии. Он обладает обширным опытом в области разработки серверных технологий, шифрования и интернет-решений. Уильям является автором многих технических докладов и учебных курсов по широкому кругу предметов. Его часто приглашают в качестве эксперта и консультанта по различным предметным областям.

Уильям обладает степенью магистра информационных систем и дипломом бакалавра информатики. Он гордится своей службой в армии во время военных действий в Персидском заливе в качестве члена экипажа самолета радиоэлектронного противоборства. Он участвовал во многих боевых операциях в Ираке и был награжден девятью медалями за свою военную службу, включая одну из наград военно-воздушных сил США — крест "За лётные боевые заслуги". В настоящее время он проживает со своей женой и детьми на тихоокеанском северо-западе США.

Недавно Уильям снова увлекся природным туризмом. Когда он не работает над очередной книгой, то совершает пешие прогулки, велосипедные поездки, турпоходы с ночевкой, путешествует или странствует со своей семьей в поисках приключений.

Уильяма можно найти на Twitter под ником *WilliamStanek* и на Facebook по адресу **www.facebook.com/William.Stanek.Author**.

Введение

Работа над этой книгой доставила мне большое удовольствие, хотя и была очень трудоемкой. Приступая к работе над ней, моей первоначальной целью было определить, чем Windows 8 отличается от предшествующих версий Windows и какие новые возможности и опции она предоставляет. Как с любой новой операционной системой, мне пришлось выполнить большой объем исследований и разобраться с "устройством" этой операционной системы, чтобы получить четкое представление о ее работе.

Пользователи, переходящие на Windows 8 с предыдущей версии Windows, обнаружат обширные изменения пользовательского интерфейса. Это одна из самых значительных переработок операционной системы. Операционная система Windows 8 теперь поддерживает сенсорный пользовательский интерфейс в дополнение к традиционным мыши и клавиатуре. При работе с компьютерами, обладающими возможностями сенсорного интерфейса, элементами на экране можно управлять такими способами, какие ранее были невозможны. В частности, можно выполнять следующие управляющие действия.

- **Нажатие.** Нажмите элемент, коснувшись его пальцем. Нажатие или двойное нажатие элемента на экране обычно эквивалентно одинарному или двойному щелчку левой кнопкой мыши.
- **Длительное нажатие.** Коснитесь пальцем элемента и удерживайте нажатие в течение 2—3 секунд. Этот жест эквивалентен щелчку правой кнопкой мыши.
- **Скольжение вниз (выбор).** Слегка проведите пальцем вниз по элементу. Этот жест выбирает элемент и открывает его контекстное меню. Если жест длительного нажатия не открывает контекстное меню элемента, попробуйте открыть его этим жестом.
- **Скольжение от края экрана.** Проведите пальцем от края экрана к центру. Скольжение от правого края открывает кнопочную панель (Charms bar). А скольжение от левого края позволяет переключаться между открытыми приложениями, подобно использованию комбинации клавиш <Alt>+<Tab>. Скольжение от нижнего или верхнего края отображает команды для активного элемента.
- **Щипок.** Коснитесь элемента двумя пальцами, а затем сведите пальцы вместе. Этот жест уменьшает масштаб элемента.
- **Растяжение.** Коснитесь элемента двумя пальцами, а затем разведите пальцы. Этот жест увеличивает масштаб элемента.

Еще одной возможностью нового интерфейса является экранная клавиатура. Хотя изменения пользовательского интерфейса довольно обширные, это не самые важные изменения операционной системы. Наиболее важные изменения находятся, так сказать, за кулисами,

затрагивают базовую архитектуру операционной системы и предоставляют многие новые возможности.

Справочники должны быть портативными и читабельными, т. е. книгами такого типа, которые применяются для решения проблем и выполнения задач в любом месте и в любое время. Поэтому мне пришлось внимательно следить за тем, чтобы в своих исследованиях фокусироваться на основных аспектах Windows 8. В результате получилась книга, которую вы держите в руках и которая, я надеюсь, вы согласитесь, является одним из наилучших "портативных" руководств по Windows 8. По мере углубления в книгу, в ней охватывается все, что необходимо для выполнения основных задач по настройке, оптимизации и обслуживанию Windows 8.

Так как моей основной целью было предоставить как можно больше полезной информации в справочнике, читателю нет надобности перелистывать бесчисленные страницы с ненужной информацией в поисках той, которая ему действительно требуется. Вместо этого вы найдете в ней как раз то, что вам необходимо для решения конкретной проблемы или выполнения определенной задачи. Одним словом, эта книга призвана быть тем ресурсом, к которому можно обращаться при возникновении у вас любых вопросов касательно настройки и обслуживания Windows 8. Внимание читателя будет фокусировано на ежедневных процедурах, часто выполняемых задачах, задокументированных примерах и опциях, которые являются типичными, хотя не обязательно исчерпывающими.

Одна из целей этой книги — предоставить читателю как можно больше информации, чтобы сделать ее ценным ресурсом, и представить книгу в компактной и удобной для просмотра форме. Вместо увесистого фолианта в тысячу с лишним страниц или тетрадки-справочника, вы получите ценное руководство, которое поможет вам быстро и с легкостью выполнять общие задачи, решать распространенные проблемы и реализовать повседневные решения.

Для кого предназначена эта книга

Эта книга основана на выпусках Standard, Professional и Enterprise операционной системы Windows 8 и предназначена для следующего круга читателей:

- продвинутых пользователей, которые планируют самостоятельно настраивать и обслуживать Windows 8;
- системных администраторов и персоналу поддержки, работающих с Windows 8;
- администраторов, выполняющих обновление более ранних версий Windows к Windows 8;
- администраторов, которые переходят на Windows 8 с других платформ.

Задача "упаковать" в книгу как можно больше информации предусматривает, что ее читатели имеют основные навыки работы с сетями и базовые знания об операционных системах Windows. В результате книга не содержит глав, полностью направленных на объяснение основных понятий Windows, архитектуры этой операционной системы или организации сетей в ней. Но, с другой стороны, в ней охватывается настройка рабочего стола, мобильные сети, настройка параметров TCP/IP, профилей пользователей и оптимизация системы. Также в ней углубленно рассматривается вопрос поиска и устранения неполадок. В этом отношении, каждая глава, насколько это применимо, содержит рекомендации и обсуждение диагностирования проблем, касающихся рассматриваемого в ней материала. Рекомендации по поиску и устранению неполадок интегрированы с основным материалом книги, вместо выделения их в отдельную всеохватывающую главу, добавленную для проформы. Автор надеется, что после прочтения этой книги, разобравшись во всех ее подробностях, вы сможете повысить опыт ваших пользователей и понизить уровень простоя.

Организация книги

Книга предназначена для использования в качестве руководства по настройке, оптимизации и технического обслуживания Windows 8 и поэтому организована по рабочим задачам, а не по функциональностям этой операционной системы.

Книги данной серии служат для помощи в поиске быстрого и работающего решения повседневных задач. Поэтому важными составляющими этого практического руководства являются быстрота и легкость нахождения в нем требуемого материала. Книга имеет расширенное содержание и подробный алфавитный указатель для быстрого нахождения решений проблем. Кроме этого, она содержит многие другие материалы для быстрой справки, включая пошаговые инструкции, списки, таблицы с кратким изложением основных понятий, а также большое число перекрестных ссылок.

Типографские соглашения

В книге используются разные способы придания тексту ясности и удобочитаемости. В частности, листинги кода, вводимые команды и значения параметров оформлены моноширинным шрифтом. Также, при представлении или определении новых терминов, они даются *курсивом*.

Кроме этого, используются следующие текстовые вставки.

- **Рекомендации.** Описание наилучших методов для работы с расширенными возможностями настройки и обслуживания.
- **Осторожно!** Предупреждение о возможных проблемах, для которых следует быть настороже.
- **Важно!** Выделение важных понятий и вопросов.
- **Дополнительная информация.** Предоставление дополнительной информации по рассматриваемому предмету.
- **Примечание.** Предоставление дополнительных подробностей по определенному вопросу, требующему выделения.
- **Практический совет.** Практические рекомендации при рассмотрении продвинутых понятий.
- **Внимание!** Выделение важных вопросов безопасности.
- **Совет.** Полезные советы или дополнительная информация.

Автор очень надеется, что вы убедитесь: эта книга предоставляет всю необходимую информацию для выполнения основных задач в Windows 8. Ваши замечания или предложения касательно этой книги можете отправлять по адресу **williamstanek@aol.com**.

Спасибо.

Список опечаток и поддержка книги

Мы приложили все усилия для обеспечения точности информации в этой книге и сопровождающего ее содержимого. Список всех ошибок, обнаруженных после издания этой книги, выложен на странице издательства "Microsoft Press" веб-сайта издательства O'Reilly по адресу:

http://go.microsoft.com/FWLink/?Linkid=258654

Если вы обнаружите ошибку, которой нет в этом списке, можете сообщить о ней на этой же странице.

Если вам требуется дополнительная помощь по этой книге, отправьте свой запрос в службу поддержки книг издательства "Microsoft Press" по адресу **mspinput@microsoft.com**.

Обратите внимание, что поддержка программного обеспечения корпорации Microsoft по данного адресу не предоставляется.

Ваше мнение о книге

Для издательства "Microsoft Press" мнение читателей является высшим приоритетом, и ваши отзывы и отклики на наши книги представляют для нас большую ценность. Дайте нам знать, что вы думаете об этой книге в опросе по следующему адресу:

http://www.microsoft.com/learning/booksurvey

Участие в этом опросе не отнимет у вас много времени, а мы читаем все ваши замечания и предложения. Заранее благодарим вас за ваше мнение.

Не пропадайте!

Давайте продолжим наше общение. Мы на Twitter: **http://twitter.com/MicrosoftPress**.

ГЛАВА 1

Введение в администрирование Windows 8

Операционная система Windows 8 главным образом предназначена для работы с клиентскими устройствами. В этой главе рассматривается начало работы с Windows 8 и основные действия для ее администрирования. Здесь, как и во всех других главах этой книги, подробно обсуждаются изменения, которые улучшают управление компьютером и его безопасностью. Хотя в этой книге основное внимание уделяется администрированию Windows 8, предлагаемые в ней советы и методы могут быть полезными для любого типа работы с Windows 8, будь то техническая поддержка, разработка программного обеспечения или выполнение пользовательских задач.

Следует иметь в виду, что эту книгу лучше читать совместно с книгой "Windows Server 2012 Pocket Consultant" (Microsoft Press, 2012). Кроме широкого круга заданий администрирования, в книгах серверной области серии "Карманный консультант" рассматривается администрирование таких конкретных аспектов, как службы каталогов, данных и сети. Эта же книга фокусируется на задачах администрирования пользователей и системы. В ней подробно рассматриваются следующие темы:

- настройка операционной системы и среды Windows;
- конфигурирование аппаратного обеспечения и сетевых устройств;
- управление доступом пользователей и глобальными настройками;
- конфигурирование мобильных сетей;
- использование возможностей удаленного управления и помощи;
- поиск и устранение неисправностей системы.

Кроме этого, также важно обратить внимание на то, что почти каждой опцией конфигурации операционной системы Windows можно управлять посредством групповой политики. Вместо того чтобы каждый раз оговаривать, что возможность *А* или *Б* можно конфигурировать, только если это разрешено в групповой политике, предполагается, что читатель обладает достаточными знаниями и понимает глобальное влияние групповых политик на конфигурирование и управление системой. Кроме этого, предполагается, что читатель знает, как работать с командной строкой и интерфейсом Windows PowerShell. Это позволит фокусироваться на важных задачах администрирования.

Начало работы с Windows 8 — краткий обзор

Операционная система Windows 8 является последней версией семейства операционных систем Windows для клиентских компьютеров. В Windows 8 встроена поддержка установки

и развертывания на основе образов. Операционные системы Windows 8, Windows 8 Pro и Windows 8 Enterprise поддерживают 32-разрядные процессоры *x*86 и 64-разрядные процессоры *x*64 для настольных и планшетных компьютеров. Windows 8 RT поддерживает процессоры ARM. Для многих продвинутых возможностей, таких как технология шифрования BitLocker, шифрующая файловая система EFS (Encrypting File System), присоединение к домену, групповая политика и подключение к удаленному рабочему столу, требуется версия Windows 8 Pro или Windows 8 Enterprise.

32- и 64-разрядные версии Windows 8 поставляются на отдельных установочных носителях. Для установки 32-разрядной версии Windows 8 на компьютер с архитектурой *x*86 нужно использовать 32-разрядный установочный носитель, а для установки 64-разрядной версии Windows 8 на компьютер с архитектурой *x*64 — 64-разрядный. В общем, для установки 64-разрядной операционной системы на компьютер с уже установленной 32-разрядной ОС (аппаратные средства которого поддерживают обе версии операционной системы) компьютер необходимо перезагрузить с установочного носителя. То же самое обычно действенно и для установки 32-разрядной операционной системы на компьютер с установленной 64-разрядной ОС.

Примечание

Операционная система Windows 8 RT, как правило, предустанавливается на устройствах с процессорами ARM и значительно отличается от других версий Windows 8.

Для обеспечения языковой независимости в Windows 8 применяется модульность, а для аппаратной независимости используются образы дисков. Каждый компонент операционной системы разработан как независимый модуль, который можно с легкостью добавить или удалить. Эта функциональность составляет основу архитектуры конфигурации Windows 8. Корпорация Microsoft распространяет Windows 8 на носителях, содержащих сжатые единичные экземпляры образов дисков, что значительно уменьшает размер файлов образов. Для образов дисков используется формат Windows Imaging (WIM).

Вместо MS-DOS в качестве предустановочной среды для Windows 8 используется среда Windows PE[1] 4.0, которая предоставляет начальную загрузочную среду для установки, развертывания, восстановления, поиска и устранения неполадок. Диспетчер загрузки предустановочной среды Windows позволяет выбрать приложение для загрузки операционной системы. На компьютерных системах с возможностью загрузки нескольких операционных систем возможность загрузки операционной системы, предшествующей Windows 7, предоставляется в загрузочной среде посредством предоставления выбора требуемой унаследованной системы.

Возможность контроля учетных записей пользователей UAC (User Account Control) повышает безопасность компьютерной системы, обеспечивая настоящее разделение учетных записей обычных пользователей и пользователей с правами администратора. Возможность UAC позволяет исполнять все приложения либо с разрешениями обычного пользователя, либо с разрешениями администратора. При попытке запуска любого приложения, требующего разрешений администратора, выводится соответствующее сообщение системы безопасности. Условия для вывода данного сообщения системы безопасности определяются настройками групповой политики. Для пользователей, вошедших в систему под встроенной учетной записью администратора, сообщения системы безопасности не выводятся.

[1] Preinstallation Environment.

Windows 8 содержит несколько ключевых элементов пользовательского интерфейса, включая следующие:

- экран **Пуск** (Start);
- панель кнопок (Charm Bar);
- панель поиска;
- панель настроек рабочего стола;
- экран настройки параметров компьютера;
- экран приложений (также называется **Все приложения**[1]).

В Windows 8 традиционное меню **Пуск** предыдущих версий операционной системы заменено экраном **Пуск**. Обратите внимание, что теперь **Пуск** является *окном*, а не меню. Программы в окне **Пуск** представляются посредством *плиток* и запускаются с помощью касания (на системах с сенсорным вводом) или щелчка мышью (на системах с обычным вводом). При нажатии и удерживании плитки или при щелчке по ней правой кнопкой мыши вместо контекстного меню выводится *панель опций*.

Одним из быстрых способов запуска программы из окна **Пуск** будет нажатие клавиши <Windows>, ввод имени исполняемого файла программы, а затем нажатие клавиши <Enter>. Но этот способ действенен только в том случае, если окно **Поиск приложений** (Apps Search) находится в фокусе (что обычно происходит по умолчанию).

Нажатие клавиши <Windows> переключает между окном **Пуск** и рабочим столом или, при работе с параметрами компьютера (**PC Settings**), между окном **Пуск** и окном настройки параметров. В окне **Пуск** есть плитка **Рабочий стол**, касание или щелчок по которой отображает рабочий стол. Рабочий стол можно также отобразить, нажав комбинацию клавиш <Windows>+<D>, а нажав и удерживая комбинацию клавиш <Windows>+<+>, рабочий стол можно отобразить для просмотра, пока вы не отпустите эту комбинацию клавиш.

Кнопочная панель (Charm Bar) является средством для выбора опций для окон **Пуск**, **Рабочий стол** и **Параметры**. На платформе с сенсорным экраном кнопочную панель можно отобразить, выполнив скользящее движение по экрану справа налево. В системе с традиционным интерфейсом (т. е. с клавиатурой и мышью) кнопочную панель можно отобразить, поместив указатель мыши над скрытой кнопкой в правом верхнем или нижнем углу экрана **Пуск**, **Рабочий стол** или **Параметры** либо нажав комбинацию клавиш <Windows>+<C>.

На кнопочной панели размещено пять кнопок.

- **Поиск** (Search). Касание или щелчок кнопки **Поиск** отображает одноименную панель. Все, что вводится с клавиатуры в экране **Пуск**, вводится в поле поиска панели **Поиск**. Фокус этой панели можно установить на опции **Приложения** (Apps), **Параметры** (Settings) или **Файлы** (Files). Когда фокус поиска установлен на одной из этой опций, панель **Поиск** можно использовать для быстрого нахождения соответствующих элементов — установленных программ, настроек и опций в Панели управления или файлов.
- **Отправка** (Share). Касание или нажатие кнопки **Отправка** включает возможности общего доступа для приложения рабочего стола. Например, при работе с приложением **Карты** (Maps) обычно предоставляются опции для общего использования карты, с которой выполняется работа.
- **Пуск** (Start). Касание или нажатие кнопки **Пуск** переключает между рабочим столом и окном **Пуск** (или, при работе с настройкой параметров компьютера, между окном **Пуск** и окном параметров).

[1] All Apps.

- **Устройства** (Devices). Касание или нажатие кнопки **Устройства** предоставляет быстрый доступ к присоединенным устройствам, например второму экрану.
- **Параметры** (Settings). Касание или нажатие кнопки **Параметры** открывает одноименную панель, предоставляющую возможность настройки различных параметров, включая опции питания для переключения компьютера в спящий режим, выключения и перезагрузки.

> ***Совет***
>
> Обычно по умолчанию фокус поиска установлен на опции **Приложения**, что позволяет быстро открыть программу из окна **Пуск**, введя название ее исполняемого файла и нажав клавишу <Enter>.

Панель **Параметры** можно также открыть, нажав комбинацию клавиш <Windows>+<I>. Из этой панели можно выполнять следующие операции:

- просматривать подключенные сети и их статус (значок **Сеть**);
- просматривать и изменять громкость звука (значок динамика);
- изменять уровень яркости экрана (только для портативных устройств);
- временно скрывать уведомления (значок **Уведомления**);
- выбирать один из режимов работы компьютера — спящий, завершение работы, перезагрузка;
- открывать экранную клавиатуру (только для устройств с сенсорным интерфейсом);
- открывать окно **Параметры**, нажав ссылку **Изменение параметров компьютера** (Change PC Settings).

Панели настройки параметров окна **Пуск**, рабочего стола и компьютера очень похожи. Панель **Параметры** окна **Пуск** имеет опцию **Плитки** (Tiles), касание или щелчок по которой открывает панель для добавления к экрану **Пуск** (или удаления с него) плиток для средств администрирования, а также опцию для удаления личной информации с плиток. Панель **Параметры** рабочего стола содержит другие опции, а именно:

- **Панель управления** (Control Panel) для открытия панели управления;
- **Персонализация** (Personalization) для открытия одноименного окна Панели управления;
- **Сведения о компьютере** (PC Info) для открытия окна **Система** (System) Панели управления;
- **Справка** (Help) для открытия окна **Справка и поддержка** (Help and Support).

Одним из способов получения быстрого доступа к панели **Параметры** (окна **Пуск** или рабочего стола, в зависимости от текущего выбора этих элементов) будет нажатие комбинации клавиш <Windows>+<I>.

Панель задач рабочего стола по умолчанию содержит значок средства просмотра файловой системы **Проводник**. Это позволяет открыть панель управления, выполнив следующие действия:

- открыть Проводник, коснувшись или щелкнув по его значку в панели задач;
- коснуться или щелкнуть по узлу **Компьютер** в левой панели;
- коснуться значка **Открыть панель управления** в панели инструментов или щелкнуть по нему.

Еще рекомендуется освоить метод быстрого открытия окна **Приложения**, которое содержит список всех установленных приложений, разбитых по категориям.

Окно **Приложения** отображается при запуске поиска приложений (панель **Поиск**, опция **Приложения**). Чтобы закрыть панель **Поиск** и отображать только окно **Приложения**, нужно коснуться или щелкнуть в области окна **Приложения**. Для быстрого доступа к окну приложения из окна **Пуск** или рабочего стола нужно нажать комбинацию клавиш <Windows>+<Q>. Другим способом открыть окно **Приложения** будет открытие панели **Поиск**, выбор опции **Приложения**, а затем прикосновение или щелчок в области окна **Приложения**, чтобы скрыть панель **Поиск**.

В категории **Служебные | Windows** (Windows System) окна **Приложения** содержатся приложения, применяемые для основных задач администрирования системы, включая такие, как **Командная строка** (Command Prompt), **Компьютер** (Computer), **Панель управления** (Control Panel), **Диспетчер задач** (Task Manager), **Проводник** (File Explorer) и **Windows PowerShell**.

Примечание

В версиях Windows 8 Pro и Enterprise приложение Windows PowerShell обычно поставляется как стандартная функция. Чтобы открыть приложение Windows PowerShell из окна **Пуск**, введите с клавиатуры `powershell` и нажмите клавишу <Enter>. Но этот способ действенен только в том случае, если приложение Windows PowerShell является первым совпадением в списке результатов для ключевого слова "powershell". В случае возвращения нескольких результатов вместо нажатия клавиши <Enter> коснитесь того из них или щелкните[1] по тому, который соответствует требуемому приложению.

Совет

Приложения из окна **Приложения** можно поместить в окно **Пуск** или панель задач рабочего стола. Для этого нажмите и удерживайте пальцем или щелкните правой кнопкой требуемый значок, а затем, в открывшейся панели, коснитесь или щелкните мышью значок **Закрепить на экране "Пуск"** (Pin To Start) или **Закрепить на панели задач** (Pin To Taskbar). Для упрощения администрирования компьютера рекомендуется добавить на панель задач значки **Командная строка**, **Компьютер**, **Панель управления** и **Windows PowerShell**.

С Windows 8 имеет смысл использовать приложение Windows PowerShell для исполнения как обычных команд Windows, так и команд Windows PowerShell. Но хотя любые обычные консольные команды можно исполнять в консоли Windows PowerShell, нужно иметь в виду, что это возможно благодаря тому, что это приложение полагается в своей работе на внешние приложения и утилиты. Поэтому обычные консольные команды будут исполняться в консоли Windows PowerShell только в том случае, если для их исполняемых файлов указан правильный путь в переменной среды `PATH` и при наличии этих файлов в указанном месте. Также нужно иметь в виду, что порядок исполнения команд в консоли Windows PowerShell может повлиять на ожидаемое исполнение команды. Порядок исполнения команд в консоли Windows PowerShell следующий:

1. Альтернативные встроенные или определенные в профиле псевдонимы.
2. Встроенные или определенные в профиле функции.

[1] С целью избежания многословия и сопутствующего рассредоточения внимания в книге используется только один вариант описания основных действий с устройствами ввода — для устройств с традиционными средствами ввода, а соответствующие действия для сенсорных устройств подразумеваются. В частности, это относится к работе с кнопками мыши — левый щелчок мыши также подразумевает краткое касание сенсорного экрана, правый щелчок мыши также подразумевает длительное нажатие сенсорного экрана, а двойной щелчок мышью — двойное касание сенсорного экрана. В случаях отсутствия соответствия сенсорного ввода традиционному способу дается описание обоих вариантов.

3. Командлеты[1] или текстовые ключевые слова.
4. Сценарии с расширением psl.
5. Внешние команды, утилиты и файлы.

Таким образом, если любой элемент из категории 1—4 порядка исполнения имеет то же самое имя, что и обычная консольная команда, вместо ожидаемого исполнения требуемой команды исполнится данный элемент.

Приложение Windows PowerShell входит в стандартный комплект поставки Windows 8. Настроив это приложение для удаленной работы, в нем можно различными способами исполнять команды на удаленных компьютерах. Один из способов — установить сеанс удаленной работы с требуемыми компьютерами. В следующем примере показано, как проверить версию Windows на удаленных компьютерах:

```
$s = new-pssession -computername engpc15, hrpc32, cserpc28
invoke-command -session $s {dism.exe /online /get-currentedition}
```

В результате исполнения этой команды выводится следующее (показанное частично) сообщение:

```
Deployment Image Servicing and Management tool
Version: 6.1.7600.16385

Image Version: 6.1.7600.16385

Current Edition: Ultimate
The operation completed successfully.
```

Внутренний номер версии для Windows 7 — 6.1, а для Windows 8 — 6.2. Таким образом, по выводу результата исполнения этой команды мы знаем, что на удаленном компьютере установлена версия Windows 7 Ultimate.

> ***Примечание***
>
> С командой `New-PSSession` применяется параметр `-ComputerName` для указания удаленных компьютеров по имени DNS, NetBIOS или IP-адресу. При указании нескольких удаленных компьютеров их имена или IP-адреса разделяются запятыми. Дополнительную информацию по удаленной работе в целом и работе с консолью Windows PowerShell в частности *см. в главе 6* книги "Windows PowerShell 2.0. Справочник администратора"[2].

64-разрядные вычисления

С того времени, когда 64-разрядные вычисления начали применяться в операционных системах Windows, они (вычисления) претерпели значительные изменения. Компьютеры под управлением 64-разрядных версий Windows не только работают быстрее и лучше, чем компьютеры с 32-разрядными версиями, но они также масштабируются лучше, т. к. могут обрабатывать больший объем данных за один такт, обращаться к более обширному адресному пространству памяти, а также выполнять числовые расчеты быстрее.

---

[1] Командлеты (cmdlets) — это специализированные команды PowerShell, которые реализуют различную функциональность. Это встроенные в PowerShell команды.

[2] Станек У. Р. Windows PowerShell 2.0. Справочник администратора. — СПб.: Русская редакция, БХВ-Петербург, 2010.

Существуют две разные 64-разрядные архитектуры.

- **Архитектура *x*64.** Эта архитектура основана на 64-разрядном расширении набора инструкций *x*86 и реализуется в процессорах Opteron компании AMD (AMD64), в процессорах Xeon с 64-разрядным расширением компании Intel, а также в других процессорах. Эта архитектура поддерживает интегрированный 32-разрядный режим вычислений и 64-разрядное расширение, что позволяет одновременно выполнять 32- и 64-разрядные вычисления.
- **Архитектура IA64.** Эта архитектура основана на микропроцессорной архитектуре EPIC[1], применяемой в процессорах Itanium компании Intel (IA64) и в других процессорах, и поддерживает интегрированные 64-разрядные вычисления, позволяя 64-разрядным приложениям достичь оптимальной производительности.

Более распространена архитектура *x*64, которая также является основной 64-разрядной архитектурой для персональных и планшетных компьютеров, поддерживаемой Windows 8. В общем, 64-разрядные вычисления предназначены для операций, интенсивно использующих память и требующих выполнения обширных числовых расчетов. Применяя 64-разрядные вычисления, приложения могут загружать большие объемы данных в физическую (т. е. оперативную) память, что уменьшает необходимость вытеснения данных в файл подкачки на диск и значительно повышает производительность.

В настоящее время наиболее распространенными являются следующие микропрограммные интерфейсы:

- BIOS (Basic input/output system, базовая система ввода/вывода);
- EFI (Extensible Firmware Interface, расширяемый микропрограммный интерфейс);
- UEFI (Unified Extensible Firmware Interface, единый расширяемый микропрограммный интерфейс).

Компьютеры на основе архитектуры Itanium отличаются от компьютеров на основе архитектуры *x*86 и *x*64 во многих фундаментальных аспектах. Тогда как в компьютерах с архитектурой Itanium используется интерфейс EFI и диски с таблицами разделов типа GPT[2] для загрузочных и системных разделов, в компьютерах с архитектурой *x*86 для этого используется интерфейс BIOS и диски с главной загрузочной записью MBR (Master Boot Record). В компьютерах типа *x*64 применяется оболочка UEFI над BIOS или EFI *(см. разд. "Опции микропрограммы и их значения" главы 4)*. Это означает, что управление компьютерами с этими различными архитектурами осуществляется по-разному, особенно при установке и конфигурировании диска. Но со все возрастающим признанием и популярностью интерфейса UEFI и возможностью Windows 8 использовать как диски с MBR, так и диски с GPT, базовая архитектура микропроцессора не обязательно будет определяющей для используемого в компьютере типа микропрограммного обеспечения и диска. Это решение будет в руках производителей аппаратного обеспечения.

> ***Примечание***
>
> Методы работы с дисками типа MBR и GPT подробно рассматриваются в *главе 12*. Обычно в компьютерах с BIOS для загрузочных дисков или дисков данных используют диски с записью MBR, а диски GPT применяются только для хранения данных. А в компьютерах с интерфейсом EFI можно использовать как GPT, так и MBR-диски, но при этом требуется наличие хотя бы одного диска GPT, содержащего системный раздел EFI и основной раздел или простой том, содержащий операционную систему для загрузки.

[1] Explicitly Parallel Instruction Computing — вычисления с заданным параллелизмом команд.

[2] GUID partition table.

В большинстве случаев 64-разрядное оборудование совместимо с 32-разрядными приложениями, но 32-разрядные приложения работают лучше на 32-разрядном оборудовании. 64-разрядные версии Windows поддерживают как 64-разрядные, так и 32-разрядные приложения, используя для этого слой эмуляции WOW64[1]. Подсистема WOW64 изолирует 32-разрядные приложения от 64-разрядных, вследствие чего предотвращаются проблемы с файловой системой и реестром. Операционная система предоставляет функциональную совместимость через барьер 32/64-разрядности для модели COM и для таких основных операций редактирования, как вырезание, копирование и вставка посредством буфера обмена. Но 32-разрядные процессы не могут загружать 64-разрядные динамические библиотеки (DLL), а 64-разрядные процессы — 32-разрядные библиотеки.

При переходе на 64-разрядные вычисления рекомендуется отслеживать компьютеры, поддерживающие 64-разрядные операционные системы, и компьютеры, на которых такие системы уже установлены. В этом отношении с помощью консоли Windows PowerShell можно получить следующую информацию.

- Определить, установлена ли на компьютере 64-разрядная операционная система, используя для этого свойство `OSArchitecture` объекта `Win32_OperatingSystem`. Вот пример использования этого свойства в команде Windows PowerShell:

  ```
  get-wmiobject -class win32_operatingsystem | fl osarchitecture
  ```

  Результат исполнения этой команды будет следующим:

  ```
  osarchitecture : 32-разрядная
  ```

- Определить, поддерживает ли компьютер 64-разрядные операционные системы, используя для этого свойства `Name` и `Description` объекта `Win32_Processor`:

  ```
  get-wmiobject -class win32_processor | fl name, description
  ```

  Пример результата исполнения этой команды таков:

  ```
  name        : Intel(R) Core(TM)2 Quad CPU@ 2.66CHZ
  description : x64 Family 6 Model 15 Stepping 7
  ```

В выводе первой команды сообщается, что на компьютере установлена 32-разрядная версия Windows, а в выводе второй, что данный компьютер имеет процессор типа *x*64. Это означает, что компьютер можно модернизировать до 64-разрядной версии Windows 8.

Для облегчения задачи проверки всех компьютеров можно создать сценарий, который выполнит всю работу автоматически. С примерами сценариев с пошаговым объяснением их работы можно ознакомиться в *главе 8* книги "Windows PowerShell 2.0. Справочник администратора".

Развертывание Windows 8

Windows 8 позволяет выполнять ручное или автоматизированное развертывание специализированных сборок. Для ручного развертывания Windows нужно создать обязательные загрузочные и установочные образы, а также факультативно — образы для восстановления. Для автоматизации процесса развертывания необходимо установить службу развертывания Windows Deployment Services (WDS). Независимо от типа развертывания — полностью ручного, полностью автоматизированного или комбинированного — выполняются подоб-

[1] Windows-on-Windows 64-bit.

ные административные задания. Для выполнения этих заданий необходимо понимать и использовать набор Windows ADK[1] для Windows 8 и службу WDS[2].

Набор Windows ADK для Windows 8 можно загрузить с сайта загрузок корпорации Microsoft (**download.microsoft.com**). Этот набор содержит инструменты для развертывания образов Windows, включая следующие:

- набор ACT[3];
- стандартные средства для развертывания и создания образов;
- инструмент USMT[4];
- инструмент VAMT[5];
- службы оценки Windows Assessment Services (WAS);
- набор инструментов оценки Windows Assessment Toolkit (WAT);
- набор WPT[6];
- среду предустановки Windows (WPE[7]).

С помощью службы развертывания WDS развертывание Windows 8 можно выполнять по сети. Роль службы WDS можно добавить на любой сервер, работающий под управлением Windows Server 2012.

Для Windows 8 и Windows Server 2012 используется среда предустановки Windows PE 4.0. Она предоставляет возможности операционной системы для выполнения следующих заданий.

- **Установка.** При установке Windows 8 графические инструменты, которые собирают информацию о системе на этапе настройки, исполняются в среде Windows PE.
- **Развертывание.** Когда при установке операционной системы компьютер загружается по сети, встроенный клиент среды предзагрузки PXE[8] может подключиться к серверу службы WDS, загрузить по сети образ Windows PE, а затем исполнить в этой среде сценарии развертывания.
- **Восстановление.** В случае проблем с запуском Windows 8 вследствие поврежденных системных файлов среда Windows PE позволяет запустить средство SRP[9] для восстановления возможности загрузки.
- **Поиск и устранение неполадок.** В случае проблем в работе Windows 8 компьютер можно загрузить в среду Windows PE для поиска и устранения неполадок или для диагностики, если причину этих проблем невозможно обнаружить иным способом.

Модульная и расширяемая среда Windows PE предоставляет полный доступ к разделам файловых систем FAT и NTFS. Так как среда Windows PE состоит из подмножества компо-

---

[1] Windows Assessment and Deployment Kit — набор для оценки и развертывания Windows.

[2] Windows Deployment Services — службы развертывания Windows.

[3] Application Compatibility Toolkit — набор средств для обеспечения совместимости приложений.

[4] User State Migration Tool — инструмент для переноса состояния пользователя.

[5] Volume Activation Management Tool — средство управления активацией корпоративных лицензий.

[6] Windows Performance Toolkit — набор средств для оценки производительности Windows.

[7] Windows Preinstallation Environment.

[8] Preboot Execution Environment — предзагрузочная среда исполнения.

[9] Startup Repair Tool.

нентов Windows, в ней можно исполнять многие приложения Windows, работать с аппаратными устройствами и работать в сетевом окружении по IP-протоколу. Среда Windows PE содержит несколько инструментов командной строки, включая следующие.

- **BCDBoot.** Инструмент для инициализации хранилища данных о конфигурации загрузки BCD; также позволяет копировать файлы среды загрузки в системный раздел.
- **Bootsect.** Средство для создания и работы с загрузочными секторами на жестких и твердотельных дисках (флеш-накопителях).
- **Copype.** Средство для создания структуры каталогов для файлов Windows PE и копирования файлов с носителя Windows PE, что является предусловием для создания загрузочного носителя Windows PE.
- **DiskPart.** Инструмент для создания и работы с дисками, разделами и томами.
- **DISM.** Инструмент с расширенными возможностями для технического обслуживания и содержания в исправности образов.
- **Drvload.** Средство поддержки для добавления драйверов устройств и динамической загрузки драйверов после запуска среды Windows PE.
- **ImageX.** Средство для создания и заливки образов Windows.
- **Lpksetup.** Инструмент для добавления и удаления языковых пакетов.
- **Makewinpemedia.** Средство для создания загрузочного носителя Windows PE.
- **Net.** Набор утилит для управления локальными пользователями, запуска и остановки служб и подключения к общим папкам.
- **Netcfg.** Инструмент для настройки доступа к сети.
- **Oscdimg.** Средство для создания файлов образов ISO для CD и DVD.
- **Wpeinit.** Средство, которое инициирует Windows PE при загрузке.

Новые инструменты в наборе Windows PE — Copype и Makewinpemedia — позволяют облегчить создание загрузочного носителя Windows PE. Средство Copype применяется для установки среды сборки Windows PE. После выполнения необходимой настройки сборки с помощью средства Makewinpemedia создается загрузочный носитель, для которого можно использовать CD, DVD, флеш-накопитель или внешний жесткий диск с USB-интерфейсом.

Использование DISM

Одним из наиболее важных средств развертывания является система DISM[1]. Система DISM поставляется в штатном порядке с версиями Windows 8 Pro и Windows 8 Enterprise.

С помощью этой системы можно управлять подключенными и автономными образами операционной системы Windows, включая образы для развертывания и образы для виртуальных машин. Для развертывания Windows 8 применяются файлы образов Windows (с расширением wim), а для виртуальных машин — файлы виртуальных жестких дисков (с расширением vhd). Для работы с файлами WIM и VHD применяются одинаковые команды.

С помощью средства DISM можно выполнять следующие задания:

- добавлять и удалять из образа пакеты, такие как языковые пакеты, заплатки, утилиты и т. п.;

[1] Deployment Image Servicing and Management — система обслуживания образов развертывания и управления ими.

- включать и отключать функциональности Windows;
- добавлять и удалять драйверы устройств сторонних разработчиков.

Для работы со средством DISM в командной строке с правами администратора выполните следующие действия:

1. В экране **Приложения** программа **Командная строка** находится в категории **Служебные | Windows** (Windows System).
2. Нажмите и удерживайте значок консоли или щелкните на нем правой кнопкой мыши и в открывшейся панели внизу экрана коснитесь или щелкните на опции **Запуск от имени администратора** (Run As Administrator).
3. Если откроется окно **Контроль учетных записей пользователей** (User Account Control), запрашивающее, можно ли разрешить данной программе вносить изменения на этом компьютере, нажмите кнопку **Да**.
4. В открывшемся окне командной строки введите команду `dism /?`, чтобы просмотреть доступные команды и опции утилиты DISM.
5. Для просмотра списка команд для работы с оперативными образами введите команду `dism /online /?`.

Хотя утилита DISM предназначена в основном для работы с автономными и подключенными образами, некоторые из ее команд можно использовать для получения важной информации о "живой" операционной системе, работающей на компьютере. В табл. 1.1 приводится список и краткое описание подмножества онлайновых команд средства DISM, которые можно использовать с "живыми" операционными системами. Например, для отображения списка версий Windows, к которым можно обновить компьютер, используется команда:

```
dism /online /get-targeteditions
```

Таблица 1.1. *Онлайновые команды DISM, применимые с работающими операционными системами*

Команда	Описание
`/Disable-Feature /featurename:`*`FeatureName`*	Отключает указанную функциональность. Имена функциональностей чувствительны к регистру
`/Enable-Feature /featurename:`*`FeatureName`*	Включает указанную функциональность. Имена функциональностей чувствительны к регистру
`/Get-CurrentEdition`	Отображает установленную версию Windows
`/Get-DriverInfo /driver.`*`DriverName.inf`*	Выводит информацию об указанном драйвере стороннего разработчика, установленном в хранилище драйверов. Имена драйверов не чувствительны к регистру
`/Get-Drivers`	Выводит информацию обо всех драйверах сторонних разработчиков, установленных в хранилище драйверов
`/Get-FeatureInfo /featurename:`*`FeatureName`*	Отображает информацию об указанной функциональности. Имена функциональностей чувствительны к регистру
`/Get-Features`	Отображает информацию об установленных возможностях Windows
`/Get-Intl`	Выводит информацию об используемом по умолчанию языке пользовательского интерфейса, языке системы, часовом поясе по умолчанию, языках клавиатуры, а также об установленных языках
`/Get-PackageInfo /packagename:`*`PackageName`*	Отображает информацию об указанном пакете. Имена пакетов чувствительны к регистру

Таблица 1.1 *(окончание)*

Команда	Описание
`/Get-Packages`	Отображает информацию об установленных пакетах Windows
`/Get-TargetEditions`	Выводит список версий Windows, к которым можно обновить текущую операционную систему

Образы Windows

Добавление или удаление функциональностей в Windows 8, применение исправлений или установка пакетов обновлений осуществляется простым изменением набора имеющихся модулей. А так как эти модули являются независимыми, эти изменения можно выполнить, не подвергая изменениям систему как целое. Тот факт, что языковые пакеты также являются отдельными модулями, позволяет с легкостью реализовывать разные языковые конфигурации без надобности выполнять отдельную остановку для каждого языка.

Корпорация Microsoft поставляет Windows 8 на носителях с образами дисков WIM. В формате WIM применяются сжатие и метод сохранения единственной копии файлов, что существенно уменьшает размер файлов образа. Сжатие уменьшает размер файла образа во многом подобно тому, как сжатие в формате ZIP уменьшает размер обычных файлов. А применения метода единственной копии уменьшает размер файла образа вследствие того, что для всех случаев вхождения определенного файла в образе сохраняется только одна физическая копия этого файла. Аппаратная независимость формата WIM позволяет обойтись только по одному двоичному файлу образа для всех 32- и 64-разрядных архитектур. Windows 8 RT поставляется отдельным образом.

Установку Windows 8 можно выполнять автоматически или интерактивно. Существует несколько способов автоматизации установки Windows, включая следующие.

- **Использование файла ответов.** Одним из способов автоматической установки Windows 8 является использование одноформатного стандартного файла ответов. Этот файл, называющийся Unattend.xml, написан на языке XML, что облегчает его обработку стандартными средствами. Автоматическая установка осуществляется, исполняя программу установки Setup, используя заранее созданный специализированный файл ответов. Программа установки выполняет установку с сетевого диска или носителя, следуя инструкциям, указанным в файле ответов.
- **Использование утилиты Sysprep.** На компьютере, используемом в качестве шаблона для развертывания, запускается утилита Sysprep и создается образ конфигурации этого компьютера. Исполняемый файл утилиты, Sysprep.exe, находится в папке *%SystemRoot%*\System32\Sysprep.

  Совместно с утилитой Sysprep применяются диспетчер WSIM[1] и утилита ImageX, которые предоставляются в пакете WAIK[2].

  Диспетчер WSIM используется для создания файлов ответа для автоматической установки Windows 8, а утилита ImageX — для создания и работы с образами дисков.

[1] Windows System Image Manager — диспетчер образов системы Windows.

[2] Windows Automated Installation Kit — пакет автоматической установки Windows.

Использование утилитой ImageX образов дисков формата WIM и модульная организация Windows 8 позволяют значительно сократить количество требуемых образов дисков. В частности, нет необходимости в содержании нескольких аппаратно-зависимых или языково-зависимых образов дисков, а обычно достаточно только одного образа диска для каждой процессорной архитектуры, применяемой в организации. Для индивидуализации отдельных установок операционной системы применяются соответствующие сценарии установки.

Применение формата WIM также предоставляет другие преимущества над ранее используемыми форматами образов дисков. В частности, этот формат позволяет автономно модифицировать и содержать образы дисков, что означает, что можно добавлять или удалять компоненты и драйверы или применять обновления, используя уже существующий образ, не требуя создания нового. Для этого образ диска подключается в файловой системе в виде папки, после чего содержащиеся в нем файлы можно редактировать, как требуется, используя для этого стандартные средства для работы с файловой системой, например Проводник Windows.

Средства WSIM, ImageX и Sysprep предоставляют несколько разных способов автоматизации развертывания, базовая процедура которого выглядит так:

1. На специально выделенном компьютере, не используемом для обычной работы, устанавливается и конфигурируется операционная система Windows 8, после чего устанавливаются и конфигурируются необходимые компоненты Windows и приложения.
2. С помощью утилиты Sysprep диск компьютера подготавливается к созданию образа. Утилита Sysprep удаляет информацию, уникальную для данного компьютера, и обозначает его в качестве основного компьютера развертывания. По завершению этого процесса компьютер больше не содержит информации, позволяющей ему выполнять вход и работать в домене или рабочей группе.
3. Выполняется команда `ImageX /capture`, в результате чего создается образ диска, который сохраняется на носителе или сетевом диске. Созданный образ можно впоследствии с помощью команды `ImageX /mountrw` подключать в виде папки в файловую систему в режиме чтения и записи и выполнять его необходимое редактирование. По завершению редактирования образ отключается посредством команды `ImageX /unmount`.

   Образы также можно подключать посредством команды `dism /mount-wim`, а отключать с помощью команды `dism /unmount-wim`. Утилита DISM предоставляет функциональность для манипулирования образами. С ее помощью можно устанавливать ключи продукта, выполнять обновления, добавлять и удалять драйверы, добавлять информацию о языках и локальных стандартах, добавлять и удалять пакеты и функциональности и выполнять чистку образов.
4. С помощью диспетчера WSIM создаются файлы ответов для автоматической установки Windows 8. Затем создаются сценарии развертывания для конфигурирования компьютера, исполнения программы установки с использованием файла ответов и заливки созданного образа диска.
5. Выполняется сценарий установки, который осуществляет конфигурирование компьютера и устанавливает на нем операционную систему.

Управление доступом и подготовка компьютеров

Как упоминалось ранее, для работы с образами можно использовать средство DISM. Предотвратить установку образов несанкционированными пользователями можно следующими способами:

- подготовить компьютеры и разрешить выполнять развертывание только на этих компьютерах;
- модифицировать настройки безопасности файлов образов, чтобы доступ к ним мог иметь только санкционированный персонал;
- установить требование получения разрешения администратора для установки на клиенте.

Подготовка компьютеров

Подготовка компьютеров состоит в создании для них учетных записей в службе каталогов Active Directory предварительно к их использованию. Подготовка компьютеров позволяет контролировать, какие клиенты и серверы могут взаимодействовать друг с другом. Прежде чем выполнять подготовку компьютеров, необходимо настроить службу развертывания WDS на принятие запросов только от известных компьютеров. Для этого нужно выполнить следующую процедуру:

1. В консоли средства развертывания WDS разверните узел **Серверы** (Servers). Нажмите и удерживайте или щелкните правой кнопкой мыши на требуемом сервере, а затем выберите команду **Свойства** (Properties).
2. На вкладке **Параметры PXE-ответа** (PXE Response Settings) нажмите или щелкните левой кнопкой мыши на опции **Отвечать только известным клиентским компьютерам** (Respond Only to Known Client Computers), после чего нажмите кнопку **OK**.

Чтобы подготовить компьютер, необходимо знать его идентификатор GUID[1]. Идентификатор GUID компьютера предоставляется активным сетевым адаптером компьютера в формате `{dddddddd-dddd-dddd-dddd-dddddddddddd}`, где `d` означает шестнадцатеричную цифру, например, `{AEFED345-BC13-22CD-ABCD-11BB11342112}`.

Требуемый идентификатор можно получить несколькими способами. Иногда производители размещают наклейку с идентификатором GUID на корпусе системного блока компьютера. Но в таком случае нужно иметь в виду, что этот идентификатор действительный только для сетевого адаптера, который был поставлен вместе с компьютером. Если заменить сетевой адаптер, то он будет иметь другой идентификатор GUID.

Идентификатор GUID установленного сетевого адаптера можно извлечь из микропрограммного обеспечения компьютера. Для этого нужно при работающем удаленном компьютере выполнить следующую команду Windows PowerShell:

```
get-wmiobject win32_networkadapter | format-list guid
```

Из возвращенных идентификаторов GUID нужно использовать тот, который связан с адаптером, подключенным к локальной сети.

Подготовка компьютеров к развертыванию осуществляется так:

1. В панели **Active Directory — Пользователи и компьютеры** (Active Directory Users and Computers) нажмите и удерживайте или щелкните правой кнопкой мыши на значке организационной единицы или контейнера, где будет выполняться подготовка компьютера, коснитесь или щелкните левой кнопкой мыши на опции **Создать** (New), а затем — опции **Компьютер** (Computer).
2. Введите имя компьютера, а затем нажмите кнопку **Далее** (Next). Либо коснитесь или нажмите пункт **Изменить** (Change), чтобы выбрать пользователя или группу, обладающего правами присоединить данный компьютер к домену, а затем коснитесь или нажмите кнопку **Далее**.

[1] Globally unique identifier — глобально уникальный идентификатор.

3. На странице **Управляемый** (Managed) установите опцию **Это управляемый компьютер** (This Is A Managed Computer), введите идентификатор GUID компьютера, а затем коснитесь или нажмите кнопку **Далее**. Информацию о том, как узнать идентификатор GUID компьютера, *см. ранее в этом разделе*.
4. На странице **Хост-сервер** (Host Server) выберите сервер службы WDS, который будет обслуживать данного клиента. Коснитесь или нажмите кнопку **Далее**, а затем кнопку **Готово** (Finish).

Модифицирование настроек безопасности файла образа

Чтобы изменить настройки безопасности файла образа, запустите Проводник Windows. Нажмите и удерживайте или щелкните правой кнопкой мыши на значке файла образа, а затем выберите команду **Свойства**. В диалоговом окне **Свойства** перейдите на вкладку **Безопасность** (Security) и установите на ней требуемые настройки параметров безопасности. Альтернативно параметры безопасности можно настроить для папки **Группа образов** (Image Group), в которой хранится файл образа. Эти настройки потом унаследуются образами, хранящимися в этой папке.

Требование разрешения администратора

Вместо подготовки компьютеров или применения безопасности файлов образов можно затребовать разрешения администратора для установки на компьютеры операционных систем с образов. Для этого применяется следующая процедура:

1. В консоли средства развертывания WDS разверните узел **Серверы** (Servers). Нажмите и удерживайте или щелкните правой кнопкой мыши по значку требуемого сервера, а затем коснитесь или щелкните мышью на команде **Свойства**.
2. На вкладке **Параметры PXE-ответа** (PXE Response Settings) выберите опцию **Отвечать всем (известным и неизвестным) клиентским компьютерам** (Respond to All (Known And Unknown) Client Computers).
3. Также выберите опцию **Если клиент неизвестен, уведомлять администратора и отвечать после утверждения** (For Unknown Clients, Notify Administrator And Respond After Approval), а затем коснитесь или нажмите кнопку **OK**.

Теперь загружаемые из сети компьютеры перейдут в режим ожидания. Прежде чем продолжить установку, администратор должен одобрить или отклонить запросы на установку.

Чтобы одобрить запрос на установку, выполните следующие шаги:

1. В консоли WDS выберите требуемый сервер. Щелкните мышью папку **Ожидающие устройства** (Pending Devices) сервера, чтобы отобразить список компьютеров, ожидающих одобрения установки операционной системы.
2. Щелкните правой кнопкой мыши на требуемом компьютере, а затем выберите команду **Утвердить** (Approve).

Чтобы отклонить запрос на установку, выполните следующие шаги:

1. В консоли WDS выберите требуемый сервер. Щелкните мышью папку **Ожидающие устройства** (Pending Devices) сервера, чтобы отобразить список компьютеров, ожидающих одобрения установки операционной системы.
2. Щелкните правой кнопкой мыши на требуемом компьютере, а затем выберите команду **Отказать** (Reject).

Индивидуализация образов Windows

Для подключения образов и их последующего редактирования можно использовать утилиту DISM. В табл. 1.2 приводится список и краткое описание основных команд этой утилиты. Все компоненты образа управляются посредством хранилища компонентов.

Таблица 1.2. *Основные команды утилиты DISM*

Тип команды/команда	Описание
Общие команды	
/Cleanup-Wim	Удаляет ресурсы, связанные с поврежденными образами Windows
/Commit-Wim	Сохраняет изменения на подключенном образе Windows
/Get-MountedWimInfo	Отображает информацию о подключенных образах Windows
/Get-WimInfo	Отображает информацию об образах, находящихся в файле образов Windows
/Image	Указывает путь к корневому каталогу автономного образа Windows
/Mount-Wim	Подключает образ из файла образов Windows
/Online	Обращается к работающей операционной системе
/Remount-Wim	Восстанавливает потерянный каталог подключения образа
/Unmount-Wim	Отключает подключенный образ Windows
Дополнительные опции	
/English	Отображает вывод командной строки на английском языке
/Format	Задает формат вывода отчетов
/LogLevel	Задает уровень вывода, отображаемого в журнале (1—4)
/LogPath	Задает путь файла журнала
/NoRestart	Запрещает автоматическую перезагрузку и вывод пользователю предложений выполнить перезагрузку
/Quiet	Скрывает все сведения, за исключением сообщений об ошибках
/ScratchDir	Задает путь к каталогу временных файлов
/SysDriveDir	Задает путь к файлу загрузчика системы, называющегося BootMgr
/WinDir	Задает путь к каталогу Windows

С подключенным образом можно работать, используя команды категории /Image утилиты DISM (табл. 1.3). Эти команды позволяют обновить образ к более высокой версии, добавлять и удалять драйверы устройств, задавать опции часовых поясов и языков пользовательского интерфейса, отображать исправления и установленные приложения MSI[1], добавлять и удалять пакеты, и многое другое.

[1] Message signaled interrupt — прерывание, инициируемое сообщением.

Таблица 1.3. *Основные команды для работы с подключенными и автономными образами*

Команда	Описание
/Add-Driver	Добавляет пакет драйверов к автономному образу
/Add-Package	Добавляет пакет к образу
/Apply-Unattend	Применяет к образу файл AnswerFile.xml
/Check-AppPatch	Отображает информацию о возможности применения нескольких исправлений настройки (MSP-файлов) к подключенному образу
/Cleanup-Image	Выполняет на образе операции очистки и восстановления
/Disable-Feature	Отключает в образе указанную функциональность
/Enable-Feature	Включает в образе указанную функциональность
/Gen-LangIni	Создает новый файл Lang.ini
/Get-AppInfo	Отображает информацию об указанном приложении MSI
/Get-AppPatches	Отображает информацию обо всех примененных MSP-файлах для всех приложений, установленных в автономном образе
/Get-AppPatchInfo	Отображает информацию обо всех установленных MSP-исправлениях
/Get-Apps	Отображает информацию обо всех установленных приложениях MSI
/Get-CurrentEdition	Отображает версию указанного образа
/Get-DriverInfo	Отображает информацию об указанном драйвере в автономном образе или работающей операционной системе
/Get-Drivers	Отображает информацию обо всех драйверах в автономном образе или работающей операционной системе
/Get-FeatureInfo	Отображает информацию об указанной функциональности
/Get-Features	Отображает информацию обо всех функциональностях в пакете
/Get-Intl	Отображает информацию о региональных стандартах и языках
/Get-PackageInfo	Отображает информацию об указанном пакете
/Get-Packages	Отображает информацию обо всех пакетах в образе
/Get-TargetEditions	Отображает список версий Windows, к которым можно обновить образ
/Remove-Driver	Удаляет пакет драйверов с автономного образа
/Remove-Package	Удаляет пакеты с образа
/Set-AllIntl	Устанавливает все региональные стандарты в подключенном автономном образе
/Set-Edition	Обновляет образ Windows к высшей версии
/Set-InputLocale	Задает языки ввода и раскладки клавиатуры, используемые в подключенном автономном образе
/Set-LayeredDriver	Задает уровневый драйвер клавиатуры
/Set-ProductKey	Записывает ключ продукта в автономный образ
/Set-SetupUILang	Задает язык по умолчанию, применяемый в программе установки

Таблица 1.3 *(окончание)*

Команда	Описание
/Set-SKUIntlDefaults	Присваивает всем региональным параметрам значения по умолчанию для указанного языка в подключенном автономном образе
/Set-SysLocale	Задает язык для программ, которые не поддерживают Unicode (также называется *языком системы*) и параметры шрифтов в подключенном автономном образе
/Set-TimeZone	Задает часовой пояс по умолчанию в подключенном автономном образе
/Set-UILang	Задает язык по умолчанию интерфейса пользователя для использования в подключенном автономном образе
/Set-UILangFallback	Задает резервный язык по умолчанию интерфейса пользователя для использования в подключенном автономном образе
/Set-UserLocale	Задает региональные параметры пользователя в подключенном автономном образе

Средство DISM предоставляет возможности для работы с WIM-образами. Для подключения образа применяется следующий синтаксис:

```
dism /mount-wim /wimfile:Path /index:Index /mountdir:MountPath
```

Здесь параметр *Path* указывает полный путь к образу WIM, параметр *Index* — позицию образа в файле WIM-образа, а параметр *MountPath* — папку, к которой подключается образ. Далее показан пример команды `dism` для подключения образа:

```
dism /mount-wim /wimfile:c:\winpe_x86\iso\sources\boot.wim /index:1
     /mountdir:C:\Win8
```

В подключенный к папке образ можно вносить требуемые изменения. Внесенные в образ изменения можно сохранить в любое время с помощью команды `dism /commit-wim`, как показано в примере ниже:

```
dism /commit-wim /mountdir:C:\Win8
```

В данном случае сохраняются изменения в образе WIM, подключенном к папке C:\Win8.

Для отключения подключенного образа применяется команда `dism /unmount-wim`:

```
dism /unmount-wim /mountdir:C:\Win8
```

В этом примере образ WIM, подключенный к папке C:\Win8, отключается от этой папки. Прежде чем отключать образ от папки, следует сохранить все внесенные в него изменения. Для этого к предыдущей команде нужно добавить параметр `/commit`, чтобы сохранить изменения (или `/discard`, чтобы не сохранять их). Сохраняются (или отменяются) только изменения, которые не были сохранены ранее.

Установка Windows 8

Основными редакциями Windows, предназначенными для использования в доменах Active Directory, являются Windows 8 Pro и Windows 8 Enterprise. При установке Windows 8 на компьютер, на котором уже установлена операционная система, можно выполнить новую установку (опция **Выборочная: только установка Windows**) или обновление существующей операционной системы (опция **Обновление: установка Windows с сохранением фай-**

лов, параметров и приложений). Основная разница между этими двумя типами установки заключается в следующем.

- **Новая установка.** При новой установке программа установки Windows полностью заменяет старую операционную систему; при этом также не сохраняются ни установленные приложения, ни пользовательские настройки. Новую установку следует выполнять в тех случаях, когда операционную систему нельзя обновить, на компьютере устанавливается несколько операционных систем, требуется стандартная конфигурация или же если на компьютере нет установленной операционной системы.
- **Обновление.** При обновлении сохраняются все установленные приложения и их настройки, все учетные записи, файлы и настройки пользователя; настройку основных параметров системы выполнять не требуется. Обновление следует выполнять в тех случаях, когда на компьютере установлена операционная система, поддерживающая обновление до Windows 8, и нужно минимизировать нарушения в работе компьютера, сохранив существующие настройки, пользовательскую информацию и конфигурационные настройки приложений.

Способ осуществления обновления зависит от обновляемой операционной системы. При обновлении Windows 7 программа установки Windows выполняет обновление на месте (in-place upgrade)[1], чем обеспечивается выполнение обновления, как описано ранее. В случае Windows Vista и Windows XP обновление выполняется по-другому. В частности, при обновлении Windows Vista сохраняются учетные записи пользователей, файлы и настройки пользователей, а также основные конфигурационные параметры системы, но не приложения и их настройки. А при обновлении Windows XP также сохраняются учетные записи пользователей, файлы и настройки пользователей, но не основные конфигурационные параметры системы и не приложения и их настройки.

Подготовка к установке Windows 8

Для установки Windows 8 компьютер можно загрузить с установочного носителя, запустить программу установки в текущей установленной операционной системе Windows, выполнить установку с командной строки или воспользоваться одной из возможностей автоматической установки.

Существуют два основных подхода к установке Windows 8 — интерактивный и автоматический. Интерактивная установка, при которой пользователь проходит по всем этапам установки, вводя при этом разные данные, является типом установки, которую большинство пользователей считают стандартной. Этот тип установки можно выполнить с дистрибутивного носителя, загрузив компьютер с этого носителя или запустив программу установки Windows с командной строки.

При загрузке Windows 8 с DVD, приобретенного в магазине, по умолчанию применяется интерактивная установка, в процессе которой у пользователя запрашиваются разные данные для настройки параметров системы.

Автоматическая установка достигается за счет предварительного предоставления администратором информации, которая при интерактивной установке вводится пользователем. Самая простая автоматическая установка осуществляется с использованием только файлов ответов. Файл ответов содержит всю или часть конфигурационной информации, которая

[1] Обновление, которое выполняется на том же самом аппаратном обеспечении, что и установленная предшествующая версия.

обычно запрашивается в процессе интерактивной установки. Файл ответов для автоматической установки можно создать с помощью диспетчера WSIM, который входит в состав комплекта Windows ADK. Для более продвинутой автоматической установки применяется служба развертывания WDS.

Для установки Windows 8 применяется стандартная программа установки — Setup.exe. Эту программу можно запустить из операционной системы Windows, установленной на компьютере в настоящее время, чтобы выполнить обновление. Можно также загрузить компьютер с установочного носителя и выполнить новую установку Windows 8. При работе с Windows 8 на системах с архитектурой *x*86 следует знать о существовании специальных типов секций диска, используемых операционной системой.

- **Активный** (Active). Активный раздел или том — это раздел диска, используемый для системного кэша и файлов запуска. Активный раздел может отображаться для некоторых съемных носителей.
- **Загрузочный** (Boot). Загрузочный раздел или том содержит операционную систему и ее вспомогательные файлы. Загрузочный раздел может быть объединен с системным разделом *(см. следующий пункт)*.
- **Система** (System). Системный раздел или том содержит файлы, специфичные для аппаратного обеспечения данного компьютера, необходимые для загрузки операционной системы. Будучи частью конфигурации программного обеспечения, системный раздел не может располагаться на динамическом диске.

Раздел и том означают практически одно и то же понятие. Разные термины применяются по той причине, что разделы создаются на базовых дисках, а тома — на динамических дисках. На компьютере архитектуры *x*86 раздел можно пометить активным с помощью оснастки **Управление дисками** (Disk Management), доступной в утилите **Управление компьютером** (Computer Management).

Хотя активный, загрузочный и системный разделы могут быть объединены, тем не менее, наличие каждого из них является обязательным. При установке Windows 8 программа установки оценивает все доступные дисковые ресурсы. Обычно загрузочные и системные файлы Windows 8 помещаются на один и тот же привод и раздел, который помечается как активный. Преимуществом такой конфигурации является то, что она не требует нескольких приводов для операционной системы, а дополнительный привод можно использовать для зеркалирования разделов операционной системы.

Установка Windows 8 на компьютеры с микропрограммным интерфейсом EFI отличается в нескольких отношениях. Процесс установки начинается с загрузки интерфейсом EFI микропрограммного меню загрузки. Обычно диски компьютеров с интерфейсом EFI имеют структуру разделов типа GPT[1], которая значительно отличается от структуры разделов MBR 32-разрядных платформ.

Диски типа GPT имеют два обязательных раздела и один или больше (до 128) необязательных раздела (для нужд производителя или данных):

- системный раздел EFI (ESP, EFI system partition);
- резервный раздел Microsoft (MSR, Microsoft reserved partition);
- по крайней мере, один раздел для данных.

Загрузочное меню EFI предоставляет набор опций, одной из которых является оболочка EFI. Оболочка EFI предоставляет рабочую среду, поддерживающую файловые системы

[1] GUID partition table — таблица разделов GUID.

FAT и FAT32, а также команды конфигурирования и управления файлами. Для просмотра списка разделов компьютера архитектуры EFI применяется команда `Map`. В выводе результатов исполнения этой команды ключевое слово `blk` обозначает блоки разделов, а `fs#` — читаемые файловые системы. Для перехода в определенный раздел нужно ввести номер блока этого раздела с двоеточием в конце. Для просмотра содержимого раздела применяется стандартная команда `dir`. Для настройки меню загрузки в интерфейсе EFI предоставляется диспетчер обслуживания загрузки (Boot maintenance manager).

При установке Windows 8 программа установки автоматически создает раздел со средой восстановления Windows (WRE, Windows Recovery Environment) и устанавливает в нем дополнительные компоненты, которые можно использовать для поиска неполадок в этом разделе и его восстановления. Таким образом, на компьютерах под управлением Windows 8 всегда в наличии средства для восстановления операционной системы. Дополнительную информацию по этому вопросу *см. в разд. "Восстановление после сбоя запуска" главы 10*.

Администратор может пользоваться этими средствами для восстановления компьютеров. Также, если удаленный пользователь не может запустить Windows на своем компьютере, администратор может проинструктировать его, как запустить среду WRE и выполнить восстановление компьютера. Для этого пользователю нужно будет открыть меню **Дополнительные параметры восстановления** (Advanced Repair Options), как рассматривается в *разд. "Восстановление после сбоя запуска" главы 10*.

Выполнение установки Windows 8

Прежде чем приступать к установке Windows 8 на компьютер, нужно определить, отвечает ли аппаратное обеспечение данного компьютера требованиям этой операционной системы касательно объема оперативной памяти, мощности процессора и графических возможностей. Корпорация Microsoft предоставляет как минимальные, так и рекомендуемые требования. Требования для памяти и графического адаптера измеряются в мегабайтах и гигабайтах, а для процессора — в гигагерцах.

Для установки Windows 8 требуется следующее:

- 32-разрядный (*x*86) или 64-разрядный (*x*64) процессор с рабочей частотой 1 ГГц или выше;
- минимум 1 Гбайт оперативной памяти (RAM) для 32-разрядной версии или 2 Гбайт для 64-разрядной версии;
- графический адаптер, поддерживающий DirectX 9 с драйвером модели WDDM[1] 1.0 или более поздней версии;
- для поддержки сенсорного пользовательского интерфейса требуется планшетный компьютер или экран с мультисенсорными возможностями.

> ***Примечание***
>
> Для установки Windows 8 корпорация Microsoft рекомендует наличие, по крайней мере, 16 Гбайт свободного дискового пространства для 32-разрядной версии и 20 Гбайт — для 64-разрядной. Разнообразные дополнительные функциональности Windows 8, такие как точки восстановления, которые сохраняют предшествующие версии измененных файлов и папок, могут очень быстро и очень значительно повысить требования к свободному дисковому пространству. Для оптимальной работы жесткого диска необходимо, чтобы, по крайней мере, 15% от его полного объема было свободно в любое время, а также, чтобы на нем имелось достаточно места для файла подкачки, размер которого обычно должен быть вдвое больше объема оперативной памяти. Кроме

[1] Windows Display Driver Model — модель драйверов дисплея Windows.

этого, при выполнении обновления на месте папки и файлы предыдущей операционной системы сохраняются на диске в папке Windows.old, что также следует учитывать при определении требуемого свободного дискового пространства.

Любой компьютер, технические характеристики которого отвечают или превосходят эти требования, может работать с операционной системой Windows 8. *Новую установку* Windows 8 можно выполнить, следуя нижеприведенной процедуре:

1. Включите компьютер и вставьте дистрибутивный диск с Windows 8 в привод DVD-ROM компьютера. Нажмите любую клавишу, чтобы загрузить компьютер с DVD-диска, при выводе запроса. (Если запрос для загрузки с DVD не выводится, нужно будет изменить параметры загрузки в микропрограммном обеспечении компьютера.)
2. Далее выберите устанавливаемый язык, формат времени и денежных единиц и раскладку клавиатуры, после чего нажмите кнопку **Далее** (Next). На следующем экране нажмите кнопку **Установить** (Install Now).
3. В случае коробочной версии Windows обычно нужно ввести ключ продукта. Если выводится окно для ввода ключа продукта, введите его в соответствующее поле. При установке на устройство без физической клавиатуры, коснитесь значка клавиатуры справа от поля для ввода ключа продукта и используйте открывшуюся экранную клавиатуру. После ввода ключа продукта коснитесь или нажмите кнопку **Далее**.

   Примечание

   Если программа установки не принимает введенный ключ продукта, проверьте правильность введенных букв и цифр. Дефисы между группами знаков вводить не нужно, т. к. они вставляются автоматически. Иногда легче ввести полностью ключ продукта повторно, чем искать неправильно введенный знак.

4. Далее выводится окно с условиями лицензии. Если вы принимаете эти условия (что является обязательным для продолжения установки), установите флажок **Я принимаю условия лицензии** (I accept the license terms), а затем нажмите кнопку **Далее**.
5. Появится окно выбора типа установки: обновление (опция **Обновление:...**) или новая (опция **Выборочная:...**). Выберите опцию **Выборочная: только установка Windows (для опытных пользователей)** (Custom: Install Windows Only (Advanced)).
6. В следующем окне, **Выберите раздел для установки Windows** (Where do you want to install Windows), выберите диск, на который нужно установить операционную систему, а затем нажмите кнопку **Далее**.

   Совет

   При установке в окне **Выберите раздел для установки Windows** можно получить доступ к командной строке, нажав комбинацию клавиш <Shift>+<F10>. Это откроет среду MinWinPC, используемую программой установки для установки операционной системы, которая предоставляет многие средства командной строки, доступные в полной установке Windows 8.

7. Если выбранный раздел содержит предыдущую установку Windows, выводится сообщение, что старые параметры пользователей и приложений будут помещены в папку Windows.old, и их можно будет скопировать в новую установку. Нажмите кнопку **OK**.
8. Программа установки начнет выполнять установку Windows 8. Во время этого процесса образ диска Windows 8 копируется в указанный раздел, после чего выполняется его распаковка. Затем программа инсталляции устанавливает функциональности на основе конфигурации компьютера и обнаруженного аппаратного обеспечения. По завершению установки компонентов выполняется перезапуск компьютера, загружается операционная система и выполняется подготовка к первому использованию. После завершения подготовки компьютер снова перезапускается.

9. На странице **Персонализация** (Personalize) выберите фон для окна **Пуск** и рабочего стола. Введите имя компьютера, а затем нажмите кнопку **Далее**.
10. В следующем окне выберите страну или регион, формат времени и денежных единиц, раскладку клавиатуры, затем коснитесь или нажмите кнопку **Далее**.
11. При наличии беспроводных подключений к сети нужно выбрать, какое из них использовать. После выбора подключения и нажатия кнопки **Подключиться** (Connect) предлагается ввести пароль для подключения к беспроводной сети. После ввода пароля снова нужно нажать кнопку **Подключиться**. При наличии проводного подключения к Интернету выполнять беспроводное подключение не требуется.
12. На странице **Параметры** (Settings) можно выбрать опцию **Использовать стандартные параметры** (Use Express Settings), чтобы принять стандартные параметры, или же нажать кнопку **Настроить** (Customize), чтобы выполнять настройку параметров. В первом случае конфигурационным параметрам компьютера присваиваются стандартные значения:

    - включить общий доступ и подключение к устройствам сети, что подходит для домашних и рабочих сетей, но не обязательно для публичных сетей;
    - автоматически устанавливать важные и рекомендуемые обновления, а также обновления для устройств;
    - защитить компьютер от небезопасного содержания, файлов и веб-сайтов, включив фильтр SmartScreen для Internet Explorer и Windows;
    - использовать службу отчетов об ошибках Windows (Windows Error Reporting), чтобы проверить наличие решений проблем;
    - использовать списки совместимости Internet Explorer для решения проблем совместимости веб-сайтов;
    - позволить приложениям использовать ваше имя и аватар;
    - включить службу определения местоположения (Windows Location Platform), чтобы приложения могли запрашивать у пользователей их местонахождение.

13. Если компьютер подключен к Интернету, на следующей странице после принятия стандартных параметров, **Вход в систему** (Sign in to your PC), можно задать учетную запись для входа в систему — учетную запись Microsoft или же локальную учетную запись. Если подключение к Интернету отсутствует, можно выбрать только локальную учетную запись. Так как для компьютера в домене или рабочей группе обычно используется локальная учетная запись, выберите опцию **Вход без учетной записи Microsoft** (Sign in without a Microsoft account), нажмите кнопку **Далее** и в следующем окне подтвердите выбор, нажав кнопку **Локальная учетная запись** (Local Account). На следующей странице окна **Вход в систему** введите в соответствующие поля имя пользователя, пароль и подтверждение и подсказку для пароля, а затем нажмите кнопку **Готово** (Finish).

    Примечание

    Учетные записи Microsoft и подробности об их создании и использовании рассматриваются в *главе 7*.

14. Windows 8 начнет выполнение настройки параметров, по завершению которого будет отображен экран **Пуск** и компьютер будет готов к работе.

Обновление старой операционной системы компьютера к Windows 8 можно осуществить, выполнив следующую процедуру:

1. Включите компьютер и войдите в систему под учетной записью, обладающей правами администратора. Вставьте дистрибутивный диск с Windows 8 в привод DVD-ROM компьютера. Запустится программа установки Windows 8. Если программа установки Windows 8 не запустилась, откройте DVD-диск в Проводнике Windows и запустите программу установки вручную, дважды коснувшись или щелкнув на ее исполняемом файле Setup.exe.

   Примечание

   При установке доступен только язык текущей операционной системы. Поэтому, если раскладка клавиатуры и язык устанавливаемой версии Windows 8 отличаются от языка текущей операционной системы, при вводе могут отображаться непонятные символы, так называемые "кракозябры".

2. Программа установки сначала скопирует временные файлы, а затем приступит к собственно установке. Если компьютер подключен к Интернету, вы должны будете выбрать: получить ли и установить необходимые обновления или отказаться от них. Для этого нужно установить один из двух переключателей: **Установить обновления из Интернета** (Go online to install updates) или **Нет, спасибо** (No, thanks). Сделав требуемый выбор, коснитесь или нажмите кнопку **Далее**.

   Совет

   Установка обновлений при установке операционной системы не является обязательной. Нужные обновления можно установить позже с помощью Центра обновлений Windows. Установка обновлений при установке операционной системы может быть оправданной тем, что таким образом обеспечивается полная готовность компьютера к работе после завершения установки операционной системы.

3. В случае "коробочной" версии Windows обычно нужно ввести ключ продукта. Если выводится окно для ввода ключа продукта, введите его в соответствующее поле. При установке на устройство без физической клавиатуры коснитесь значка клавиатуры и используйте открывшуюся экранную клавиатура. По умолчанию Windows будет автоматически активирована при следующем подключении к Интернету. Коснитесь или нажмите кнопку **Далее**.

   Примечание

   Если программа установки не принимает введенный ключ продукта, проверьте правильность введенных букв и цифр. Дефисы между группами знаков вводить не нужно, т. к. они вставляются автоматически. Иногда легче ввести полностью ключ продукта повторно, чем искать неправильно введенный знак.

4. Далее выводится окно с условиями лицензии. Если вы принимаете эти условия (что является обязательным для продолжения установки), установите флажок **Я принимаю условия лицензии** (I accept the license terms), а затем нажмите кнопку **Принять** (Accept).
5. Содержимое следующего окна, **Выберите, что вы хотите сохранить** (Choose what to keep), зависит от версии Windows, установленной на компьютере в настоящее время. Доступными могут быть следующие опции.

   - **Параметры Windows** (Windows Settings). Если такая опция доступна и выбрана, программа установки попытается сохранить основные параметры системы, включая параметры фона рабочего стола, экрана, список закладок веб-сайтов, журнал посещения веб-сайтов, а также настройки Центра специальных возможностей (Ease of Access). Не все параметры текущей операционной системы могут быть сохранены для использования в Windows 8.

- **Личные файлы** (Personal files). Если такая опция доступна и установлена, программа установки сохраняет личные файлы в папке Пользователи. Сохраняются и будут доступными в Windows 8 личные файлы, находящиеся в папках Мои документы, Моя музыка, Мои рисунки, Мои видео и в других личных папках.
- **Приложения** (Apps). Если эта опция доступна и выбрана, программа установки Windows 8 сохранит и сделает доступными после обновления параметры приложений. Сами программы нужно будет переустановить.
- **Ничего** (Nothing). Если выбрать эту опцию, программа установки сохранит папки и файлы предыдущей операционной системы в папке Windows.old. От предыдущей операционной системы не останется ничего больше.

ВНИМАНИЕ!

При обновлении системы, вход в которую осуществляется посредством считывания отпечатка пальца или другими биометрическими средствами, нужно будет записать пароль для входа в систему, т. к. для первого входа в Windows 8 потребуется ввести имя пользователя и пароль.

6. Коснитесь или нажмите кнопку **Далее**, а затем кнопку **Установить**. Далее выполнятся шаги 8—14 процедуры для новой установки.

При установке Windows 8 могут возникнуть разные проблемы. Далее приводятся наиболее распространенные из них и возможные способы их решения.

- **Невозможно загрузиться с установочного носителя Windows 8.** Хотя большинство компьютеров могут загружаться с DVD-диска, иногда эта возможность может быть отключена в микропрограммном обеспечении. Чтобы исправить эту проблему, войдите в меню микропрограммного обеспечения[1] и выставьте CD/DVD-привод первым в списке устройств загрузки. Дополнительную информацию по этому вопросу *см. в главе 4*.
- **Программа установки не обнаруживает жесткий диск.** Хотя установочный носитель Windows 8 содержит драйверы для большинства дисковых контроллеров, вы можете оказаться несчастным владельцем контроллера диска, для которого драйвера на установочном диске нет. В таком случае, на странице **Выберите раздел для установки Windows** нужно вставить в CD/DVD-привод диск с драйверами для вашего привода и выбрать опцию **Загрузить драйверы** (Load Drivers). Если драйвер находится на внутреннем жестком диске, нажмите комбинацию клавиш <Shift>+<F10>, чтобы получить доступ к командной строке, а затем скопируйте файлы драйвера на флеш-накопитель или иной съемный носитель, после чего опять выберите опцию **Загрузить драйверы**, чтобы загрузить драйверы со съемного носителя.
- **Жесткий диск не сконфигурирован должным образом.** На странице **Выберите раздел для установки Windows** нажмите **Настройка диска** (Drive Options). Откроется диалоговое окно с опциями для создания, удаления и форматирования разделов. Если необходимо расширить или уменьшить раздел (даже при обновлении), нажмите комбинацию клавиш <Shift>+<F10>, чтобы открыть консоль командной строки, а затем запустите утилиту Diskpart для работы с разделами. Чтобы расширить или уменьшить разделы, удалять их не требуется. С помощью утилиты Diskpart можно также изменить тип диска и раздела. Дополнительную информацию по работе с утилитой Diskpart *см. в гла-*

[1] Как правило, для этого при запуске компьютера нужно нажать клавишу <Delete> или <F2> или, довольно редко, какую-либо другую клавишу. Обычно, какую клавишу следует нажать, чтобы войти в меню интерфейса микропрограммного обеспечения (то, что раньше называлось BIOS), выводится на начальном этапе запуска компьютера.

вах 10—12 книги "Windows Command-Line Administrator's Pocket Consultant, Second Edition" (Microsoft Press, 2008 г.)[1].

Работа в Windows 8

По умолчанию в Windows 8 данные профилей пользователей хранятся в папке *%SystemDrive%\Users\%UserName%*. Для каждого пользователя, который входит в систему, в папке профилей пользователей создается отдельная папка профиля этого пользователя, название которой соответствует имени данного пользователя. Эта папка содержит дополнительные папки, в которых хранятся специфические типы данных и файлов данного пользователя:

- AppData (скрытая папка) — данные приложений, специфичные для конкретного пользователя;
- Контакты (Contacts) — контакты и контактные группы;
- Рабочий стол (Desktop) — рабочий стол пользователя;
- Загрузки (Downloads) — программы и данные, загруженные из Интернета;
- Избранное (Favorites) — закладки веб-страниц;
- Ссылки (Links) — ссылки на веб-страницы;
- Мои документы (My Documents) — файлы документов пользователя;
- Моя музыка (My Music) — музыкальные файлы пользователя;
- Изображения (My pictures) — файлы рисунков пользователя;
- Мои видео (My videos) — видеофайлы пользователя;
- Сохраненные игры (Saved games) — данные сохраненных игр пользователя;
- Поиски (Searches) — сохраненные результаты поисков.

> ***ПРИМЕЧАНИЕ***
>
> Параметры *%SystemDrive%* и *%UserName%* обозначают переменные среды `SystemDrive` и `UserName` соответственно. В операционной системе Windows используется большое число переменных среды, которые содержат значения, специфичные для пользователей и системы. В этой книге для обозначения переменных среды применяется следующий синтаксис: *%ИмяПеременной%*. При обновлении ОС до Windows 8 личная папка пользователя может также содержать символьные ссылки (которые выглядят наподобие ярлыков) к папкам и настройкам предшествующей операционной системы. Символьная ссылка — это указатель на файл или папку, который часто создается для обеспечения обратной совместимости с приложениями, осуществляющими поиск перемещенной в другое место папки или файла. Символьные ссылки можно создавать самостоятельно с помощью утилиты командной строки Mklink. Чтобы получить список опций этой утилиты, введите команду `mklink /?`.

Кроме личных папок, в Windows 8 используются личные библиотеки. *Библиотека* — это просто коллекция файлов и папок, собранных в одну группу и представляемых посредством общего вида. Стандартные библиотеки включают следующие:

- **Документы** (Documents). Содержит папки Мои документы пользователя и папку Общие документы (Public Documents).

[1] Или *главы 8—10* книги: Станек У. Р. Командная строка Microsoft Windows. Справочник администратора. — СПб.: Русская редакция, 2009.

- **Музыка** (Music). Содержит данные папки Моя Музыка пользователя и папки Общая Музыка.
- **Изображения** (Pictures). Содержит данные папки Изображения пользователя и папки Общие Изображения.
- **Видео.** Содержит данные папки Мои видео пользователя и папки Общие видео.

Новую библиотеку для представления разных коллекций данных можно создать, щелкнув правой кнопкой мыши на узле **Библиотеки** и выбрав в контекстном меню пункт **Создать** (New), а затем **Библиотека** (Library).

> ***Важно!***
>
> При работе с библиотеками важно помнить, что они являются только представлениями наборов данных. Windows 8 создает объединенные представления файлов и папок, которые добавляются в библиотеки. Библиотеки не содержат никаких настоящих данных, и любое действие, предпринимаемое на файле или папке в библиотеке, в действительности выполняется на исходном файле или папке.

В Windows 8 предоставляются темы для настройки внешнего вида меню, окон и рабочего стола. Задать тему можно в окне **Персонализация** (Personalization), которое открывается после выбора в Панели управления в группе **Оформление и персонализация** (Appearance and Personalization) ссылки **Изменение темы** (Change the theme). Темы стиля Aero добавляют к интерфейсу улучшенное визуальное оформление и расширенные динамические эффекты. Если нет желания разбираться во всех тонкостях оформления внешнего вида, можно выбрать одну из тем Windows по умолчанию.

Но важно отметить, что доступные усовершенствования интерфейса зависят от установленной версии Windows 8 и аппаратного обеспечения.

Работа с Центром поддержки и активирование Windows 8

При входе в систему в области извещений рабочего стола по умолчанию отображается значок сообщений Центра поддержки (Action Center), на котором отображен белый флаг. Центр поддержки представляет собой программу, которая отслеживает состояние важных областей безопасности и технического обслуживания компьютера. При изменении статуса отслеживаемых элементов Центр поддержки обновляет значок сообщений в соответствии с серьезностью уведомления. При касании или щелчку по этому значку Windows открывает диалоговое окно со списком кратких описаний каждого уведомления или элемента отслеживания, на который требуется обратить внимание. Щелчок по ссылке сообщения открывает диалоговое окно для решения данной проблемы. Щелчок по ссылке **Открыть центр поддержки** (Open Action Center) открывает главное окно Центра поддержки.

Если отображение значка Центра поддержки было отключено в настройках области уведомлений, открыть главное окно центра можно следующим образом:

1. В панели инструментов коснитесь или щелкните мышью по ссылке категории **Система и безопасность** (System and Security).
2. В открывшемся списке элементов этой категории коснитесь или щелкните мышью по ссылке **Центр поддержки**.

В главном окне Центра поддержки (рис. 1.1) предоставляется обзор состояния основных областей системы и перечисляются проблемы, требующие внимания.

После установки Windows 8 Центр поддержки может содержать сообщения в категории **Обслуживание** (Maintenance) о необходимости установки драйверов устройств. Касание

или щелчок мышью на таком сообщении запускает процесс установки соответствующего драйвера. Подробно работа с Центром поддержки рассматривается в *разд. "Использование автоматической справки и поддержки" главы 9*.

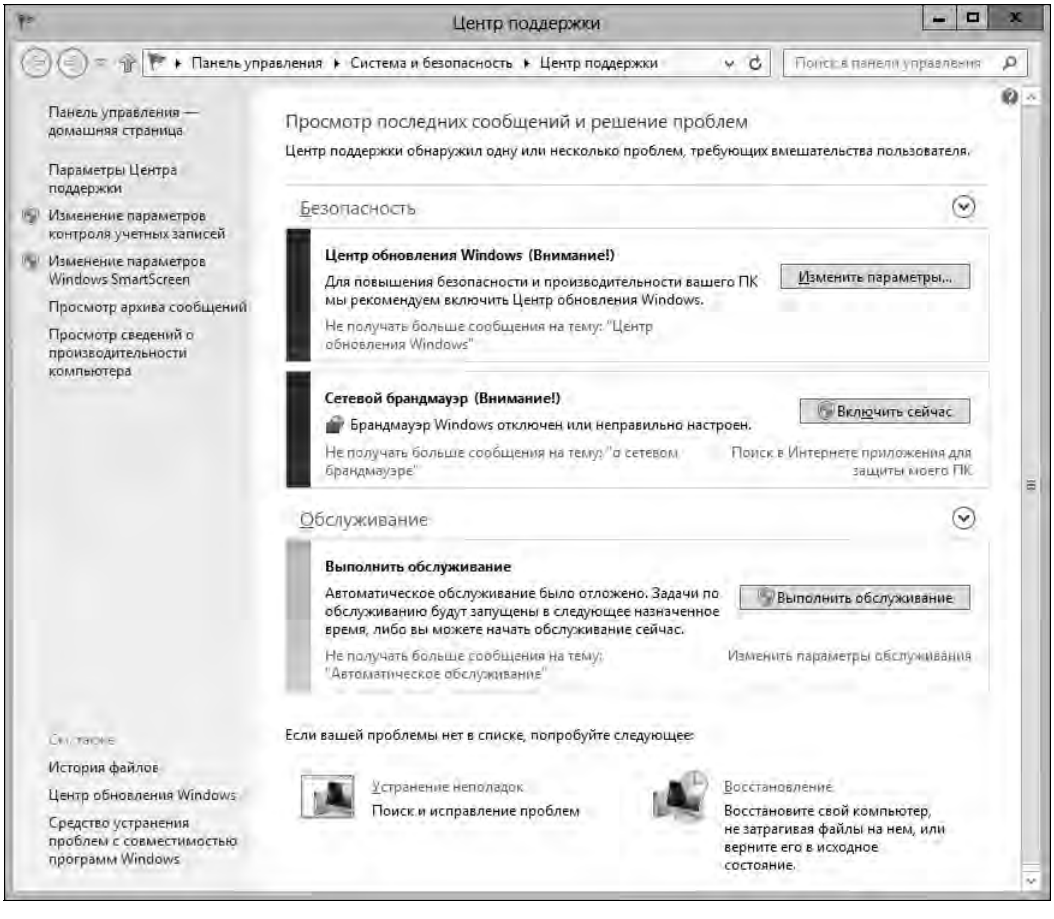


Рис. 1.1. Главное окно Центра поддержки

Редакции Windows 8 Pro и Enterprise поддерживают корпоративное (многопользовательское) лицензирование. Хотя редакции Windows 8 с корпоративным лицензированием не требуют ввода ключа продукта и активации, как ключ продукта, так и активация требуется для розничных версий этой операционной системы. Узнать, была ли выполнена активация Windows 8, можно в Панели управления. Для этого щелкните на ссылке категории **Система и безопасность** и в открывшемся списке элементов этой категории выберите ссылку **Система**. Далее, на открывшейся странице **Система** ознакомьтесь с содержимым раздела **Активация Windows** (Windows activation), где указывается, была ли активирована операционная система. Если активация Windows не была выполнена и компьютер подключен к Интернету, нажмите ссылку **Подробнее об активации Windows** (View details in Windows Activation), а затем коснитесь или щелкните мышью на опции **Активировать** (Ativate). Будет выполнена активация Windows, и новый статус активации отобразится в Центре поддержки.

Работа с Windows 8 в группах и доменах

Компьютеры под управлением Windows 8 могут быть членами домашних групп, рабочих групп или доменов. Термин *"домашняя группа"* (homegroup) означает слабосвязанное объединение компьютеров в домашней сети. Для доступа к данным компьютеров домашней группы применяется пароль, общий для всех пользователей домашней группы. Пароль домашней группы задается при ее создании и может быть изменен в любое время.

Под *рабочей группой* (workgroup) имеется в виду слабосвязанное объединение компьютеров, каждый из которых управляется отдельно.

Доменом (domain) называется набор компьютеров под единым управлением посредством контроллеров доменов[1] (domain controller).

Домашние группы доступны только в том случае, когда компьютер под управлением Windows 8 подключен к домашней сети. Рабочие группы доступны, когда компьютер подключен к рабочей сети. Управление сетевым окружением и сетевыми подключениями подробно рассматривается в *главе 15*.

Некоторые аспекты Windows 8 варьируются в зависимости от того, является ли компьютер членом домашней группы, рабочей группы или домена. Эти различия касательно контроля учетных записей пользователей, входа в систему, быстрого переключения пользователей и управления паролями рассматриваются в последующих разделах.

Контроль учетных записей пользователей в Windows 8

В домашней или рабочей группе компьютер под Windows 8 имеет только локальные учетные записи. В домене же такой компьютер имеет как локальные, так и доменные учетные записи. Операционная система Windows 8 поддерживает два основных типа локальных учетных записей пользователей.

- **Стандартная.** Пользователи стандартных учетных записей могут использовать большинство программного обеспечения и изменять системные параметры, которые не затрагивают других пользователей или безопасность компьютера.
- **Администратор.** Пользователи учетных записей с правами администратора имеют полный доступ к компьютеру и могут выполнять любые требуемые действия.

В Windows 8 добавлена специальная локальная учетная запись, называющаяся *учетной записью Microsoft* (Microsoft account), которой не было в предыдущих версиях Windows. Учетные записи Microsoft можно рассматривать как синхронизованные учетные записи. Более подробно этот тип учетной записи рассматривается в *разд. "Пользовательские и групповые учетные записи" главы 7*.

В Windows 8 контроль учетных записей пользователей применяется для повышения безопасности компьютерной системы посредством обеспечения настоящего разделения учетных записей обычных пользователей и пользователей с правами администратора. Вследствие применения в Windows 8 контроля учетных записей пользователей все приложения исполняются или с правами обычного пользователя, или с правами администратора. При попытке запуска любого приложения, требующего разрешений администратора, выводится соответствующее сообщение системы безопасности, независимо от типа запускающего его пользователя — обычного или администратора. Обстоятельства вывода сообщения системы безо-

[1] Компьютер на базе Windows Server, осуществляющий аутентификацию пользователей в сети, проведение политики безопасности и хранящий главную базу данных домена.

пасности зависят от параметров групповой политики *(см. разд. "Оптимизация контроля учетных записей пользователей и режима одобрения администратором" главы 7*) и от типа учетной записи, под которой выполнен вход в систему — стандартная или администратора.

Когда вход в систему выполнен под стандартной учетной записью, пользователь должен предоставить пароль учетной записи администратора (рис. 1.2).

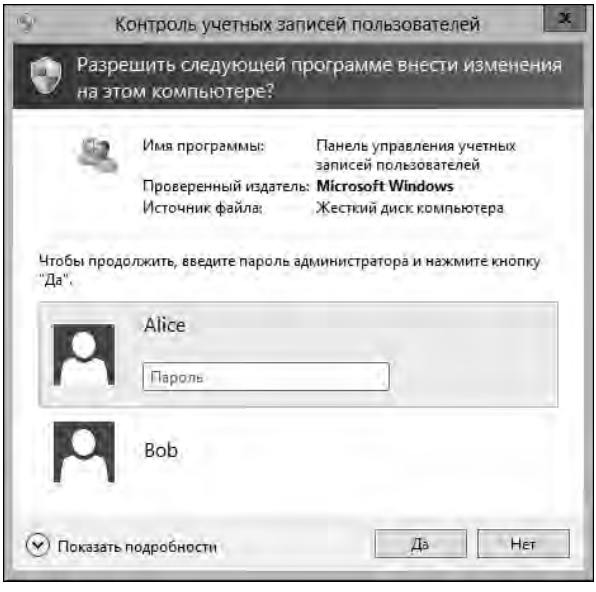


Рис. 1.2. Запрос ввода пароля администратора

В домашних и рабочих группах в этом окне приводится список имен всех локальных учетных записей администратора. Чтобы продолжить выполнение программы, нужно выбрать требуемую учетную запись администратора, ввести пароль для нее, а затем нажать кнопку **Да**.

В доменах диалоговое окно контроля учетных записей пользователей не содержит списка имен учетных записей администраторов, поэтому для продолжения выполнения программы нужно знать требуемое имя учетной записи администратора (и пароль для нее) в домене по умолчанию (домен входа в систему) или в доверяемом домене[1]. Когда появится диалоговое окно с запросом пароля администратора, введите в соответствующие поля имя учетной записи и пароль для нее, а затем нажмите кнопку **Да**. Если учетная запись находится в домене по умолчанию, имя домена указывать не требуется. Но если учетная запись находится в другом домене, нужно указать домен и имя учетной записи в формате *домен\имя_пользователя*, например *cpandl\Alice*.

Когда вход в систему выполнен с учетной записью администратора, выводится только запрос подтвердить намерение выполнения программы (рис. 1.3).

Чтобы разрешить продолжение выполнения программы, нажмите кнопку **Да**; в противном случае — кнопку **Нет**. Щелчок по кнопке **Показать подробности** (Show details) отображает полный путь к исполняемому файлу программы, а также другие сведения о ней.

[1] Trusted domain — домен, пользователям которого разрешено обращаться к ресурсам других, доверяющих доменов.

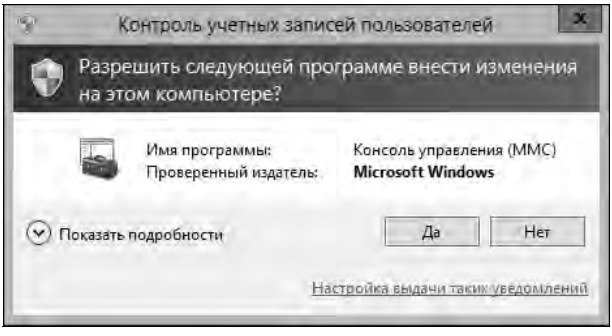


Рис. 1.3. Запрос подтвердить намерение выполнения программы

Возможность повышения прав позволяет стандартному пользовательскому приложению исполняться с правами администратора. Запуск приложения на исполнение с повышенными правами осуществляется таким способом:

1. Нажмите и удерживайте или щелкните правой кнопкой мыши на плитке или значке приложения, а затем в открывшейся панели внизу экрана коснитесь или щелкните мышью на значке **Запуск от имени администратора** (Run as administrator).
2. Когда откроется окно **Контроль учетных записей пользователей**, действуйте, как и в случае, когда нужно разрешить приложению исполняться с правами администратора.

> ***Примечание***
>
> Чтобы выполнять администрирование компьютера из командной строки, консоль командной строки нужно запустить с правами администратора. В противном случае, при попытке запустить утилиту, требующую прав администратора, будет выведено сообщение об ошибке.

Вход в систему, завершение работы и перезапуск Windows 8

После запуска компьютера и загрузки операционной системы выводится *экран блокировки* (lock screen), щелчок по которому открывает экран приветствия. Свойства экрана приветствия зависят от настроек групповой политики и членов домашней группы, рабочей группы или домена компьютера. Нужно иметь в виду следующее:

- в домашней или рабочей группе на экране приветствия выводится список имен учетных записей компьютера. Чтобы войти в систему под одной из этих учетных записей, коснитесь или щелкните по ней мышью и введите ее пароль;
- в доменах, на экране приветствия по умолчанию отображается имя пользователя, выполнившего последний предыдущий вход в систему. В систему можно войти с этой учетной записью, введя соответствующий пароль. Но вход в систему можно также выполнить и с другой учетной записью. Для этого нужно нажать кнопку **Сменить пользователя** (Switch User), выбрать одну из предоставленных учетных записей и ввести пароль для нее. Альтернативно, можно нажать кнопку **Другой пользователь** (Other User) и ввести имя пользователя и пароль для него. Обратите внимание, что кнопка **Сменить пользователя** обозначена стрелкой влево в круге и находится слева от аватара пользователя.

По умолчанию учетная запись, по которой выполнялся последний вход в систему, указывается в формате *компьютер\имя_пользователя* или *домен\имя_пользователя*. Чтобы войти в систему под этой учетной записью, нужно ввести ее пароль, а затем нажать кнопку **Отпра-**

вить (Submit). Кнопка **Отправить** является частью раздела **Пароль** и обозначена стрелкой вправо. Чтобы войти в систему под другой учетной записью, нажмите опцию **Сменить пользователя**, нажмите комбинацию клавиш <Ctrl>+<Alt>+<Del>, а затем кнопку **Другой пользователь**. Информация, которую требуется предоставить при входе в систему, зависит от типа используемой учетной записи:

- если учетная запись находится в текущем домене (домене по умолчанию), введите имя пользователя и пароль, а затем нажмите кнопку со стрелкой;
- если учетная запись находится в другом домене, нужно указать домен и имя учетной записи в формате *домен\имя_пользователя*, например *cpandl\Alice*;
- чтобы войти в систему на локальном компьютере, имя пользователя вводится в формате *.\имя_пользователя*, где *имя_пользователя* — это имя локальной учетной записи, например *.\alice*.

Когда выполнен вход в систему, можно показать экран входа, нажав комбинацию клавиш <Ctrl>+<Alt>+<Del>. На этом экране предоставляются опции для блокировки компьютера, смены пользователя, выхода из системы, смены пароля и запуска Диспетчера задач. В правом нижнем углу этого экрана находится кнопка выключения компьютера. При нажатии этой кнопки открывается меню с тремя опциями: **Спящий режим** (Sleep), **Завершение работы** (Shut down) и **Перезагрузка** (Restart).

Поскольку опции завершения работы и перезагрузки являются частью параметров питания, выключить или перезагрузить компьютер можно также посредством следующей процедуры:

1. Проведите пальцем справа к центру экрана или нажмите комбинацию клавиш <Windows>+<C>.
2. В открывшейся с правой стороны экрана кнопочной панели нажмите опцию **Параметры** (Settings). Откроется панель **Параметры**, на которой нажмите кнопку **Выключение** (Power).
3. В открывшемся меню нажмите требуемую опцию — **Завершение работы** или **Перезагрузка**.

> ***Примечание***
>
> Операционная система Windows поддерживает быстрое переключение пользователей при работе в доменах и в рабочих и домашних группах. Быстрое переключение пользователей позволяет осуществить вход другому пользователю без необходимости выполнять выход текущего пользователя. Для быстрой смены пользователя нажмите комбинацию клавиш <Ctrl>+<Alt>+<Del>, а затем — опцию **Сменить пользователя**.

Управление паролями учетных записей в Windows 8

В Windows 8 предоставляются способы быстро и с легкостью управлять паролями учетных записей. В частности, возможно выполнять такие задачи:

- изменять пароль текущего пользователя;
- изменять пароль для учетной записи другого домена или локального компьютера;
- создавать диск для сброса пароля;
- выполнять сброс пароля пользователя.

Эти задачи рассматриваются в последующих разделах.

Изменение пароля текущего пользователя

Изменить пароль текущего пользователя можно следующим образом:

1. Нажмите комбинацию клавиш <Ctrl>+<Alt>+<Del>, а затем выберите опцию **Сменить пароль** (Change a password).

> ***Примечание***
>
> В доменах имя учетной записи пользователя предоставляется в формате *домен\имя_пользователя*. В домашних или рабочих группах указывается просто имя локальной учетной записи текущего пользователя.

2. Введите текущий пароль в поле **Старый пароль** (Old password).
3. Введите и подтвердите новый пароль в полях **Новый пароль** (New password) и **Подтверждение** (Confirm password) соответственно.
4. Нажмите стрелку вправо в поле **Подтверждение**, чтобы подтвердить изменение пароля.

Изменение пароля другой учетной записи

Пароль для доменной или локальной учетной записи, иной, чем учетная запись текущего пользователя, можно изменить следующим образом:

1. Нажмите комбинацию клавиш <Ctrl>+<Alt>+<Del>, а затем выберите опцию **Сменить пароль** (Change a password).
2. Введите в поле с именем пользователя имя учетной записи, для которой нужно сменить пароль.

> ***Примечание***
>
> Имя доменной учетной записи указывается в формате *домен\имя_пользователя*, например *cpandl\alice*. Имя локальной учетной записи вводится в формате *.\имя_пользователя*, где *имя_пользователя* — это имя локальной учетной записи, например *.\alice*.

3. Введите текущий пароль в поле **Старый пароль** (Old password).
4. Введите и подтвердите новый пароль в полях **Новый пароль** (New password) и **Подтверждение** (Confirm password) соответственно.
5. Нажмите стрелку вправо в поле **Подтверждение**, чтобы подтвердить изменение пароля.

Создание и использование диска сброса пароля

Пароли доменных и локальных пользователей управляются по-разному. В доменах паролями доменных пользователей управляют администраторы, которые могут выполнять сброс забытого пароля с помощью оснастки консоли MMC, называющейся **Active Directory — Пользователи и компьютеры** (Active Directory Users and Computers).

В домашних и рабочих группах пароли для локальных учетных записей можно сохранить в защищенном шифрованием файле на диске, который можно использовать для сброса забытых паролей. Диск для сброса пароля можно создать посредством следующей процедуры:

1. Нажмите комбинацию клавиш <Ctrl>+<Alt>+<Del>, а затем выберите опцию **Сменить пароль** (Change a password).
2. Нажмите опцию **Создать диск сброса пароля** (Create a password reset disk), в результате чего будет запущен мастер забытых паролей (Forgotten Password Wizard).
3. Ознакомьтесь с информацией по сбросу паролей, представленной на вступительной странице мастера. Вставьте в один из портов USB флеш-накопитель, а затем нажмите кнопку **Далее**.

4. В списке приводов выберите требуемый флеш-накопитель. Коснитесь или нажмите кнопку **Далее**.
5. Введите пароль для текущего пользователя, а затем нажмите кнопку **Далее**.
6. После создания мастером диска для сброса пароля нажмите кнопку **Далее**, удалите флеш-накопитель из разъема, а затем кнопку **Готово**.

Созданный диск сброса пароля следует хранить в безопасном месте, т. к. с его помощью любое лицо может получить доступ к данным пользователя. Теперь, если пользователь забыл пароль и не может войти в систему под своей учетной записью, с помощью созданного диска можно создать новый пароль.

ПРАКТИЧЕСКИЙ СОВЕТ

Флеш-накопители и другие съемные носители можно защитить, зашифровав их с помощью средства BitLocker To Go. Заблокированный таким образом носитель можно разблокировать посредством пароля или PIN-кода смарт-карты, но для этого пользователь должен выполнить вход в систему. Когда же пользователь не может войти в систему, то защищенный с помощью средства BitLocker To Go носитель нельзя разблокировать. Поэтому диски для сброса пароля не следует защищать с помощью средства BitLocker To Go. Дополнительную информацию *см. в главе 11*.

Сброс пароля пользователя

Администраторы могут выполнять сброс забытого пароля с помощью оснастки консоли MMC, называющейся **Active Directory — Пользователи и компьютеры** (Active Directory Users and Computers). В домашних и рабочих группах сброс пароля можно выполнить следующим образом:

1. На экране входа в систему не вводите пароль, а просто нажмите стрелку с правой стороны поля ввода пароля. Выведется сообщение о неправильном пароле и предложение попробовать еще раз. Нажмите кнопку **OK**. Снова откроется экран входа в систему, но под полем ввода пароля отобразится подсказка для пароля и опция **Сбросить пароль** (Reset password). Подсказка и предложение сброса пароля также отображаются при вводе неправильного пароля.
2. Вставьте в USB-порт флеш-накопитель с файлом сброса пароля *(см. предыдущий раздел)*, а затем нажмите кнопку **Сбросить пароль**. Откроется начальная страница мастера сброса пароля.
3. Ознакомьтесь с инструкциями по сбросу пароля, представленными на этой странице, а затем нажмите кнопку **Далее**.
4. На следующей странице мастера укажите привод со съемным носителем, содержащим файл сброса пароля, а затем нажмите кнопку **Далее**.
5. На следующей странице мастера, **Сброс пароля текущей учетной записи** (Reset the user account password), введите новый пароль и подтвердите его.
6. Также введите подсказку для пароля, а затем нажмите кнопку **Далее**. На последней странице мастера нажмите кнопку **Готово**.

Схемы управления питанием, спящий режим и завершение работы

Обычно компьютеры под управлением Windows 8 используют сбалансированную схему управления питанием. Согласно этой схеме после определенного периода отсутствия дейст-

вий со стороны пользователя автоматически отключается дисплей, а затем компьютер переводится в спящий режим.

При переходе в спящий режим операционная система автоматически сохраняет всю работу, выключает дисплей и переводит компьютер в режим сна. Спящий режим — это режим низкого энергопотребления, в котором состояние компьютера хранится в оперативной памяти, а жесткие диски и вентиляторы выключены.

При переходе в спящий режим Windows 8 сохраняет состояние компьютера, поэтому пользователю не требуется завершать работу программ перед этим. Также энергопотребление компьютера в этом режиме очень низкое.

> ***Совет***
>
> В зависимости от типа компьютера, спящий режим работает немного по-разному. В частности, спящим режимом мобильных компьютеров часто можно управлять, закрывая и открывая крышку с экраном: при закрытии крышки ноутбук переходит в спящий режим, а при открытии — возвращается в рабочий режим. Если ноутбук находится в спящем режиме длительное время или заряд его батареи понижается к критическому уровню, состояние компьютера сохраняется на жесткий диск и выполняется полное выключение компьютера. Это конечное состояние похоже на состояние гибернации, которое использовалось в ранних версиях Windows.

Просмотр или изменение параметров энергопитания осуществляется из Панели управления. Откройте раздел **Система и безопасность**, а затем в разделе **Электропитание** (Power Options) выберите опцию **Настройка перехода в спящий режим** (Change when the computer sleeps). Доступные здесь опции зависят от типа компьютера. В случае ноутбуков и планшетов, может предоставляться возможность настройки параметров **От батарей** (On battery) и **От сети** (Plugged in) для понижения яркости экрана, отключения экрана, перевода компьютера в спящий режим и настройки яркости экрана (рис. 1.4).

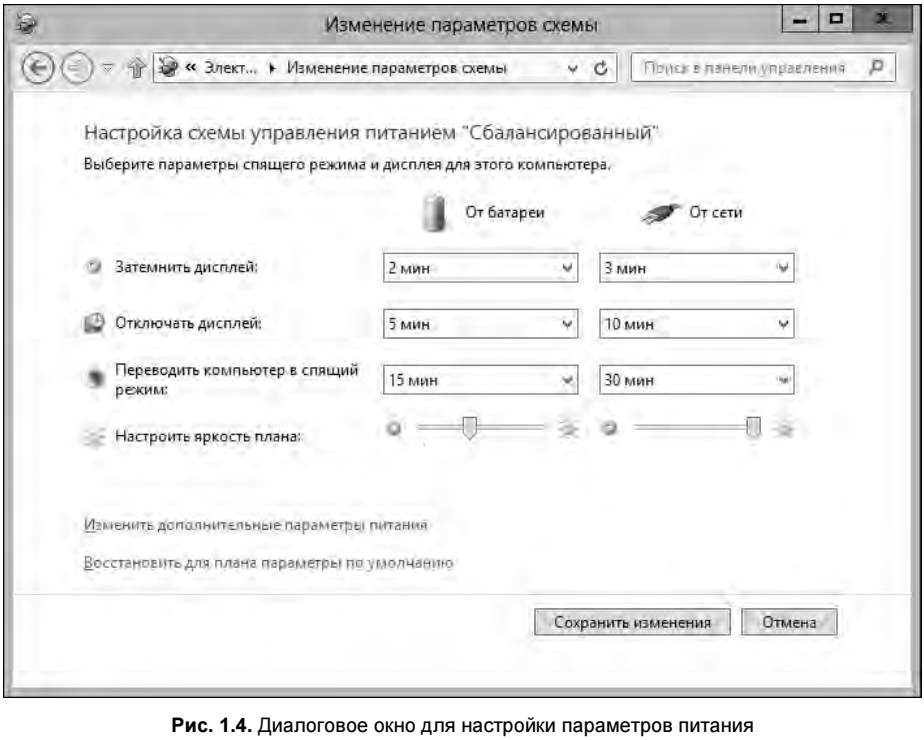


Рис. 1.4. Диалоговое окно для настройки параметров питания

А для настольных компьютеров можно только задать время для отключения экрана и для перехода компьютера в спящий режим. Установив требуемые параметры, нажмите кнопку **Сохранить изменения** (Save changes), чтобы сохранить их и закрыть окно настройки параметров питания.

Большинство компьютеров можно перевести в спящий режим, нажав кнопку **Параметры** в кнопочной панели, затем — кнопку **Выключение** и в открывшемся меню выбрав опцию **Спящий режим**. Чтобы вывести компьютер из спящего режима, нужно выполнить длительное нажатие на сенсорном экране, подвигать мышь или нажать любую клавишу. Обратите внимание, что корпуса некоторых компьютеров оснащены отдельными кнопками включения/выключения питания и управления спящим режимом. Особенности работы этих кнопок можно настроить в окне параметров питания.

В некоторых случаях компьютер не может выполнять переход в режим сна. Работа кнопок питания и управления режимом сна зависит от аппаратного обеспечения системы, ее конфигурации и настройки. Аппаратное обеспечение некоторых компьютеров не поддерживает режим сна. Соответственно, такие компьютеры не могут выполнять переход в этот режим. То же самое имеет место в случае при установленных обновлениях или программах, которые требуют перезагрузки компьютера. Кроме этого, администратор компьютера может настроить параметры компьютера и его кнопок питания и управления спящим режимом на альтернативные действия. В таком случае вместо действий выключения и перехода в режим сна по умолчанию будут выполняться установленные администратором действия.

> ***Осторожно!***
>
> При обслуживании компьютера, который находится в спящем режиме, не забывайте, что он продолжает получать питание. Поэтому никогда нельзя устанавливать аппаратные компоненты в компьютер, который находится в спящем режиме. Для этого в обязательном порядке выньте шнур питания компьютера из розетки электросети, прежде чем устанавливать в компьютер внутренние устройства. Исключение составляют внешние устройства USB, FireWire и eSATA, которые не требуют выключения и обесточивания компьютера для их подключения.

Чтобы изменить параметры по умолчанию для кнопки питания, откройте Панель управления, в ней — раздел **Система и безопасность**, а затем в разделе **Электропитание** выберите опцию **Настройка функций кнопок питания** (Change what the power buttons do). Как и в случае с настройкой параметров питания, доступные здесь опции зависят от типа компьютера. В мобильных компьютерах можно установить параметры **От батарей** и **От сети**, чтобы задать действия при нажатии кнопки питания, нажатии кнопки спящего режима и закрытии крышки (рис. 1.5).

Кроме этого, нажатие опции **Изменение недоступных в данный момент параметров** (Change settings that are currently available) предоставляет доступ к настройке требования ввода пароля и завершения работы. В частности:

- можно установить переключатель **Запрашивать пароль** (Require a password), чтобы при выходе из режима сна было необходимо ввести пароль для разблокирования компьютера;
- установить флажок опции **Включить быстрый запуск** (Turn on fast startup), чтобы при выключении компьютера сохранять системную информацию в файл на системном диске. Этот файл считывается при запуске компьютера с целью ускорить процесс загрузки. При перезагрузке компьютера быстрый запуск не применяется;
- выбрать режимы питания, отображаемые при нажатии кнопки **Выключение**.

Установив требуемые параметры, нажмите кнопку **Сохранить изменения** (Save changes), чтобы сохранить их и закрыть окно настройки кнопок питания и спящего режима.

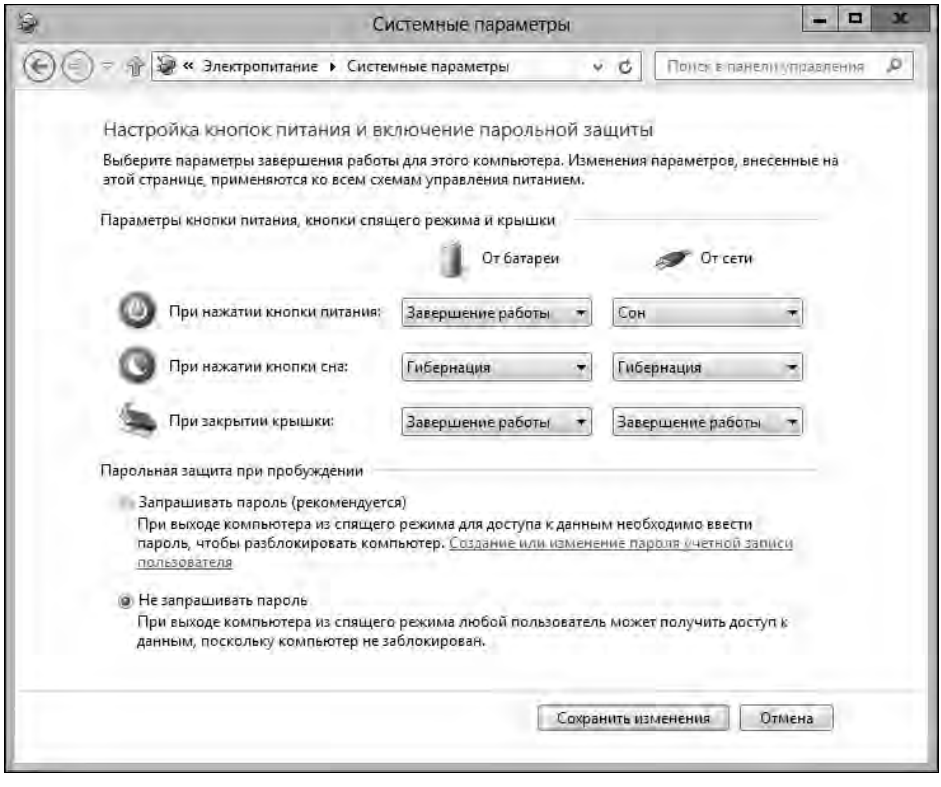


Рис. 1.5. Настройка параметров кнопок питания и спящего режима

Архитектура Windows 8

Тем, кто хочет по-настоящему понять работу Windows 8, нужно заглянуть поглубже во внутреннее устройство этой операционной системы. Для загрузки Windows 8 не применяется файл инициализации. Вместо этого для инициализации и запуска этой операционной системы используется диспетчер загрузки Windows (Windows Boot Manager).

Эта среда загрузки существенным образом изменяет способ загрузки операционной системы. Данная среда загрузки была разработана корпорацией Microsoft с целью решения нескольких трудных проблем, связанных с целостностью загрузки и операционной системы, и абстракцией микропрограммного обеспечения. Среда загрузки загружается перед операционной системой и играет роль среды предоперационной системы. В этом качестве среда загрузки может использоваться для проверки целостности, как процесса запуска, так и самой операционной системы до того, как собственно запускать операционную систему.

Среда загрузки представляет собой расширяемый уровень абстракции, который позволяет операционной системе работать с разными типами микропрограммных интерфейсов, не требуя создания операционной системы специально для работы с этими микропрограммными интерфейсами. Вместо того чтобы обновлять операционную систему при каждой новой разработке микропрограммного интерфейса (МПИ), разработчики МПИ могут использовать стандартные программные интерфейсы среды загрузки, чтобы разрешить операционной системе взаимодействовать требуемым образом посредством МПИ.

Абстракция микропрограммного интерфейса является первой составляющей, которая позволяет Windows 8 работать как с компьютерами с архитектурой BIOS, так и с компьютерами с архитектурой EFI одним и тем же образом. В этом заключается один из главных способов достижения аппаратной независимости в Windows 8. Среда загрузки рассматривается более подробно в *главах 2* и *4*.

Другой составляющей достижения аппаратной независимости в Windows 8 является формат WIM. Корпорация Microsoft поставляет Windows 8 на носителях с образами дисков WIM. В формате WIM применяется сжатие и метод сохранения единственной копии файлов, что существенно уменьшает размер файлов образа. Сжатие уменьшает размер файла образа во многом подобно тому, как сжатие формата ZIP уменьшает размер обычных файлов. А применение метода единственной копии сокращает размер файла образа вследствие того, что для всех случаев вхождения определенного файла в образе сохраняется только одна физическая копия этого файла.

Последней составляющей, обеспечивающей аппаратную независимость Windows 8, является модульность. Благодаря использованию в Windows 8 модульной архитектуры, каждый компонент этой операционной системы определяется как независимая единица или модуль. Так как модули могут содержать другие модули, различные основные функциональности можно группировать вместе и описывать независимо от других основных функциональностей. А независимость модулей друг от друга позволяет добавлять или удалять модули для достижения специальных целей.

Windows 8 содержит обширную вспомогательную архитектуру, центром которой являются встроенные возможности диагностики, поиска и устранения неполадок. Разработчики Microsoft сделали эти встроенные средства способными самостоятельно выполнять диагностирование и устранение обнаруженных неполадок, а в случае, когда они не в силах делать этого, предоставлять пользователю руководство по диагностированию.

Операционная система Windows 8 содержит функциональности осведомленности о сетевом состоянии и обнаружения сетевых ресурсов. Возможность осведомленности о сетевом состоянии отслеживает изменения в конфигурации и связности узлов сети. А функциональность обнаружения сетевых ресурсов управляет возможностями компьютера по обнаружению других компьютеров и устройств в сетевом окружении.

Функциональность осведомленности о сетевом состоянии позволяет Windows 8 обнаруживать текущее состояние конфигурации и связности сети. Это важная возможность, т. к. многие параметры сети и безопасности зависят от типа сети, к которой подключен компьютер. Операционная система Windows 8 предоставляет разные сетевые конфигурации для доменных, частных и публичных сетей и может обнаруживать:

- изменение подключения к сети;
- наличие подключения к Интернету;
- возможность подключения к корпоративной сети через Интернет.

Брандмауэр Windows 8 поддерживает одновременное подключение к нескольким сетям и множественные активные профили брандмауэра. Благодаря этой возможности активный профиль брандмауэра для сетевого подключения зависит от типа подключения.

Если отключить компьютер от одного сетевого коммутатора или концентратора и подключить его к другому, можно непреднамеренно заставить компьютер подумать, что было выполнено подключение к другой сети. В зависимости от параметров групповой политики это может вызвать блокировку компьютера, когда применяются дополнительные параметры сетевой безопасности. Статус сетевых подключений можно просматривать в Центре управ-

ления сетями и общим доступом (Network and Sharing Center) (рис. 1.6). Чтобы открыть окно этой консоли, в Панели управления выберите раздел **Сеть и Интернет** (Network and Internet), а затем опцию **Центр управления сетями и общим доступом**.

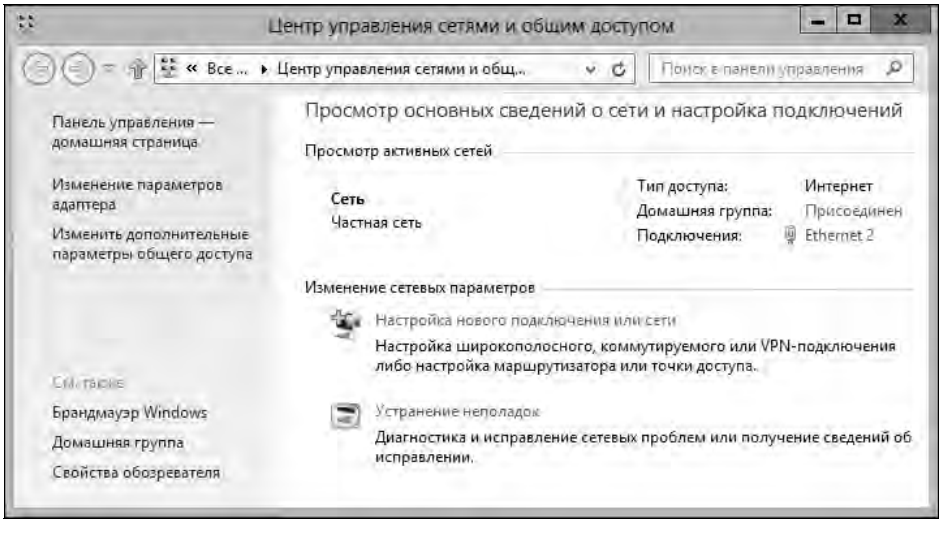


Рис. 1.6. Центр управления сетями и общим доступом

Совет

Посредством возможности DirectAccess компьютеры под управлением Windows 8 могут напрямую связываться с корпоративными сетями, откуда бы то ни было, при условии наличия доступа к Интернету и вдобавок для этого им не нужно инициировать VPN-подключения. Эта функциональность требует наличия в корпоративной сети должным образом настроенных серверов DirectAccess и включения DirectAccess в групповой политике. Дополнительные сведения об этой функциональности *см. в главе 16*.

Операционная система Windows 8 отслеживает статус идентифицирования всех сетей, к которым подключался компьютер. Когда Windows 8 выполняет идентификацию сети, в Центре управления сетями и общим доступом отображается состояние **Идентифицирование сети** (Identifying Networks). Это временное состояние для сети, которая определяется. После того как Windows 8 определит сеть, эта сеть становится *опознанной сетью* (Identified Network) и отображается в Центре управления сетями под своим именем или именем домена.

Если Windows 8 не может идентифицировать сеть, она отображается в Центре управления сетями как **Неопознанная сеть** (Unidentified network). В групповой политике можно задать типы расположения и разрешения пользователей по умолчанию для каждого состояния сети, а также для всех сетей, используя для этого **Политики диспетчера локальных сетей** (Network List Manager Policies). Для доступа к этому узлу в консоль MMC нужно добавить оснастку **Редактор объектов групповой политики** (Group Policy Object Editor), объект **Локальный компьютер** (Local Computer), а затем из корня консоли последовательно развернуть узлы **Политика "Локальный компьютер"\Конфигурация компьютера\Конфигурация Windows\Параметры безопасности** (Local Computer Policy\Computer Configuration\Windows Settings\Security Settings).

При работе в Центре управления сетями и общим доступом можно попытаться выполнить диагностику состояния предупреждения с помощью еще одного ключевого компонента ин-

фраструктуры диагностирования и поиска и устранения неполадок — средства диагностики сетей Windows (Windows Network Diagnostics). Чтобы запустить это средство диагностики, щелкните по ссылке **Устранение неполадок** (Troubleshoot problems) в разделе **Изменение сетевых параметров** (Change your network settings) центра, а затем нажмите кнопку **Далее**. Средство диагностики сетей Windows попытается определить проблему с сетью и предоставить возможное решение этой проблемы.

Инфраструктура Windows для выполнения диагностики и поиска и устранения неполадок предоставляет улучшенное руководство по диагностированию, дополнительные сведения в сообщениях об ошибках, расширенное протоколирование событий, а также всесторонние политики восстановления. Хотя ранние версии Windows содержали некоторые возможности диагностирования, большинство этих возможностей не способны самостоятельно выполнять диагностирование и устранение определенных неполадок. Эта же версия Windows может определять многие типы проблем с аппаратным обеспечением, памятью и производительностью и автоматически устранять их или же предоставлять пользователю помощь в процессе их устранения. Дополнительную информацию *см. в разд. "Работа с автоматизированной системой справки и поддержки" главы 9*.

Также автоматизировано обнаружение ошибок устройств и отказов жестких дисков. В случае проблем с устройством, средство диагностирования аппаратного обеспечения может обнаружить состояние сбоя и/или автоматически устранить неисправность или же руководить пользователем в процессе ее устранения. В случае жестких дисков, средство диагностирования аппаратного обеспечения может использовать отчеты о сбоях, предоставляемые приводами жестких дисков, для обнаружения возможных отказов и заблаговременного предупреждения пользователя об этом. После предупреждения о возможном отказе диска средство диагностирования аппаратного обеспечения также может руководить процессом создания резервной копии этого диска.

Операционная система Windows 8 может автоматически обнаруживать проблемы с производительностью, которые включают медленный запуск приложений, медленную загрузку компьютера, медленный переход в состояние ожидания и обратно в рабочий режим, а также медленное завершение работы. В случае пониженной производительности компьютера, средства диагностики Windows 8 могут определить источник проблемы и предоставить возможные решения. В случае более сложных проблем с производительностью можно отслеживать данные, качающиеся производительности и достоверности, в консоли Монитора ресурсов.

Операционная система Windows 8 также может обнаруживать проблемы, связанные с утечкой памяти и ее неисправностями. При подозрении наличия проблемы с памятью, которая не обнаруживается автоматически, можно выполнить ручную диагностику памяти с помощью Средства проверки памяти Windows (Windows Memory Diagnostic). Процедура диагностики памяти следующая:

1. В окне **Пуск** введите с клавиатуры имя исполняемого файла средства проверки памяти mdsched.exe, а затем нажмите клавишу <Enter>. Обычно текст, вводимый с клавиатуры в экране **Пуск**, по умолчанию вводится в поле поиска приложений.
2. Выберите, выполнить ли перезагрузку и проверку сейчас же или же выполнить проверку при следующем включении компьютера (рис. 1.7).
3. Средство проверки памяти запустится автоматически после перезагрузки компьютера и выполнит стандартное тестирование памяти. Для выполнения дополнительных тестов (или сокращения количества стандартных тестов) нажмите клавишу <F1>, а затем с помощью клавиш <↑> и <↓> выберите один из наборов тестов — **Базовый** (Test Mix as

Basic), **Стандартный** (Standard) или **Широкий** (Extended), а затем нажмите клавишу <F10>, чтобы продолжить тестирование с установленными параметрами.

4. По завершению тестирования выполняется перезагрузка компьютера, и после входа в систему о результатах проверки памяти сообщается во всплывающем сообщении в области уведомлений панели задач.

Если вследствие проблем с памятью происходит сбой компьютера и Средство диагностики памяти обнаруживает эту проблему, пользователю предлагается запланировать проверку памяти при следующей загрузке компьютера.

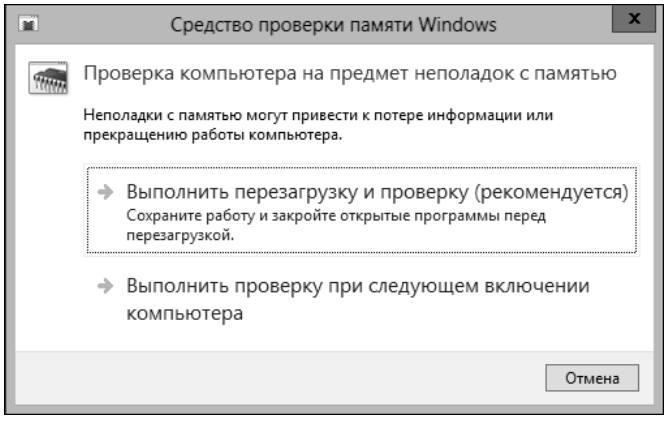


Рис. 1.7. Окно средства проверки памяти Windows

ГЛАВА 2

Конфигурирование компьютеров Windows 8

Одной из основных обязанностей администратора является управление конфигурацией операционной системы. Windows 8 обладает многими уникальными характеристиками, включая перечисленные далее.

- **Модульная архитектура** и **двоичные файлы**, которые распределяются посредством образов дисков формата WIM. Это позволяет использовать инструмент DISM для управления пакетами, драйверами, функциональностями и региональными параметрами в файлах образа Windows (файлы с расширением wim) и в файлах виртуальных жестких дисков (файлы с расширением vhd). Как оснастка **Управление дисками**, так и инструмент DiskPart были модернизированы для работы с vhd-файлами.
- **Предзагрузочная среда**, в которой для управления запуском системы и загрузки выбранного приложения применяется диспетчер загрузки Windows. По этой причине для загрузки Windows 8 не используются файлы Ntldr и Boot.ini, которые требовались для загрузки предыдущих операционных систем, а также предоставляются дополнительные опции загрузки. Например, компьютер можно загрузить операционной системой, находящейся в vhd-файле. Один из способов сделать это — создать основной загрузочный образ, который при запуске компьютера посредством утилиты Xcopy копирует требуемый vhd-файл на указанный диск.
- **Средство управления правами и доступом пользователем**, называющееся *контролем учетных записей пользователей* (User Account Control, UAC), которое применяется для контроля исполнения процессов и взаимодействия приложений с операционной системой. Вследствие этого, управление правами пользователей и контроль доступа в Windows 8 осуществляется иначе, чем в предыдущих версиях этой ОС. Как рассматривается в *главе 7*, вывод сообщений контроля учетных записей пользователей можно оптимизировать или отключить, но это не отключает другие функциональности контроля учетных записей, таких как виртуализации приложений.

Кроме этого, нужно знать и понимать инструменты и опции конфигурирования Windows 8, что и рассматривается в этой главе. Многие из этих требуемых инструментов доступны с экрана **Приложения**, быстрый доступ к которому можно получить, нажав комбинацию клавиш <Windows>+<Q>. В случае сенсорного интерфейса для этого нужно провести пальцем с правой стороны экрана к центру, а затем выбрать опцию **Поиск**, чтобы отобразить экран **Приложения** (т. к. обычно по умолчанию фокус поиска установлен на приложениях). Если вы последовали моему совету в *главе 1*, то закрепили основные инструменты для ежедневной работы на экране **Пуск** или на панели задач рабочего стола, что также позволяет получить быстрый доступ к ним.

Поддержка компьютеров с операционной системой Windows 8

Для успешного управления компьютером, диагностирования проблем и поиска и устранения неполадок требуется знать конфигурацию компьютера. Информацию о конфигурации компьютера можно получить с помощью следующих инструментальных средств поддержки.

- **Консоль Управление компьютером** (Computer Management). Предоставляет доступ к важным инструментам для обслуживания и управления системой, службами и хранилищами данных.
- **Консоль производительности** (Performance Console). Позволяет выполнять мониторинг производительности системы и обнаруживать наличие проблем, отрицательно сказывающихся на производительности.
- **Монитор ресурсов** (Resource Monitor). Обеспечивает просмотр подробной информации об использовании системных ресурсов, включая ресурсы процессоров, памяти, дисков и сетевого окружения. Монитор ресурсов следует использовать в тех случаях, когда требуется более подробная информация, чем можно получить с помощью диспетчера задач.
- **Система** (System). Позволяет просматривать основную информацию о компьютере и управлять свойствами системы.
- **Сведения о системе** (System Information). Отображает подробную системную статистику о конфигурации и наличии ресурсов. Компонент **Сведения о системе** можно также использовать для поиска и устранения неполадок с системой.
- **Диспетчер задач** (Task Manager). Позволяет просматривать информацию об использовании системных ресурсов.

Способы применения этих инструментов рассматриваются в этом разделе. Но сначала может быть полезным добавить средства администрирования (Administrative Tools) в экран **Пуск**. Для этого с экрана **Пуск** выполните следующее:

- для сенсорных устройств: проведите пальцем справа к центру экрана, коснитесь опции **Параметры**, затем опции **Плитки** и, наконец, опции **Показать средства администрирования** (Show administrative tools);
- для устройств с мышью и клавиатурой: откройте кнопочную панель, поместив указатель мыши в правый нижний или верхний угол экрана. На кнопочной панели нажмите кнопку **Параметры**, в открывшейся одноименной панели выберите опцию **Плитки**, а в этой панели щелкните на ползунке **Показать средства администрирования**.

Касание или щелчок по этому ползунку переключает его между состояниями **Да** и **Нет**, означая показывать или скрывать значки средств администрирования на экране **Пуск**. Теперь при открытии экрана **Пуск** на нем будут отображаться плитки для утилит администрирования.

С экрана **Пуск** и рабочего стола можно открыть очень полезное меню, нажав и удерживая или щелкнув правой мышью по левому нижнему углу экрана. Для компьютеров с мышью и клавиатурой это меню может быть просто полезным, но для устройств с сенсорной клавиатурой оно просто неоценимо. Это меню содержит опции для открытия Панели управления, консоли **Управление компьютером**, оснастки настройки параметров электропитания, оснастки **Система**, поиска, диспетчера задач, Проводника и других средств для администрирования системы.

Дополнительная информация

На экране **Пуск** (начальном экране) при наведении курсора мыши на скрытую кнопку в левом нижнем углу экрана отображается эскиз рабочего стола, щелчок по которому открывает рабочий стол. А на рабочем столе при наведении курсора мыши на скрытую кнопку в левом нижнем углу экрана отображается эскиз экрана **Пуск**, щелчок по которому открывает этот экран. Длительное же нажатие этой кнопки в сенсорных устройствах или щелчок по ней правой кнопкой мыши в устройствах со стандартным вводом отображает контекстное меню.

Работа в консоли *Управление компьютером*

Консоль **Управление компьютером** (Computer Management) предназначена для выполнения основных задач администрирования локальных и удаленных систем. Если на экран **Пуск** были добавлены средства администрирования, консоль **Управление компьютером** можно запустить, коснувшись плитки этой утилиты или щелкнув по ней. Другим способом открыть консоль управления компьютером будет ввести текст `compmgmt.msc` в поле поиска в панели поиска приложений, а затем нажать клавишу <Enter>.

Главное окно консоли управления компьютером состоит из нескольких панелей и похоже на главное окно Проводника Windows (рис. 2.1).

Дерево узлов консоли в левой панели используется для перемещения по инструментам консоли и их выбора. Панель **Действия** (Actions), которая на рис. 2.1 не показана, дублирует

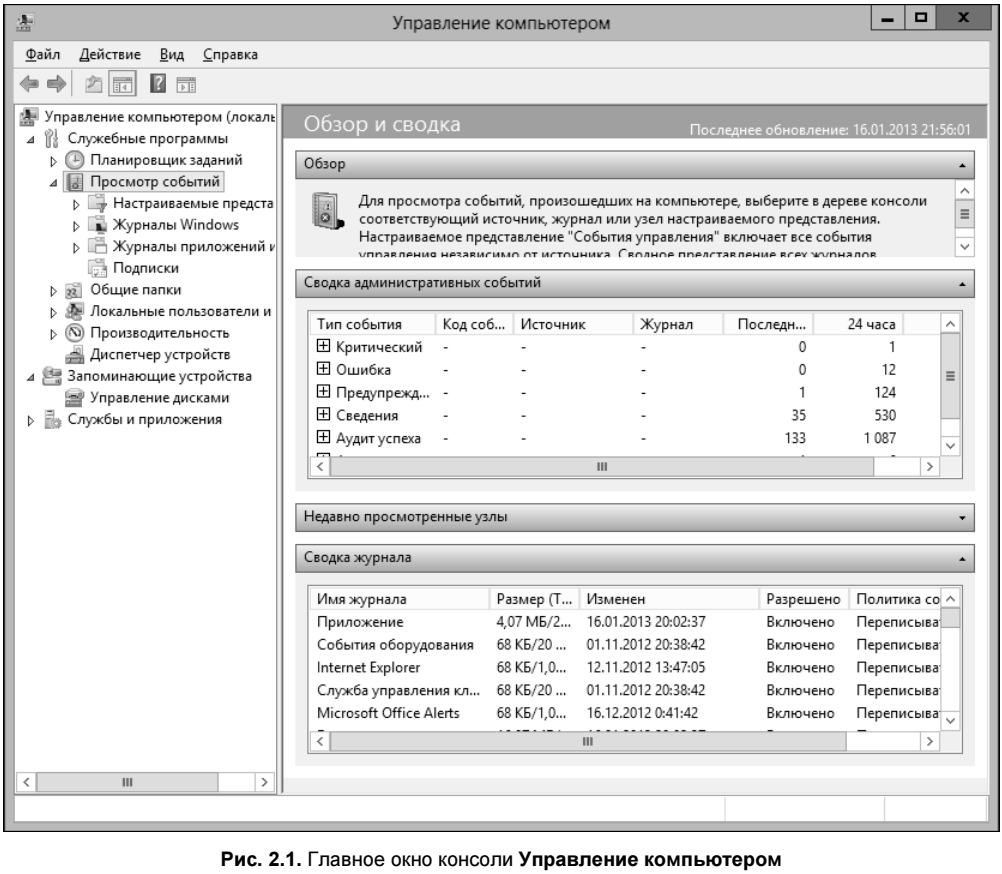


Рис. 2.1. Главное окно консоли **Управление компьютером**

элементы контекстного меню узлов консоли, отображаемого при щелчке на узле правой кнопкой мыши или длительном нажатии. Отобразить эту панель можно, нажав значок **Отображение и скрытие панели действий** (Show/Hide Action Pane) на панели инструментов консоли[1]. Инструменты консоли сгруппированы по трем общим категориям:

- **Служебные программы** (System Tools) — инструменты общего назначения для управления системой и просмотра системной информации;
- **Запоминающие устройства** (Storage) — средство управления дисками;
- **Службы и приложения** (Service and Applications) используются для просмотра и управления свойствами установленных служб и приложений.

Эти категории содержат следующие инструменты.

- **Планировщик заданий** (Task Scheduler). Средство для просмотра и управления запланированными заданиями. Запланированные задания применяются для автоматизации таких процессов, как очистка диска или диагностическое тестирование. Запланированные задания и автоматизация рассматриваются в *главе 10*.
- **Просмотр событий** (Event Viewer). Средство для просмотра журналов событий на выбранном компьютере. В журналах событий протоколируются важные события компьютера. С их помощью можно определить проблемы с конфигурацией компьютера и т. п. Предмет событий и журналов событий обсуждается в *главе 10*.
- **Общие папки** (Shared Folders). Средство для просмотра и управления общими папками, а также связанными сеансами и открытыми файлами. Общие папки рассматриваются в *главе 13*.
- **Локальные пользователи и группы** (Local Users and Groups). Средство для управления локальными пользователями и группами локальных пользователей на выбранном компьютере. На каждом клиентском компьютере имеются как локальные пользователи, так и локальные группы, отдельные от доменных пользователей и групп. Работа с локальными пользователями и группами обсуждается в *главе 7*.
- **Производительность** (Performance). Этот узел содержит инструменты мониторинга и отчетности, с помощью которых можно определить текущую производительность компьютера, а также отслеживать производительность в течение некоторого времени.
- **Диспетчер устройств** (Device Manager). Центральный пункт для проверки состояния всех установленных на компьютере устройств, а также для обновления их драйверов. Также можно использовать для диагностирования проблем с устройствами. Управление устройствами рассматривается в *главе 9*.
- **Управление дисками** (Disk Management). Средство для управления жесткими дисками, разделами дисков и наборами томов. Операционная система Windows 8 поддерживает такие способы организации дисков, как объединение дисков, чередование дисков, чередование дисков с контролем по четности, а также зеркалирование дисков. Объединение дисков дает возможность создать том, охватывающий несколько физических дисков. Чередование дисков позволяет распределять данные поблочно на нескольких дисках, чтобы ускорить доступ к данным. Но ни один из этих способов организации дисков не обеспечивает защиты от отказов, и в случае отказа одного из объединенных или чередующихся дисков из строя выходит весь том.

---

[1] Другой способ отобразить эту панель — установить флажок **Панель действия** (Action pane) в диалоговом окне **Настройка вида** (Customize View). Для открытия этого окна нужно в меню **Вид** (View) выбрать команду **Настроить...** (Customize...).

- **Службы** (Services). Оснастка для просмотра и управления системными службами, исполняющимися на компьютере. В Windows 8 для каждой службы имеется политика восстановления. В случае сбоя службы, Windows 8 пытается перезапустить ее автоматически и также автоматически обрабатывает как компоненты, зависящие от службы, так и компоненты, от которых зависит сама служба. Прежде чем пытаться перезапустить службу, испытавшую сбой, выполняется попытка запустить службы и системные компоненты, от которых данная служба зависит. Предмет работы со службами рассматривается в *главе 9*.
- **Управляющий элемент WMI** (WMI Control). Средство для просмотра и управления службой WMI[1]. Служба WMI собирает системную информацию, выполняет мониторинг работоспособности системы, а также управляет компонентами системы. Дополнительную информацию по этой службе *см. в разд. "Работа с управляющим элементом WMI" далее в этой главе*.

Консоль **Управление компьютером** можно использовать для управления удаленным компьютером, который выбирается следующим образом:

1. Нажмите или щелкните правой кнопкой мыши на узле **Управление компьютером** в дереве консоли и в открывшемся контекстном меню выберите команду **Подключиться к другому компьютеру** (Connect to another computer). Откроется диалоговое окно **Выбор компьютера** (Select Computer).
2. Установите в этом окне флажок **другим компьютером** (Another computer) и введите в смежное с флажком поле полное имя (fully qualified name) удаленного компьютера. Например, cspc85.microsoft.com, где cspc85 означает имя компьютера, а microsoft.com — имя домена. Либо выполните поиск требуемого компьютера, нажав кнопку **Обзор** (Browse).
3. Нажмите кнопку **OK**.

Для удаленного управления компьютером с установленной на нем Windows 8 по протоколу WS-Management запустите консоль командной строки от имени администратора, введите команду `winrm quickconfig` и нажмите клавишу <Enter>. На все запросы выполнить конфигурирование нажимайте клавиши <Y> и <Enter>. В результате будет запущена служба WinRM[2], выполнена настройка этой службы на прием запросов WS-Management по любому IP-адресу, создано исключение брандмауэра для службы и, наконец, выполнена настройка параметра `LocalAccountTokenFilterPolicy` на предоставление соответствующих прав на удаленное управление.

Исключения брандмауэра требуются для многих других типов задач удаленного администрирования. Нужно иметь в виду следующее.

- Возможность удаленного рабочего стола включается и выключается отдельно от удаленного управления. Чтобы разрешить подключение к локальному серверу посредством удаленного рабочего стола, нужно разрешить соответствующие подключения к компьютеру и настроить доступ *(см. главу 16)*.
- Для удаленного управления журналами событий компьютера в брандмауэре Windows нужно установить флажок **Удаленное управление журналом событий** (Remote Event Log Management). В разделе **Дополнительные параметры** (Advanced Settings) брандмауэра Windows можно настраивать дополнительные связанные правила, которые раз-

[1] Windows Management Instrumentation — инструментарий управления Windows.

[2] Windows Remote Management — удаленное управление Windows.

решают удаленное управление журналом событий через именованные каналы NP (named pipes) и удаленный вызов процедур RPC (remote procedure call).

- Для удаленного управления назначенными задачами компьютера в брандмауэре Windows нужно установить флажок **Удаленное управление назначенными заданиями** (Remote Scheduled Task Management). В разделе **Дополнительные параметры** брандмауэра Windows можно настраивать дополнительные связанные правила, которые разрешают удаленное управление назначенными заданиями посредством RPC-механизма.
- Для удаленного управления службами в брандмауэре Windows нужно установить флажок **Удаленное управление службой** (Remote Service Management). В разделе **Дополнительные параметры** брандмауэра Windows можно настраивать дополнительные связанные правила, которые разрешают удаленное управление службами посредством именованных каналов и RPC-механизма.
- Для удаленного завершения работы в брандмауэре Windows нужно установить флажок **Удаленное завершение работы** (Remote Shutdown).
- Для удаленного управления томами в брандмауэре Windows нужно установить флажок **Удаленное управление томами** (Remote Volume Management). В разделе **Дополнительные параметры** брандмауэра Windows можно настраивать дополнительные связанные правила, которые разрешают удаленное управление службой виртуальных дисков (Virtual Disk Service) и загрузчика службы виртуальных дисков (Virtual Disk Service Loader).

Получение основных сведений о системе и производительности

Для просмотра и управления свойствами системы применяется консоль **Система** (System). Чтобы открыть эту консоль, в Панели управления коснитесь или щелкните мышью на опции **Система и безопасность** (System and Security), а затем выберите опцию **Система**. Как можно видеть на рис. 2.2, консоль **Система** разделена на четыре основные области, которые содержат ссылки для выполнения распространенных заданий и просмотра системы.

Конкретно, консоль **Система** состоит из следующих четырех областей:

- **Выпуск Windows** (Windows Edition) — здесь указываются выпуск и версия операционной системы;
- **Система** (System) — здесь указывается процессор, память, индекс производительности и разрядность установленной операционной системы (32- или 64-разрядная);
- **Имя компьютера, имя домена и параметры рабочей группы** (Computer name, domain, and workgroup settings) содержит имя и описание компьютера, а также сведения о домене, рабочей группе или домашней группе. Для редактирования сетевой информации коснитесь или щелкните мышью на ссылке **Изменить параметры** (Change settings) и в открывшемся диалоговом окне **Свойства системы** (System Properties) нажмите кнопку **Идентификация** (Network ID);
- **Активация Windows** (Windows activation) содержит сведения о статусе активации системы и код продукта. Если установленная Windows 8 еще не была активирована, коснитесь или щелкните мышью по ссылке **Подробнее об активации Windows** (View details in Windows Activation), а затем следуйте выводимым указаниям.

Ссылки в левой панели консоли **Система** предоставляют быстрый доступ к основным средствам поддержки, включая следующие:

- диспетчер устройств (Device Manager);
- настройка удаленного доступа (Remote settings);
- защита системы (System protection);
- дополнительные параметры системы (Advanced system settings).

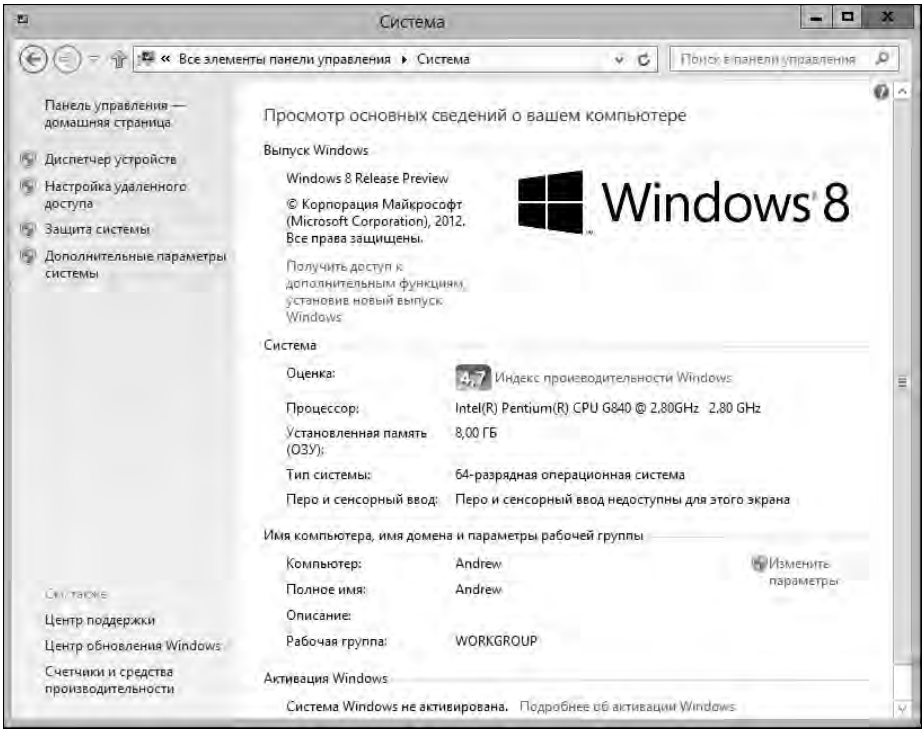


Рис. 2.2. Главное окно консоли **Система**

Нажатие ссылки **Изменить параметры** в разделе **Имя компьютера, имя домена и параметры рабочей группы** открывает диалоговое окно **Свойства системы**. Использование этого диалогового окна для управления конфигурацией компьютера рассматривается в *разд. "Управление свойствами системы" далее в этой главе.*

Индекс производительности Windows позволяет определить возможности операционной системы, поддерживаемые аппаратным обеспечением. В большинстве случаев программа установки Windows выполняет оценку производительности компьютера по завершению установки. Для просмотра сведений об оценке компьютера коснитесь или щелкните мышью по ссылке **Индекс производительности Windows** в разделе **Система**, чтобы открыть страницу **Счетчики и средства производительности** (Performance Information and Tools), показанную на рис. 2.3.

ПРАКТИЧЕСКИЙ СОВЕТ

Если оценка производительности компьютера не была выполнена автоматически после установки Windows, параметр **Оценка** раздела **Система** вместо значения индекса производительности будет содержать сообщение-ссылку **Оценка системы недоступна** (System rating not available). В таком случае можно самостоятельно выполнить оценку системы, щелкнув на этой ссылке, чтобы открыть страницу **Счетчики и средства производительности** и выполнить оценку системы.

Индекс производительности компьютера может измениться вследствие установки нового устройства. Если Windows обнаружит изменения в аппаратной конфигурации, выдается извещение о том, что **Нужно обновить индекс производительности Windows для этого компьютера** (Your Windows Experience Index needs to be refreshed). В таком случае щелкните на предоставленной ссылке, чтобы открыть страницу **Счетчики и средства производительности**, и нажмите на ней ссылку **Обновить сейчас** (Refresh now) или **Повторить оценку** (Re-run the assessment), чтобы обновить оценку производительности.

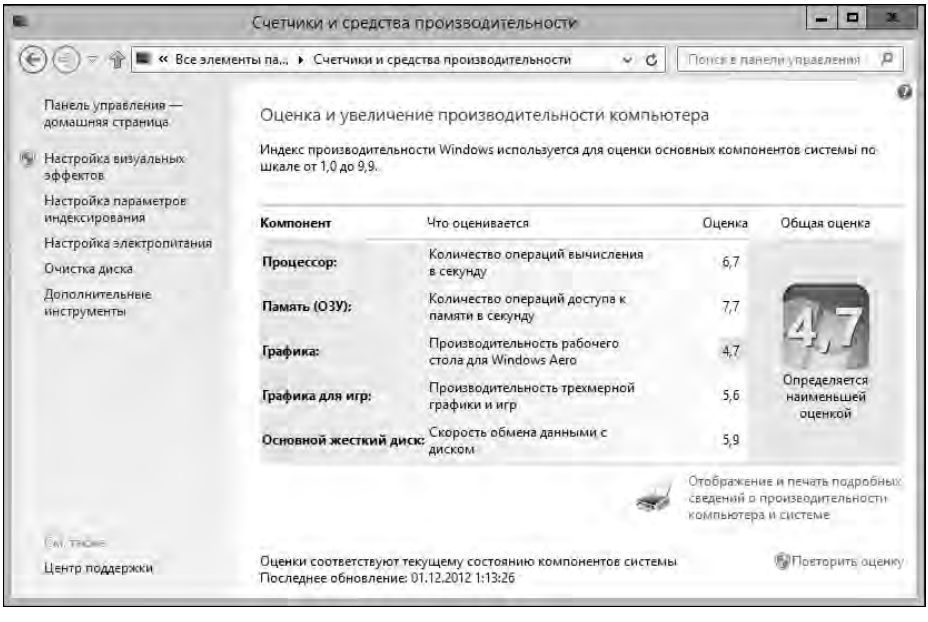


Рис. 2.3. Страница **Счетчики и средства производительности** консоли **Система**

На странице **Счетчики и средства производительности** отображается общая оценка системы, а также список оценок для пяти категорий установленного оборудования:

- процессор;
- память;
- графика;
- графика для игр;
- основной жесткий диск.

Общая оценка компьютера и оценки его отдельных компонентов используются операционной системой Windows для определения способа настройки особенностей персонализации. В случае низкой оценки компьютера, Windows 8 будет рекомендовать отключить некоторые возможности, например функцию Aero Glass, чтобы улучшить производительность системы. На основе долговременной оценки производительности Windows 8 может также рекомендовать отключить или изменить параметры других возможностей с целью повышения производительности.

Совет

На оценку производительности может оказать отрицательное влияние несколько факторов, включая малый объем свободного пространства основного диска. После установки в компьютер нового оборудования или решения проблемы производительности, такой, как малый объем сво-

бодного дискового пространства, можно выполнить повторную оценку производительности компьютера, щелкнув по ссылке **Повторить оценку** на странице **Счетчики и средства производительности** консоли **Система**.

Левая панель страницы **Счетчики и средства производительности** предоставляет быстрый доступ к нескольким полезным областям конфигурации, включая следующие.

- **Настройка визуальных эффектов** (Adjust visual effects). Открывает диалоговое окно **Параметры быстродействия** (Performance Options), в котором можно управлять визуальными эффектами, распределением времени процессора, виртуальной памятью и возможностью DEP[1].
- **Настройка параметров индексирования** (Adjust indexing options). Открывает диалоговое окно **Параметры индексирования** (Indexing Options), в котором можно выполнять настройку расположения и параметров индексов.
- **Настройка электропитания** (Adjust power settings). Открывает диалоговое окно **Электропитание** (Power Options), в котором можно выполнять настройку схем управления электропитанием, задавать действия для выполнения при нажатии кнопки питания и кнопки спящего режима и устанавливать время бездействия для отключения дисплея и для перехода в режим сна.

Одной из наиболее полезных опций страницы **Счетчики и средства производительности** является ссылка **Дополнительные инструменты** (Advanced tools) в левой панели страницы. Щелчок по этой ссылке открывает одноименное окно (рис. 2.4), предоставляющее быстрый доступ к средствам обслуживания системы.

Это окно предоставляет прямой доступ к следующим инструментам:

- диспетчеру задач, который обычно открывается нажатием комбинации клавиш <Ctrl>+<Alt>+<Delete>;
- монитору ресурсов, который обычно открывается нажатием ссылки **Открыть монитор ресурсов** (Open Resource Monitor) на вкладке **Производительность** (Performance) диспетчера задач;
- просмотру дополнительных сведений о системе в окне **Сведения о системе** (System Information), которое обычно открывается исполнением команды `msinfo32`;
- отчетам диагностики системы, которые обычно создаются только в процессе расширенного диагностирования.

Пользователи с правами администратора могут создать отчет по диагностике системы, щелкнув на ссылке **Создать отчет о работоспособности системы** (Generate a system health report). Создание этого отчета может занять около минуты или более. Отчет содержит подробную информацию о состоянии аппаратных ресурсов, быстродействии системы и выполняющихся на компьютере процессах, а также сведения о системе и конфигурационные данные (рис. 2.5).

Отчет по диагностике также содержит предложения касательно исправления проблем, максимизирования производительности и снижения накладных расходов. Отчет можно сохранить в виде HTML-документа, выполнив последовательность команд меню **Файл** | **Сохранить как** (File | Save As) и выбрав с помощью диалогового окна **Сохранение** (Save As) папку для сохранения отчета, также указав в нем его имя. Отчет также можно отправить в виде вложения по электронной почте, выбрав последовательность команд меню **Файл** | **Отправить** (File | Send To).

---

[1] Data Execution Prevention — предотвращение выполнения данных.

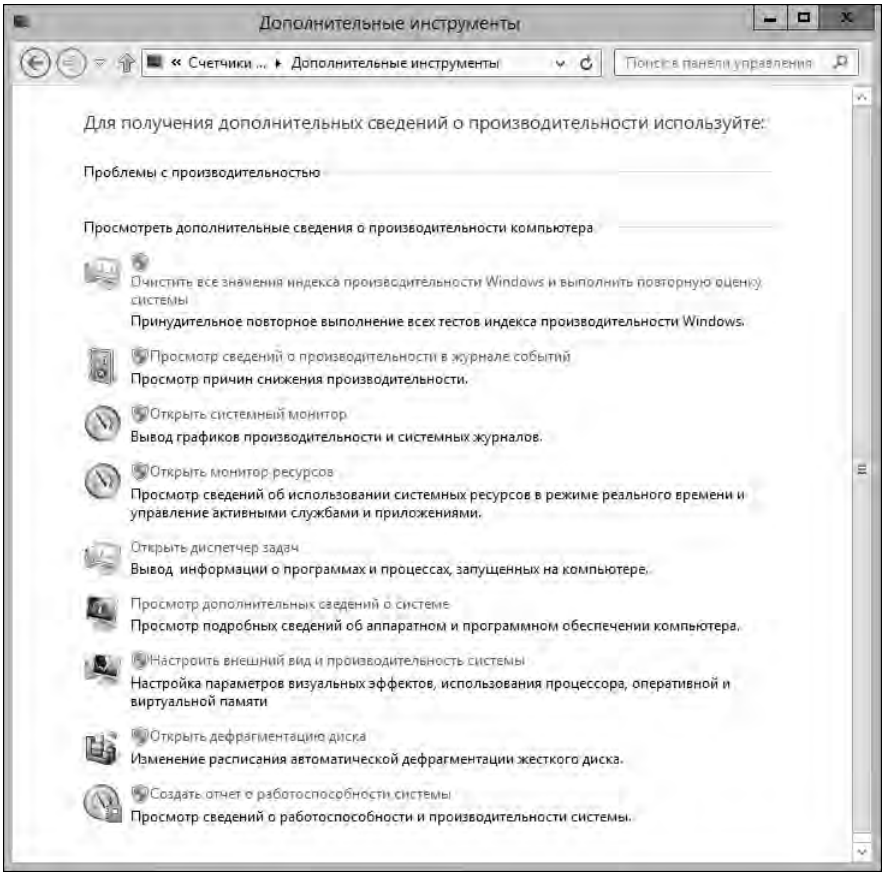


Рис. 2.4. Окно **Дополнительные инструменты** содержит средства для обслуживания системы

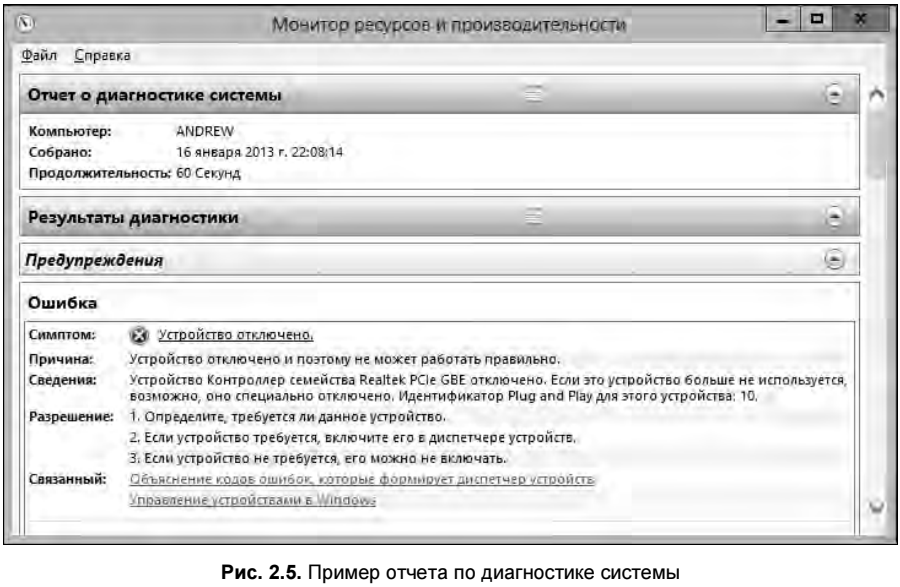


Рис. 2.5. Пример отчета по диагностике системы

Получение дополнительных сведений о системе

Получить подробные сведения о локальной или удаленной системе можно с помощью оснастки **Сведения о системе** (System Information) (исполняемый файл — msinfo32.exe). Открыть окно этой оснастки можно, щелкнув по ссылке **Сведения о системе** на экране **Приложения** или введя текст `msinfo` в поле поиска панели **Приложения** и нажав клавишу <Enter>. Как показано на рис. 2.6, общую информацию о системе можно просмотреть, выбрав узел **Сведения о системе** (System Summary).

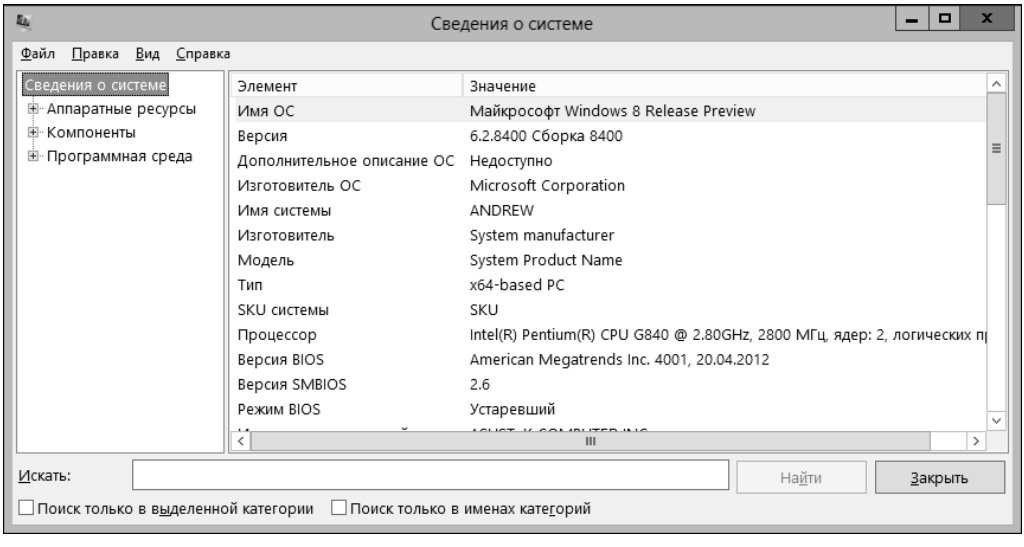


Рис. 2.6. Оснастка **Сведения о системе** может быть полезной в поиске и устранении проблем конфигурации системы

Все статистические данные по конфигурации собираются с помощью службы инструментария управления Windows WMI.

Средство **Сведения о системе** предоставляет подробную информацию о нескольких основных областях операционной системы.

- **Аппаратные ресурсы** (Hardware Resources). Этот раздел содержит подробную информацию о вводе/выводе, запросах на прерывание (IRQ), каналах прямого доступа к памяти (DMA) и устройствах Plug and Play. Ключевой областью, которую следует проверить, если система испытывает проблемы с каким-либо устройством, является узел **Конфликты и совместное использование** (Conflicts/Sharing). Этот узел содержит суммарную информацию об устройствах, разделяющих ресурсы или вызывающих системные конфликты.
- **Компоненты** (Components). Этот узел содержит подробную информацию об установленных компонентах, от аудиокодеков до устройств ввода и USB-портов. Ключевой областью, которую следует проверить, если система испытывает проблемы с каким-либо компонентом, является узел **Устройства с неполадками** (Problem Devices). Соответственно своему названию этот узел предоставляет информацию об устройствах с неполадками.
- **Программная среда** (Software Environment). Данный узел содержит подробную информацию о рабочей конфигурации операционной системы. Он может быть особенно по-

лезным при диагностировании неполадок удаленной системы. С помощью этого узла можно проверить системные драйверы, переменные среды, задачи печати и сетевые подключения, а также исполняющиеся задания, службы, группы программ и автоматически запускаемые программы.

Для просмотра конфигурационной информации удаленного компьютера применяется следующая процедура:

1. Откройте средство **Сведения о системе**. В меню **Вид** (View) выберите команду **Удаленный компьютер** (Remote Computer). Откроется диалоговое окно **Удаленный компьютер**.
2. В этом окне установите переключатель **Удаленный компьютер в сети** (Remote Computer on the Network).
3. Введите имя компьютера в поле **Сетевое имя компьютера** (Remote Machine Name) и нажмите кнопку **OK**.

Учетная запись, используемая для управления удаленным компьютером, должна обладать соответствующими правами администратора для домена или локальной машины. В случае проблем с получением информации от удаленной системы проверьте пространство имен, используемое службой WMI *(см. следующий раздел)*. При просмотре информации с удаленного компьютера этот факт фиксируется указанием имени этого компьютера в скобках в узле **Сведения о системе**.

Работа с управляющим элементом WMI

Инструментарий управления Windows WMI является ключевой частью операционной системы Windows 8. Он используется для сбора статистических данных о системе, отслеживания ее работоспособности и управления системными компонентами. Для работы инструментария WMI должным образом необходимо, чтобы исполнялась и была правильно настроена служба WMI.

Настройка конфигурации службы WMI осуществляется посредством элемента управления WMI (WMI Control), доступ к которому на локальной или удаленной системе можно получить следующим образом:

1. Откройте консоль **Управление компьютером** (с экрана **Приложения** или с экрана **Пуск**, если на него были добавлены средства администрирования).
2. Щелкните правой кнопкой мыши по узлу **Управление компьютером** в дереве консоли и в открывшемся контекстном меню выберите команду **Подключиться к другому компьютеру** (Connect to another computer). Выберите компьютер, ресурсами которого нужно управлять.
3. Разверните узел **Службы и приложения** (Services and Applications), выполнив по нему двойной щелчок мышью. В этом узле выберите подузел **Управляющий элемент WMI** (WMI Control). (Это требуется для того, чтобы выполнить чтение данного элемента.) Щелкните на этом узле правой кнопкой мыши и в контекстном меню выберите команду **Свойства**. Откроется диалоговое окно **Свойства: Управляющий элемент WMI**, в котором и выполняется настройка инструментария WMI.

Как показано на рис. 2.7, окно свойств управляющего элемента WMI содержит следующие вкладки.

- **Общие** (General). На этой вкладке отображается общая информация о системе и инструментарии WMI. Для получения информации о системе инструментарий WMI использует параметры доступа текущего пользователя.

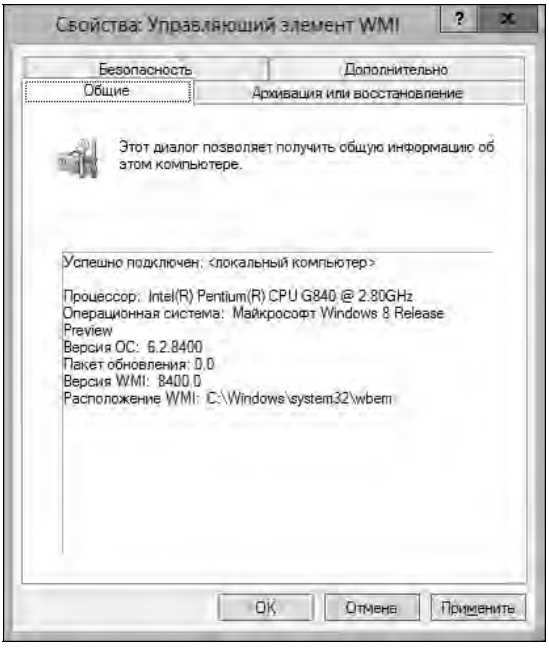


Рис. 2.7. Окно свойств управляющего элемента WMI, в котором выполняется настройка службы WMI

- **Архивация или восстановление** (Backup/Restore). Собранные инструментарием WMI статистические данные помещаются в хранилище. По умолчанию это хранилище размещается в папке *%SystemRoot%*\System32\Wbem\Repository. Для этих данных периодически осуществляется автоматическое резервное копирование. Резервное копирование данных хранилища или их восстановление из резервной копии можно выполнить вручную. Для этого служат кнопки **Архивировать** (Backup Now) и **Восстановить** (Restore Now) на вкладке **Архивация или восстановление** (Backup/Restore).
- **Безопасность** (Security). Параметры этой вкладки определяют, кому предоставляется доступ к разным уровням статистических данных WMI. По умолчанию группа **Администраторы** (Administrators) имеет полный доступ к WMI, а группа **Прошедшие проверку** (Authenticated Users) — разрешение на исполнение методов, включение учетных записей и запись собранных статистических данных.
- **Дополнительно** (Advanced). Дополнительные параметры определяют пространство имен по умолчанию для WMI, которое используется в сценариях WMI в тех случаях, когда для объекта WMI не указан полный путь пространства имен. Эти параметры по умолчанию можно изменить, нажав кнопку **Изменить** (Change), выбрав новое пространство имен по умолчанию, а затем нажав кнопку **OK**.

> ***Примечание***
>
> Служба WMI содержит журналы ошибок, которые можно использовать для диагностирования возникающих в ней проблем. По умолчанию эти журналы хранятся в папке *%SystemRoot%*\System32\Wbem\Logs. Файлы технического обслуживания, журналы и хранилища службы WMI могут занимать значительный объем дискового пространства системы. В среднем, на тестовой системе автора эти файлы занимали 65 Мбайт дискового пространства, большая часть которого (40—50 Мбайт) уходила под файлы резервных копий хранилища статистических данных.

Собранные инструментарием WMI сведения хранятся в наборе системных файлов, называющемся *хранилищем* (repository). По умолчанию файлы хранилища размещаются в папке

%SystemRoot%\System32\Wbem\Repository. Хранилище является центром инструментария WMI и инфраструктуры служб справки и поддержки (Help and Support Services). Информация перемещается по хранилищу с помощью *файла размещения* (staging file). В случае повреждения данных хранилища или файла размещения, инструментарий WMI может работать с ошибками. Такая ситуация обычно является временной, но против нее можно предпринять предохранительные меры, выполняя ручное резервное копирование файлов хранилища.

Ручное резервное копирование хранилища WMI осуществляется следующим образом:

1. Откройте диалоговое окно свойств управляющего элемента WMI, перейдите в нем на вкладку **Архивация или восстановление**, а на ней нажмите кнопку **Архивировать**. В открывшемся диалоговом окне **Укажите имя файла архива** (Specify a name for your backup file) введите имя файла резервной копии базы данных WMI и выберите папку, в которой его сохранить. Нажмите кнопку **Сохранить** (Save), чтобы создать резервную копию.
2. Начнется процесс резервного копирования, в течение которого отображается окно **Выполняется архивация** (Backup in progress). Файл резервной копии имеет расширение rec, а его размер зависит от объема информации, находящейся в базе данных WMI. Обычно, размер этого файла будет 20—30 Мбайт.

Восстановление базы данных WMI из резервной копии выполняется таким образом:

1. Откройте диалоговое окно свойств управляющего элемента WMI, перейдите в нем на вкладку **Архивация или восстановление**, а на ней нажмите кнопку **Восстановить**. В открывшемся диалоговом окне **Укажите имя файла архива для восстановления** (Specify a backup file to restore) выберите папку и файл резервной копии базы данных WMI, из которого следует выполнять восстановление, а затем нажмите кнопку **Открыть**.
2. Начнется процесс восстановления, в течение которого отображается диалоговое окно **Восстановление** (Restore in progress), а по завершении выводится предупреждающее сообщение. Нажмите кнопку **OK** в окне сообщения.
3. Процесс восстановления базы данных WMI обрывает подключение к управляющему элементу WMI. Это подключение можно восстановить, закрыв, а затем снова открыв диалоговое окно свойств управляющего элемента WMI. Эта последовательность действий восстанавливает подключение управляющего элемента WMI к локальному или удаленному компьютеру, но может быть осуществлена только после завершения восстановления базы данных WMI.

> ***Примечание***
>
> Ошибка подключения обычно означает, что управляющий элемент WMI еще не завершил восстановление базы данных WMI. Подождите секунд 30—60 и повторите попытку.

Использование инструментов системной поддержки

Операционная система Windows 8 предоставляет широкий выбор средств поддержки, включая следующие.

- **Восстановление файлов Windows 7** (Windows 7 File Recovery). Исполняемый файл — sdclt.exe. Средство для создания резервной копии и восстановления пользовательских и системных файлов. Дополнительную информацию *см. в главе 10*.

- **Встроенные средства диагностики.** Позволяют выполнять сканирование системы, исследуя аппаратные компоненты и программные конфигурации на наличие проблем. Полученную с их помощью информацию можно использовать для поиска и устранения проблем производительности и конфигурации. Применение встроенных средств диагностики рассматривается в этой главе, а также в других главах этой книги.
- **Средство диагностики** DirectX (DirectX Diagnostic Tool). Исполняемый файл — dxdiag.exe. Технология DirectX используется для ускорения производительности приложений при условии, что аппаратные средства компьютера поддерживают ее.
- **Очистка диска** (Disk Cleanup). Исполняемый файл — cleanmgr.exe. Утилита для обнаружения и удаления с диска файлов, в которых больше нет надобности. По умолчанию утилита проверяет временные файлы, файлы в Корзине и разные типы автономных вебстраниц на возможность их удаления.
- **Оптимизация дисков** (Optimize drives). Исполняемый файл — dfrgui.exe. Утилита, которая исследует диски на наличие фрагментированных файлов и выполняет дефрагментацию и оптимизацию диска. Наличие на диске большого числа фрагментированных файлов может ухудшить производительность диска. Дополнительную информацию по этой утилите *см. в главе 12*.
- **Проверка подписи файла** (File Signature Verification). Исполняемый файл — sigverif.exe. Выполняет поиск системных файлов, не снабженных цифровой подписью. Список проверенных файлов сохраняется в файле журнала *%SystemRoot%*\Sigverif.txt.
- **Предложение удаленной помощи.** Позволяет предложить помощь удаленному пользователю в решение проблем с системой. Процесс поиска и устранения проблем на компьютере пользователя, принявшего предложение помощи, рассматривается в *главе 10*.
- **Запрос удаленной помощи.** Позволяет создать запрос для поиска и устранения проблем на локальном компьютере удаленным техником. Подробно процесс запроса удаленной помощи рассматривается в *главе 10*.
- **Конфигурация системы** (System Configuration). Средство для управления конфигурационными параметрами системы. Среди прочего, позволяет установить вариант запуска системы: обычный, диагностический или выборочный.
- **Восстановление системы** (System Restore). Исполняемый файл — rstrui.exe. Средство для создания точек восстановления системы и отката состояния системы до определенной точки восстановления. Утилита **Восстановление системы** рассматривается в *главе 10*.

Среди вышеперечисленных средств более близкого немедленного знакомства заслуживают утилиты **Очистка диска**, **Проверка подписи файла** и **Конфигурация системы**.

Использование утилиты *Очистка диска*

Утилита **Очистка диска** (Disk Cleanup) проверяет диски на наличие файлов, в которых больше нет надобности. Процедура работы с этой утилитой следующая:

1. Запустите утилиту, введя в поле поиска панели **Приложения** имя исполняемого файла утилиты `cleanmgr` и нажав клавишу <Enter>, или, альтернативно, щелкнув по значку утилиты на экране **Приложения**.
2. Для систем, оснащенных несколькими жесткими дисками, выводится диалоговое окно **Очистка диска: выбор устройства** (Drive Selection) для выбора очищаемого диска. В выпадающем списке **Диски** (Drives) выберите требуемый диск, а затем нажмите кнопку **OK**.

Утилита исследует выбранный диск на предмет пользовательских файлов, которые можно удалить, и файлов, подлежащих удалению. Чем больше файлов содержит диск, тем дольше занимает процесс поиска.

По завершению первоначальной проверки выводится окно **Очистка диска** (Disk cleanup) со списком категорий файлов, которые можно удалить. Этот список можно расширить, нажав кнопку **Очистить системные файлы** (Cleanup system files) внизу окна. Снова появится диалоговое окно выбора диска, а по завершению его проверки — слегка измененное окно **Очистка диска** для выбора файлов для удаления (рис. 2.8).

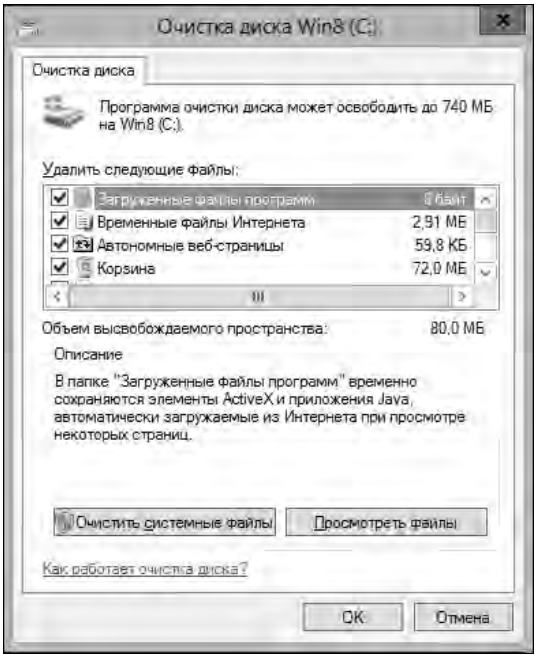


Рис. 2.8. Конечное окно **Очистка диска** со списком файлов, которые можно удалить

Список файлов, доступных для удаления, может включать следующие категории.

- **Загруженные файлы программ** (Downloaded Program Files). Содержит файлы, загружены для использования в браузере, такие как элементы управления ActiveX и апплеты Java. Это временные файлы, которые можно безопасно удалить.
- **Файлы обновлений Windows.** Файлы, сохраненные с предшествующей установки Windows, которые не были определены, как системные файлы Windows. После сохранения всех необходимых данных с предыдущих установок Windows, включая пользовательские данные, можно установить флажок этой категории, чтобы удалить эти файлы.
- **Очистка файла гибернации** (Hibernation File Cleaner). Содержит файл состояния компьютера при переходе в режим гибернации. Если на компьютере гибернация не применяется, этот файл можно безопасно удалить.
- **Временные файлы Microsoft Office** (Temporary Microsoft Office Files). Содержит временные файлы и журналы Microsoft Office. Эти файлы также можно удалить, чтобы высвободить место на диске.

- **Автономные файлы** (Offline Files). Содержит локальные копии сетевых файлов, выделенных для автономного использования. Эти файлы используются для автономной работы и их также можно удалить.
- **Автономные веб-страницы** (Offline webpages). Содержит локальные копии веб-страниц, выделенные для автономного использования. Эти файлы используются для автономной работы и их также можно удалить.
- **Предыдущие установки Windows** (Previous Windows Installations). Файлы предыдущих установок Windows, хранящиеся в папке *%SystemDrive%*\Windows.old. После сохранения всех необходимых данных с предыдущих установок Windows, включая пользовательские данные, можно установить флажок этой категории, чтобы удалить эти файлы.
- **Временные автономные файлы** (Temporary Offline Files). Содержит автоматически кэшируемые общие файлы. Эти файлы используются для автономной работы и их также можно удалить.
- **Корзина** (Recycle Bin). Содержит файлы, удаленные из файловой системы, но доступные для восстановления. Удаление этих файлов из Корзины полностью удаляет их с жесткого диска.
- **Временные файлы** (Temporary files). Основные временные файлы данных и приложений, хранящиеся в папке Temp.
- **Временные файлы Интернета** (Temporary Internet Files). Кэшированные веб-страницы, которые можно безопасно удалить.
- **Эскизы** (Thumbnails). Содержит эскизы рисунков, видео и документов, созданных в Windows 8. При первом обращении к папке Windows 8 создает эскизы содержащихся в ней рисунков, видео и документов. Эти эскизы сохраняются, чтобы не повторять процесс их создания при последующих обращениях к папке, ускорив таким образом их отображение. Удаленные эскизы создаются снова при следующем обращении к папке.

3. Для удаления файлов требуемой категории установите соответствующий флажок, а затем нажмите кнопку **OK**. При выводе запроса подтвердить удаление выбранных файлов нажмите кнопку **Да**.

Проверка системных файлов с помощью средства *Проверка подписи файла*

Критические файлы операционной системы снабжаются цифровой подписью. Цифровые подписи способствуют подтверждению аутентичности этих файлов и обеспечивают легкость в отслеживании изменений, которые могут вызвать проблемы в работе системы. При наличии проблем, причина которых не может быть с легкостью установлена, что случается, когда система становится нестабильной после установки приложения, будет хорошей идеей проверить, что критические системные файлы не были изменены. Такую проверку можно выполнить с помощью утилиты **Проверка подписи файла**.

Исполняемый файл этой утилиты называется Sigverif.exe. Процедура работы с утилитой проверки подписи файла следующая:

1. Введите команду `sigverif` в поле поиска панели **Приложения**, а затем нажмите клавишу <Enter>. Откроется главное окно утилиты **Проверка подписи файла** (рис. 2.9).
2. По умолчанию утилита проверки подписи файла отображает список системных файлов, которые не снабжены цифровой подписью, и сохраняет результаты проверки в файл

%SystemRoot%\System32\Sigverif.txt. Прежде чем проверять цифровые подписи файлов, может быть желательным задать параметры протоколирования. Для этого в окне утилиты нужно нажать кнопку **Дополнительно** (Advanced). Как показано на рис. 2.10, результаты проверки сохраняются в файл журнала sigverif.txt. Также, по умолчанию, результаты новой проверки заменяют результаты предыдущей.

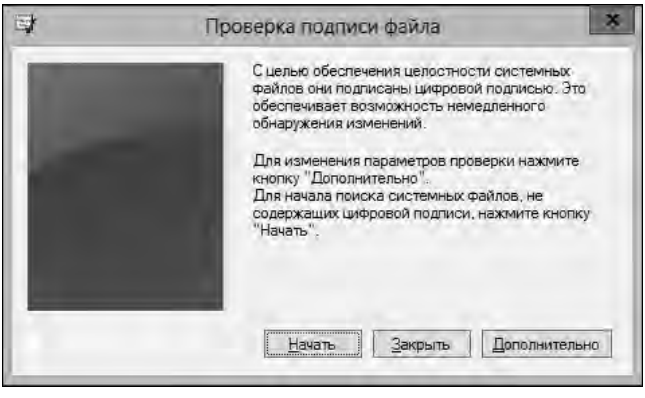


Рис. 2.9. Главное окно утилиты **Проверка подписи файла**

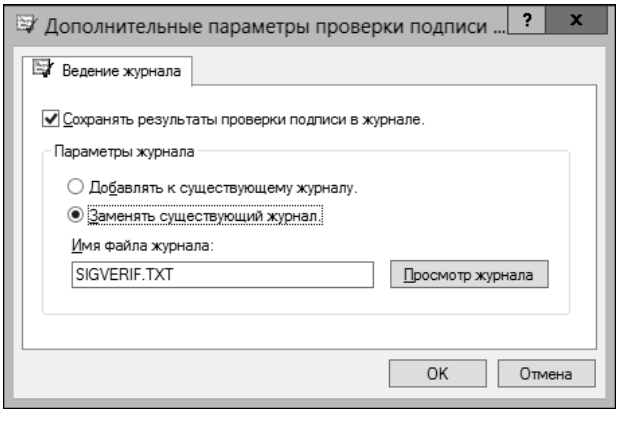


Рис. 2.10. Страница дополнительных параметров утилиты проверки подписи файлов

Чтобы упростить задачу отслеживания изменений файлов, результаты проверок лучше добавлять к предыдущим, вместо того чтобы заменять их. Установив требуемые параметры протоколирования, нажмите кнопку **OK**, чтобы сохранить их и возвратиться в главное окно утилиты.

3. Запустите утилиту на исполнение, нажав кнопку **Начать** (Start). По завершению работы утилиты обратите внимание на список файлов в ее отчете в окне **Результаты проверки подписи**. Эти файлы не снабжены цифровой подписью, и может быть, что они были заменены вредоносными программами с такими же именами. Нажмите кнопку **Закрыть** (Close), чтобы возвратиться в главное окно утилиты. При наличии подозрений на проблемы просмотрите журналы событий и другие журналы, чтобы увидеть, не встречаются ли какие-либо из этих файлов в отчетах об ошибках.
4. Для просмотра журнала проверки нажмите кнопку **Дополнительно** и на странице дополнительных параметров утилиты — кнопку **Просмотр журнала** (View Log). Журнал

утилиты, по умолчанию хранящийся в файле *%SystemRoot%*\System32\Sigverif.txt, можно также открыть с помощью программы Блокнот. Проверьте в журнале, не были ли какие-либо файлы изменены после их установки. Файлы в журнале обозначаются как **Подписано** (Signed) и **Не подписано** (Not signed). Обратите внимание на дату модификации и версию файла. Если с компьютером были проблемы, начиная с какой-либо определенной даты, и критические файлы были изменены этого же числа, то это может быть причиной проблемы. Например, возможно, была установлена программа, которая заменила критический файл его устаревшей версией.

Управление конфигурацией, запуском и загрузкой системы

Независимо от того, хотите ли вы обновить конфигурационные файлы системы или выяснить причину проблем с запуском системы, предпочитаемым инструментом для любой из этих задач должна быть утилита **Конфигурация системы** (System Configuration). Эта утилита представляет собой интегрированное средство для получения информации о параметрах системной конфигурации и управлении ими. С помощью этой утилиты можно управлять следующими элементами:

- параметрами запуска операционной системы;
- автоматически запускаемыми приложениями;
- параметрами автоматически запускаемых служб.

В последующих разделах рассматриваются ключевые задачи, которые можно выполнять с помощью утилиты **Конфигурация системы**. Исполняемый файл этой утилиты — Msconfig.exe. Запустить утилиту можно, введя команду `msconfig` в поле поиска панели **Приложения**, а затем нажав клавишу <Enter>.

Примечание

Утилиту **Конфигурация системы** можно также запустить с экрана **Приложения**, где она находится в разделе **Средства администрирования**.

Режимы запуска, поиск и устранение неполадок с запуском системы

С помощью утилиты **Конфигурация системы** можно выбрать один из следующих трех вариантов запуска компьютера.

- **Обычный запуск** (Normal startup). Применяется для использования системы в штатном порядке. При этом варианте запуска операционная система загружает все файлы системной конфигурации и драйверы устройств и запускает все автозагружаемые приложения и включенные службы.
- **Диагностический запуск** (Diagnostic startup). Применяется для поиска и устранения неполадок с системой. При диагностическом запуске загружаются только основные драйверы и запускаются лишь основные службы. Запустив систему в этом режиме, можно откорректировать параметры системы, чтобы разрешить проблемы конфигурации.
- **Выборочный запуск** (Selective startup). Применяется для точного определения проблемных областей конфигурации. При этом варианте запуска можно установить модифицированную конфигурацию загрузки и выборочно задать запуск определенных служб и программ автозагрузки. Это может помочь в определении параметров, вызывающих проблемы в работе системы, и исправить их.

Вариантом запуска по умолчанию является обычный. Другой вариант запуска, например для диагностирования проблем в работе системы, можно установить таким образом:

1. Запустите утилиту **Конфигурация системы**, введя в поле поиска панели **Приложения** имя исполняемого файла утилиты `msconfig` и нажав клавишу <Enter>, или, альтернативно, щелкнув по значку утилиты на экране **Приложения**.
2. На вкладке **Общие** окна утилиты (рис. 2.11) установите переключатель требуемого варианта запуска: **Диагностический запуск** или **Выборочный запуск**.

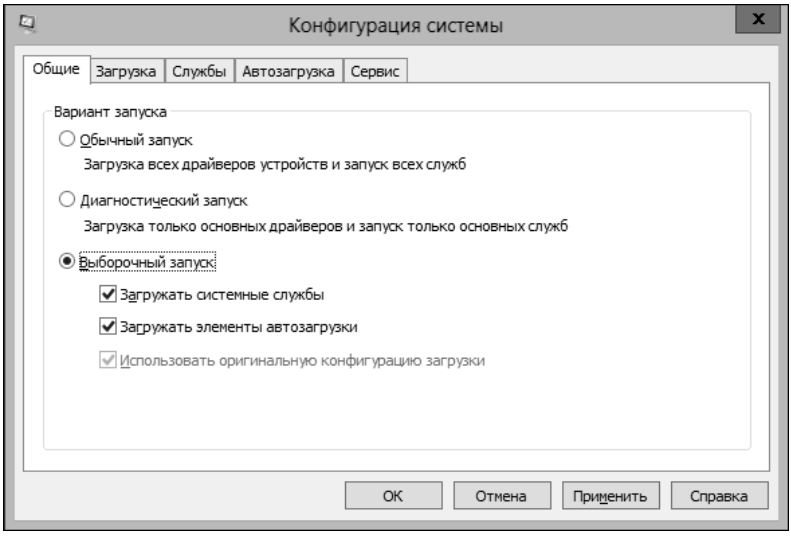


Рис. 2.11. Выбор варианта запуска на вкладки **Общие** утилиты **Конфигурация системы**

Для выборочного варианта запуска можно указать использование следующих элементов, установив соответствующие флажки:

- **Загружать системные службы** (Load system services). Системе дается указание загружать службы Windows. При установке этого флажка откройте вкладку **Службы** (Services) и укажите службы, которые следует загружать, установив их флажки;
- **Загружать элементы автозагрузки** (Load startup items). Системе дается указание запускать при загрузке программы автозапуска. При выборе этой опции можно выбрать требуемые программы автозапуска на вкладке **Автозагрузка** (Startup);
- **Использовать оригинальную конфигурацию загрузки** (Use original boot configuration). Системе дается указание при запуске обрабатывать первоначальную загрузочную конфигурацию вместо созданной посредством модифицирования параметров загрузки с помощью утилиты **Конфигурация системы**.

Примечание

Если изменить параметры на вкладках **Загрузка**, **Службы** или **Автозагрузка**, на вкладке **Общие** автоматически устанавливается переключатель **Выборочный запуск** и флажки соответствующих опций.

3. Установив нужную конфигурацию запуска, нажмите кнопку **OK**, а затем перезагрузите систему. В случае проблем при перезагрузке загрузите систему в безопасном режиме, а затем повторите эту процедуру. Опция загрузки в безопасном режиме предлагается автоматически после неудачной загрузки.

Изменение параметров загрузки

Для загрузки операционной системы Windows 8 не используются файл boot.ini и другие загрузочные файлы, применяемые для загрузки предыдущих версий Windows. Вместо этого для запуска операционной системы Windows 8 предназначен диспетчер загрузки Windows (Windows Boot Manager) и приложение загрузки. При диагностировании проблем с системой на вкладке **Загрузка** утилиты **Конфигурация системы** можно указать загрузочный раздел, метод загрузки и другие опции загрузки.

Как показано на рис. 2.12, на вкладке **Загрузка** утилиты конфигурирования системы отображаются операционные системы, которыми можно загрузить компьютер, и другие параметры загрузки.

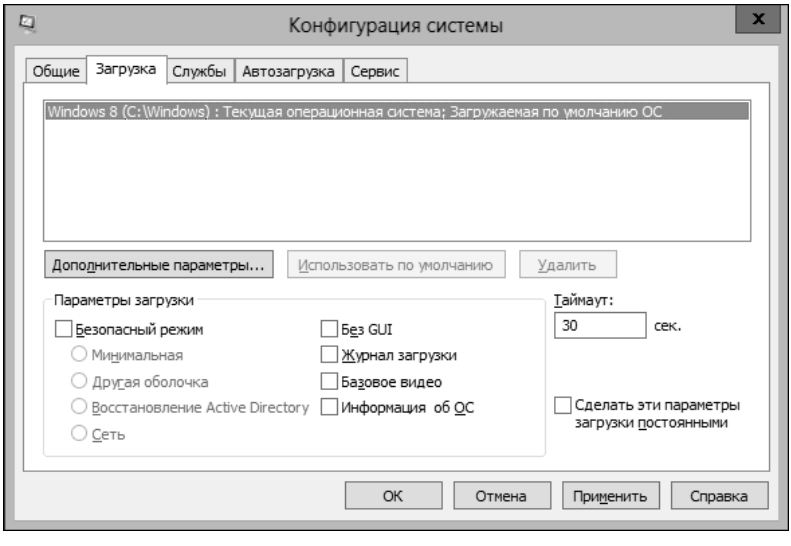


Рис. 2.12. Вкладка **Загрузка** содержит параметры для управления загрузочным разделом, методом загрузки и другими опциями загрузки

Чтобы указать для загрузки другую операционную систему, просто щелкните на ее названии в списке в верхней области вкладки. Для выбранной загружаемой операционной системы можно также задать следующие опции.

- **Использовать по умолчанию** (Set as default). Нажатие этой кнопки задает выбранный загрузочный раздел в качестве загрузочного раздела по умолчанию. Если загрузочный раздел не выбран в течение периода времени, заданного значением **Таймаут** (Timeout), автоматически выбирается загрузочный раздел по умолчанию.
- **Таймаут** (Timeout). Задает период времени для выбора загрузочного раздела, по истечении которого автоматически выбирается загрузочный раздел по умолчанию.
- **Удалить** (Delete). Удаляет выбранную операционную систему из списка доступных для загрузки систем. Восстановить в списке удаленную таким образом систему довольно проблематично, поэтому такое удаление следует выполнять только в случае крайней надобности.

Примечание

Если на компьютере установлена только одна операционная система, кнопки **Использовать по умолчанию** и **Удалить** будут отключены по причине отсутствия другой системы, которую можно было бы выбрать для загрузки. Подобным образом, если выбрана операционная система по

умолчанию, кнопка **Установить по умолчанию** будет недоступна, а если выбрана текущая операционная система, недоступной будет кнопка **Удалить**.

На вкладке **Загрузка** также можно установить следующие параметры загрузки.

- **Безопасный режим** (Safe boot). Установка этого флажка задает загрузку компьютера в безопасном режиме с возможностью задания дополнительных параметров: **Минимальная** (Minimal), **Сеть** (Net), **Другая оболочка** (Alternate shell), а также **Восстановление Active Directory** (Active Directory repair). Запустив систему в безопасном режиме, можно откорректировать параметры системы, чтобы разрешить проблемы конфигурации.
- **Без GUI** (No GUI boot). Компьютер загружается оболочкой командной строки Windows без загрузки графических компонентов операционной системы. Такой способ загрузки полезен при наличии проблем с графическими компонентами Windows 8.
- **Журнал загрузки** (Boot log). Включается протоколирование загрузки, когда основные события загрузки записываются в журнал.
- **Базовое видео** (Base video). Задает принудительное использование VGA-параметров для дисплея. Этот режим применяется при диагностировании проблем с дисплеем, например, когда установлено разрешение экрана, не поддерживаемое монитором.
- **Информация об ОС** (OS boot information). Загрузка операционной системы до загрузки графических компонентов выполняется с выводом сообщений о подробностях загрузки.

Утилита **Конфигурация системы** сохраняет все внесенные изменения в виде временных параметров загрузки. Для применения этих временных модифицированных параметров компьютер нужно перезагрузить. Чтобы возвратиться к обычным параметрам загрузки, на вкладке **Общие** утилиты нужно установить переключатель **Обычный запуск** и нажать кнопку **OK**. Опять же, для применения обычных параметров загрузки компьютер нужно перезагрузить.

На вкладке **Загрузка** также можно установить загрузочные параметры для количества процессоров, максимального объема памяти, блокировки PCI и отладки. Эти параметры задаются в диалоговом окне **Дополнительные параметры загрузки** (BOOT Advanced Options) (рис. 2.13), которое открывается нажатием кнопки **Дополнительные параметры** (Advanced options) на вкладке **Загрузка**.

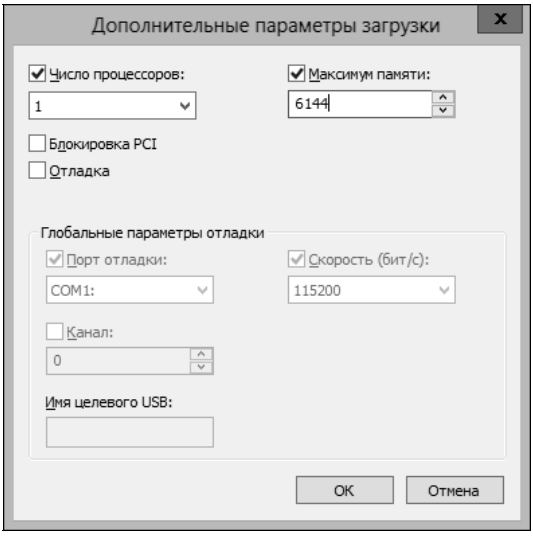


Рис. 2.13. Диалоговое окно для установки дополнительных параметров загрузки

Дополнительные параметры загрузки применяются для диагностирования проблем в работе системы. Например, если подозревается, что проблема может быть связана с использованием нескольких процессоров, можно задать применение только одного процессора. А если подозревается проблема с использованием памяти свыше 4 Гбайт, можно задать объем памяти в 4096 Мбайт. После выяснения причины проблемы и ее устранения флажки с этих параметров нужно снять, чтобы восстановить работу компьютера с обычными параметрами.

Чтобы сделать выбранные на вкладке **Загрузка** обычные или дополнительные параметры загрузки постоянными, установите на ней флажок **Сделать эти параметры загрузки постоянными** (Make all boot settings permanent) перед тем, как нажимать кнопку **OK**. Но в большинстве случаев параметры, выбранные для поиска причин неполадки или для отладки, нежелательно использовать для обычной работы компьютера, поэтому сначала следует выполнить сброс этих параметров.

Включение и отключение приложений автозагрузки для диагностирования проблем

При наличии подозрений, что запускаемое автоматически при загрузке приложение является причиной проблемы в работе системы, существует легкий способ установить, действительно ли это так. Для этого нужно просто заблокировать автоматический запуск программ при загрузке и перезагрузить компьютер. Если это устраняет проблему, тогда ее причиной, возможно, была одна из автоматически запускаемых программ, и далее можно установить, какая именно, и убрать ее из списка автоматически запускаемых программ.

Временно отключить автоматический запуск программ при загрузке можно таким образом:

1. Запустите утилиту **Конфигурация системы**, введя в поле поиска панели **Приложения** имя исполняемого файла утилиты `msconfig` и нажав клавишу <Enter>, или, альтернативно, щелкнув по значку утилиты на экране **Приложения**.
2. На вкладке **Общие** установите переключатель **Выборочный запуск**, сбросив при этом флажок **Загружать элементы автозагрузки**, а затем нажмите кнопку **OK**. Чтобы проверить полученный эффект, перезагрузите компьютер. Если проблема больше не проявляется, то ее причина была изолирована к одному (или нескольким) приложению автозагрузки.

Опция выборочной загрузки является одноразовой, поэтому при следующей загрузке компьютера приложения автозапуска будут запущены. Теперь нужно определить, какая именно из программ автозагрузки является причиной проблемы. Для этого используется диспетчер задач, запустить который можно введя команду `taskmgr` в поле поиска панели **Приложения** или нажав комбинацию клавиш <Ctrl>+<Alt>+<Delete>. Еще один способ запустить диспетчер задач — это щелкнуть правой кнопкой мыши в левом нижнем углу экрана и в открывшемся контекстном меню выбрать команду **Диспетчер задач**.

Вкладка **Автозагрузка** окна диспетчера задач содержит список всех приложений, настроенных на автоматический запуск при загрузке компьютера. Можно попробовать последовательно отключать приложения и перезагружать компьютер, чтобы посмотреть, устранит ли это проблему. Чтобы отключить приложение автозапуска, выберите его в списке приложений, а затем нажмите кнопку **Отключить** (Disable) в правом нижнем углу окна диспетчера задач. Если определить какое-либо из приложений как причину проблемы таким образом не получится, то причина может крыться в каком-либо компоненте или службе Windows либо драйвере устройства.

Осторожно!

Отключайте только те программы, которые подозреваются, как потенциальный источник проблемы, и только в том случае, если вы знаете, каким образом они используются операционной системой. Если вы не знаете, в чем заключается функция программы, не отключайте ее. Иногда дополнительные сведения о программе автозапуска можно узнать, проследив путь ее исполняемого файла, а затем исследовав папку, в которой она установлена.

Включение и отключение служб для диагностирования проблем

Подобно тому, как программы автозапуска могут вызывать проблемы в работе системы, это могут делать и автоматически запускаемые службы. Поэтому при диагностировании проблем в работе компьютера можно временно поочередно отключать службы, а затем перезагружать компьютер, чтобы посмотреть, продолжает ли проблема проявляться. Если после отключения очередной службы проблема больше не повторяется, то ее причиной, возможно, является эта служба. В качестве решения проблемы данную службу можно отключить постоянно или же связаться с ее поставщиком и узнать, нет ли более новой версии исполняемого файла этой службы.

Временное отключение служб выполняется следующим образом:

1. Запустите утилиту **Конфигурация системы**, введя в поле поиска панели **Приложения** имя исполняемого файла утилиты `msconfig` и нажав клавишу <Enter>, или, альтернативно, щелкнув по значку утилиты на экране **Приложения**.
2. В открывшемся окне утилиты выберите вкладку **Службы** (Services). Как показано на рис. 2.14, эта вкладка содержит список всех установленных на компьютере служб с указанием их состояния, т. е. **Остановлена** (Stopped) или **Работает** (Running), и источника. Облегчить поиск служб поставщиков иных, чем корпорация Microsoft, можно, установив флажок **Не отображать службы Майкрософт** (Hide all Microsoft services).
3. Сбросьте флажок одной или нескольких служб, которые не следует запускать при загрузке компьютера.

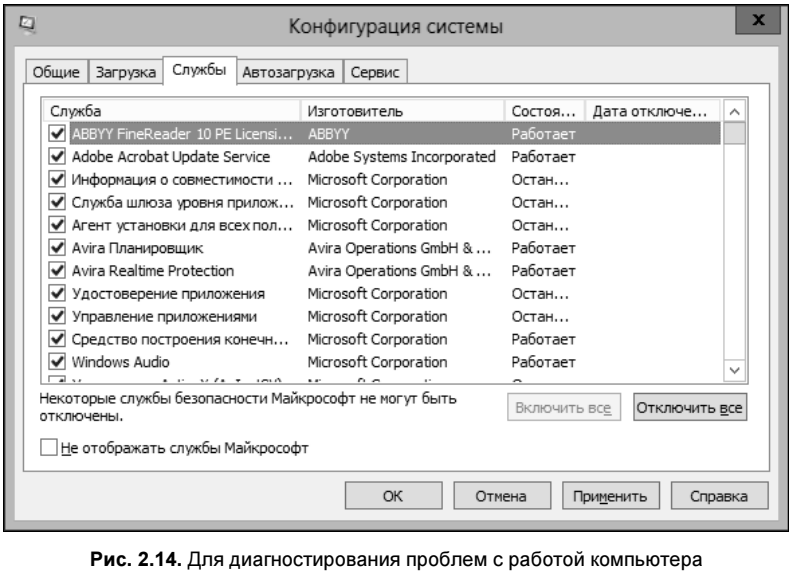


Рис. 2.14. Для диагностирования проблем с работой компьютера можно отключать установленные на нем службы

Осторожно!

Отключайте только те службы, которые подозреваются, как потенциальный источник проблемы, и только в том случае, если вы знаете, каким образом они используются операционной системой. Если вы не знаете, в чем заключается функция службы, не отключайте ее. Вкладка **Службы** утилиты **Конфигурация системы** не предоставляет никакой дополнительной информации об отображаемых на ней службах. Назначение служб можно выяснить с помощью оснастки **Службы** консоли **Управление компьютером**. Для этого выберите в этой оснастке требуемую службу и ознакомьтесь с ее описанием в правой панели на вкладке **Расширенный** (Extended). Альтернативно, можно открыть окно свойств требуемой службы, дважды щелкнув по ней мышью на любой из вкладок (**Расширенный** или **Стандартный**), и ознакомиться с ее описанием на вкладке **Общие** этого окна.

4. Нажмите кнопку **OK**. Чтобы проверить эффект внесенных изменений, нужно перезагрузить систему, поэтому при запросе перезагрузки нажмите кнопку **Да** или перезагрузите систему вручную.
5. Повторяйте эту процедуру, сколько потребуется, чтобы изолировать службу, являющуюся причиной проблемы. Если определить какую-либо из служб как причину проблемы таким образом не получится, то причина может крыться в каком-либо компоненте Windows, приложении автозагрузки или драйвере устройства.

Управление свойствами системы

Для управления свойствами системы используется диалоговое окно **Свойства системы** (System Properties). Ключевые области операционной системы, которые можно конфигурировать с помощью этого диалогового окна, рассматриваются в последующих разделах этой главы.

Вкладка *Имя компьютера*

Сетевое имя компьютера можно просмотреть и изменить на вкладке **Имя компьютера** диалогового окна **Свойства системы** (рис. 2.15).

На вкладке **Имя компьютера** отображается полное имя компьютера и его членство в домене или группе. Полное имя компьютера является, по сути, DNS-именем компьютера, которое также определяет местонахождение компьютера в иерархии Active Directory.

Быстрым способом открыть диалоговое окно **Свойства системы** будет щелкнуть правой кнопкой в левом нижнем углу экрана **Пуск** или рабочего стола, в открывшемся контекстном меню выбрать пункт **Система**, а в левой панели открывшегося окна **Система** щелкнуть на ссылке **Дополнительные параметры системы** (Advanced system settings). Альтернативно, можно ввести имя исполняемого файла (sysdm.cpl) в поле поиска панели **Приложения** и нажать клавишу <Enter>.

На вкладке **Имя компьютера** диалогового окна **Свойства системы** можно выполнять следующие задания:

- *присоединить компьютер к рабочей группе.* Нажатие кнопки **Идентификация** (Network ID) запускает мастер присоединения компьютера к домену или рабочей группе, который руководит процессом модифицирования параметров компьютера для доступа к сети;
- *изменить имя компьютера.* Нажатие кнопки **Изменить** открывает диалоговое окно, в котором компьютеру можно присвоить другое имя и/или изменить домен либо группу компьютера.

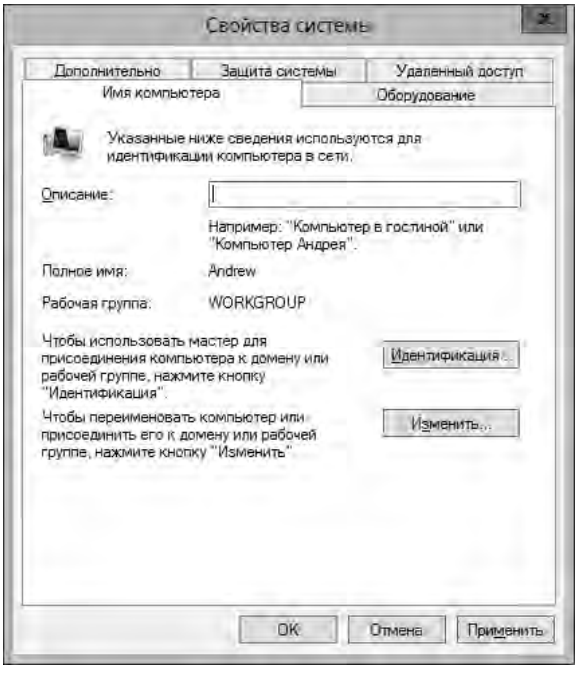


Рис. 2.15. Вкладка **Имя компьютера** диалогового окна **Свойства системы**

Практический совет

Прежде чем пытаться присоединить компьютер к домену, убедитесь в правильности IP-параметров, включая параметры DNS, для сети, к которой подключается компьютер. Чтобы клиентский компьютер мог использовать службу DNS, он должен иметь соответствующее имя компьютера и должным образом сконфигурированный DNS-суффикс. Вместо использования произвольных или своеобразных имен следует разработать схему назначения имен, которые имеют смысл как для пользователей, так и для администраторов. В системе DNS имя компьютера служит именем его хоста, а основной DNS-суффикс определяет домен, к которому он принадлежит для целей разрешения имени. Разрешение всех неполных имен хостов осуществляется по основному DNS-суффиксу. Например, если на компьютере с основным DNS-суффиксом **tech.cpandl.com** выполнить команду `ping CorpSvr28`, этот запрос будет направлен по адресу **corpsvr28.tech.cpandl.com**.

По умолчанию основным DNS-суффиксом компьютера выступает домен, членом которого он является. При необходимости основной DNS-суффикс компьютера можно изменить. Например, если основной DNS-суффикс компьютера — **seattle.tech.cpandl.com**, чтобы упростить разрешение его имени в этой обширной DNS-иерархии, этот суффикс можно изменить на простой **cpandl.com**. Чтобы изменить основной DNS-суффикс компьютера, нажмите кнопку **Изменить** на вкладке **Имя компьютера**, в открывшемся диалоговом окне нажмите кнопку **Дополнительно** (More), в следующем диалоговом окне в текстовое поле введите новый основной DNS-суффикс, а затем закройте все открытые диалоговые окна, нажимая их кнопки **OK**.

Вкладка *Оборудование*

Вкладка **Оборудование** (Hardware) диалогового окна **Свойства системы** предоставляет доступ к диспетчеру устройств и диалоговому окну параметров установки устройств.

Чтобы открыть диалоговое окно **Свойства системы**, щелкните правой кнопкой мыши в левом нижнем углу экрана **Пуск** или рабочего стола, в открывшемся контекстном меню выберите пункт **Система**, а в левой панели открывшегося окна **Система** щелкните по ссыл-

ке **Дополнительные параметры системы** (Advanced system settings). Параметры, которые можно настраивать на вкладке **Оборудование**, включают параметры установки устройств.

При подключении к компьютеру нового устройства Windows 8 автоматически выполняет проверку на наличие для него драйверов, используя для этого функциональность обновления Windows (Windows Update). Эту функциональность можно настраивать в зависимости от требований пользователя. Для этого на вкладке **Оборудование** нужно нажать кнопку **Параметры установки устройств** и в открывшемся диалоговом окне установить один из переключателей — **Да, делать это автоматически** (Yes, do this automatically) или **Нет, предоставить возможность выбора** (No, let me choose what to do), после чего сохранить измененные настройки, нажав кнопку **OK**.

Примечание

Кнопка **Диспетчер устройств** окна **Свойства системы** открывает диспетчер устройств в консоли MMC[1]. Диспетчер устройств, который также включен в виде оснастки MMC в консоль **Управление компьютером**, рассматривается в *главе 9*.

Вкладка *Дополнительно*: параметры быстродействия

Вкладка **Дополнительно** диалогового окна **Свойства системы** предоставляет доступ к управлению многими ключевыми аспектами операционной системы Windows, включая производительность приложений, использование виртуальной памяти, профили пользователей, переменные среды и загрузку и восстановление системы.

Параметры производительности являются подмножеством расширенных конфигурационных параметров, настройка которых выполняется в диалоговом окне **Параметры быстродействия** (Performance Options). Это диалоговое окно можно открыть следующим образом:

1. В Панели управления щелкните по ссылке категории **Система и безопасность** (System and Security) и в открывшемся списке элементов этой категории выберите ссылку **Система**.
2. В левой панели окна **Система** щелкните по ссылке **Дополнительные параметры системы** (Advanced system settings).
3. Наконец, в открывшемся окне **Свойства системы** выберите вкладку **Дополнительно** и в разделе **Быстродействие** (Performance) этой вкладки нажмите кнопку **Параметры** (Settings), вследствие чего откроется диалоговое окно **Параметры быстродействия** (Performance Options).

А самым прямым и быстрым способом открыть это диалоговое окно будет ввести в поле поиска панели **Приложения** команду `systempropertiesperformance` и нажать клавишу <Enter>.

Настройка быстродействия Windows

В интерфейс Windows 8 было добавлено много графических улучшений, включая такие, как визуальные эффекты для меню, панелей инструментов, окон и панели задач. Но эти улучшения влияют на производительность Windows и при необходимости их можно настраивать согласно требованиям пользователя в диалоговом окне **Параметры быстродействия**.

[1] Microsoft Management Console — консоль управления Microsoft.

По умолчанию, при открытии этого окна выбирается вкладка **Визуальные эффекты** (Visual Effects), в которой предоставляются следующие варианты настройки визуальных эффектов.

- **Восстановить значения по умолчанию** (Let Windows choose what's best for my computer). Выбор параметров быстродействия предоставляется операционной системе, в зависимости от конфигурации оборудования. На новых компьютерах установка этого переключателя будет, скорее всего, равносильна выбору опции **Обеспечить наилучший вид** (Adjust for best appearance). Но ключевая разница состоит в том, что эта опция выбирается операционной системой на основе доступного оборудования и его технических возможностей.
- **Обеспечить наилучший вид** (Adjust for best appearance). Настройка Windows для получения наилучшего вида состоит в разрешении всех визуальных эффектов для всех графических интерфейсов. В частности, в меню и панелях инструментов применяются визуальные переходы и тени, сглаживаются неровности экранных шрифтов, выполняется плавная прокрутка элементов списков, для папок применяются веб-представления и много другое.
- **Обеспечить наилучшее быстродействие** (Adjust for best performance). Оптимизация Windows для наилучшего быстродействия заключается в отключении ресурсоемких визуальных эффектов, таких как скользящие переходы и сглаживание экранных шрифтов, но при этом обеспечиваются базовые визуальные эффекты.
- **Особые эффекты** (Custom). Установка этого переключателя позволяет самостоятельно выбирать визуальные эффекты из предоставленного списка эффектов. Если не выбрать никакой опции, в системе не будет использоваться никаких визуальных эффектов.

Завершив настройку визуальных эффектов, нажмите кнопку **Применить** (Apply), чтобы сохранить настройки, а затем дважды кнопку **OK**, чтобы позакрывать открытые диалоговые окна.

Настройка быстродействия приложений

Быстродействие приложений связано с установкой для Windows 8 параметров распределения времени процессора. Распределение времени процессора определяет быстроту реагирования приложений, исполняющихся в интерактивном режиме (в отличие от приложений, которые могут исполняться в системе в фоновом режиме как службы). Управление быстродействием приложений осуществляется путем настройки параметров на вкладке **Дополнительно** диалогового окна **Параметры быстродействия** (открыть которое можно, выполнив команду `systempropertiesperformance` в поле поиска панели **Приложения**, утилите **Выполнить**, командной строке или Windows PowerShell).

Раздел **Распределение времени процессора** (Processor scheduling) этой вкладки позволяет выбрать оптимизацию одного из следующих видов приложений.

- **Программ.** Установка этого переключателя предоставляет большую часть времени процессора программам, что улучшает их время отклика. Обычно эта опция выбирается для рабочих станций Windows 8.
- **Служб, работающих в фоновом режиме** (Background services). Установка этого переключателя распределяет время процессора в пользу исполняющихся в фоновом режиме служб, улучшая их время отклика. Обычно эта опция выбирается для компьютеров с Windows 8, работающих в качестве серверов, т. е. имеющих серверные роли и не использующихся, как рабочие станции. Например, компьютер может использоваться как сервер печати для обслуживания всех запросов печати отдела.

Установив требуемую опцию, сохраните настройки, нажав кнопку **Применить**.

Настройка виртуальной памяти

Виртуальная память позволяет расширить оперативную память (RAM), используя в этом качестве дисковое пространство посредством технологии, называющейся *подкачкой страниц* (paging). Суть этой технологии заключается в том, что на жестком диске создается специальный файл, называющийся *файлом подкачки* (paging file), в который из оперативной памяти записываются данные, не использующиеся в настоящий момент. Когда в данных возникает надобность, они снова возвращаются в память, возможно, вытесняя при этом на жесткий диск другой блок данных.

Первоначальный файл подкачки создается автоматически на жестком диске, на котором установлена операционная система. По умолчанию файлы подкачки для других дисков не создаются, поэтому, если в этом есть надобность, их нужно создавать вручную. При создании файла подкачки для него задается исходный и максимальный размеры. В Windows 8 файл подкачки называется pagefile.sys.

> ***ПРАКТИЧЕСКИЙ СОВЕТ***
>
> Обычно в Windows 8 размер файла подкачки устанавливается как минимум вдвое больше общего объема физической памяти, установленной на компьютере. Это помогает избежать фрагментации файла подкачки, что может вызвать падение производительности системы. При ручном управлении виртуальной памятью фрагментацию файла подкачки можно уменьшить, установив его исходный размер равным как минимум общему объему физической памяти. При объеме установленной оперативной памяти равным 4 Гбайт или меньше максимальный размер файла подкачки должен быть, по крайней мере, вдвое больше объема оперативной памяти. При объеме установленной оперативной памяти больше, чем 4 Гбайт, максимальный размер файла подкачки должен быть, по крайней мере, в полтора раза больше объема физической памяти (или таким, как рекомендуется производителем компьютера). Это способствует поддержке целостности файла и записи в него данных в виде смежных блоков (если это возможно при доступном объеме тома).

Настройка виртуальной памяти выполняется следующим образом:

1. Откройте диалоговое окно **Параметры быстродействия**. Одним из способов открытия этого окна будет ввод команды `systempropertiesperformance` в поле поиска панели **Приложения** и нажатие клавиши <Enter>.
2. На вкладке **Дополнительно** этого окна нажмите кнопку **Изменить** (Change), вследствие чего откроется диалоговое окно **Виртуальная память** (Virtual Memory) (рис. 2.16).

   В этом окне предоставляется следующая информация.

   - **Диск [метка тома]** и **Файл подкачки (МБ)** (Drive [Volume Label] и Paging File Size (MB)). Информация о текущих настройках виртуальной памяти системы. Для каждого тома указывается его файл подкачки (если имеется). Диапазон размера файла подкачки указывает его исходный и максимальный размеры.
   - **Общий объем файла подкачки на всех дисках** (Total paging file size for all drives). Этот раздел содержит информацию о рекомендуемом объеме виртуальной памяти для системы и текущем выделенном объеме. Обратите внимание на то обстоятельство, что (в большинстве случаев) для системного диска уже был выделен рекомендуемый объем файла подкачки, на что указывает установленный переключатель **Размер по выбору системы** (System managed size).
3. По умолчанию Windows 8 управляет размером файла подкачки для всех дисков. Для ручного управления виртуальной памятью сбросьте флажок **Автоматически выбирать объем файла подкачки** (Automatically manage paging file size for all drives).
4. В списке дисков выберите диск, для которого нужно настроить файл подкачки.

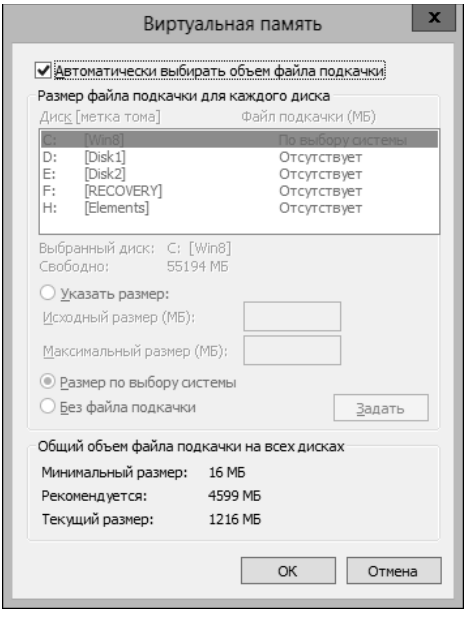


Рис. 2.16. Диалоговое окно **Виртуальная память** для настройки параметров файла подкачки

5. Установите переключатель **Указать размер** (Custom size) и введите значения для исходного и максимального размеров файла подкачки.
6. Нажмите кнопку **Задать** (Set), чтобы применить заданные параметры.
7. Выполните шаги 4—6 для каждого тома, который нужно настроить.
8. По завершению настройки нажмите кнопку **OK**. В случае вывода окна с запросом, затереть ли старый файл pagefile.sys новым, нажмите в нем кнопку **Да**.
9. При изменении параметров файла подкачки, используемого в настоящее время, выводится сообщение о необходимости перезагрузить компьютер, чтобы внесенные изменения вступили в силу. Нажмите кнопку **OK**.
10. Закройте все открытые диалоговые окна, последовательно нажимая в них кнопку **OK**. При закрытии окна **Свойства системы** выводится сообщение, что для применения внесенных изменений компьютер нужно перезагрузить.

Настройка Windows 8 на автоматическое управление виртуальной памятью выполняется следующим образом:

1. На вкладке **Дополнительно** диалогового окна **Параметры быстродействия** нажмите кнопку **Изменить**, чтобы открыть диалоговое окно **Виртуальная память**.
2. Установите в этом окне флажок **Автоматически выбирать объем файла подкачки**.
3. Закройте все открытые диалоговые окна, последовательно нажимая в них кнопку **OK**.

Совет

В качестве меры безопасности при выключении компьютера рекомендуется удалять содержимое файла подкачки. Настроить это действие можно следующим образом: в Панели управления откройте папку **Администрирование**, а из нее запустите консоль **Локальная политика безопасности**. В левой панели консоли разверните узел **Локальные политики** и выберите в нем подузел **Параметры безопасности**. Теперь в правой панели консоли дважды щелкните на политике **Завершение работы: очистка страничного файла виртуальной памяти** и в открывшемся окне свойств установите переключатель **Включить**.

Настройка предотвращения выполнения данных

Предотвращение выполнения данных (Data Execution Prevention, DEP) представляет собой функциональность защиты памяти. При задействовании этой функциональности процессор помечает все адреса памяти приложения как неисполняемые, если только данный адрес явно не содержит исполняемый код. При попытке исполнения кода на странице памяти, помеченной как неисполняемая, процессор порождает исключение, не допуская исполнения этого кода. Таким образом предотвращается проникновение вредоносного кода, такого как вирус, в большинство областей памяти, т. к. только определенные области памяти помечены, как содержащие исполняемый код.

> ***Примечание***
>
> 32-разрядные версии Windows поддерживают возможность DEP в том виде, в каком она реализуется процессорами AMD[1], которые предоставляют возможность No Execute (NX) для защиты страниц памяти. Такие процессоры поддерживают соответствующие инструкции и должны работать в режиме PAE[2] для поддержки конфигураций памяти больших объемов. 64-разрядные версии Windows также поддерживают возможность NX, но для поддержки конфигураций памяти больших объемов им не требуется работать в режиме PAE.

Для поддержки возможности DEP приложение должно обладать возможностью явно помечать память разрешением на исполнение. Приложения, не обладающие такой способностью, несовместимы с возможностью NX. Если при задействовании функциональности DEP возникают проблемы с памятью при исполнении приложений, следует выявить приложения, исполнение которых вызывает эти проблемы, и исключить их из действия DEP, вместо того чтобы полностью отключить эту возможность. Таким образом, система будет получать защиту предотвращения исполнения, за исключением тех программ, исполнение которых должным образом с применением этой возможности вызывает проблемы.

Защита предотвращения исполнения применяется как к пользовательским программам, так и программам, исполняющимся в режиме ядра. Срабатывание защиты при исполнении пользовательской программы генерирует исключение `STATUS_ACCESS_VIOLATION`. В большинстве процессов это исключение не обрабатывается и вызывает завершение исполнения процесса. Это требуемое поведение, т. к. большинство программ, нарушающих эти правила, будут вредоносными, такими как вирус или червь.

В отличие от приложений, защиту предотвращения исполнения нельзя выборочно включать или отключать для драйверов устройств, исполняющихся в режиме ядра. Кроме этого, на совместимых 32-разрядных системах защита предотвращения исполнения по умолчанию применяется к стеку. На совместимых 64-разрядных системах защита предотвращения исполнения по умолчанию применяется к стеку, нерезидентному пулу (paged pool) и пулу сеансов. Нарушение защиты предотвращения исполнения для драйвера устройства вызывает исключение `ATTEMPTED_EXECUTE_OF_NOEXECUTE_MEMORY`.

Узнать, поддерживает ли компьютер возможность DEP, можно с помощью утилиты **Система**. Если компьютер поддерживает DEP, выполнить ее настройку можно следующим образом:

1. Откройте диалоговое окно **Параметры быстродействия**. Один из способов открыть это окно — ввести команду `systempropertiesperformance` в поле поиска панели **Приложения** и нажать клавишу <Enter>.

---

[1] Компания Advanced Micro Devices.

[2] Physical Address Extension — расширение физических адресов.

2. Поддерживает ли процессор данного компьютера предотвращение исполнения, указывается внизу вкладки **Предотвращение выполнения данных**. В частности, для совместимых процессоров здесь содержится текст **Процессор этого компьютера имеет аппаратную поддержку DEP** (Your computer's processor supports hardware-based DEP).
3. Если процессор компьютера поддерживает предотвращение выполнения данных и эта возможность включена в микропрограммном обеспечении компьютера, возможность DEP можно настроить, используя следующие параметры.

   - **Включить DEP только для основных программ и служб Windows** (Turn on DEP for essential Windows programs and services only). Установка этого переключателя включает возможность DEP только для служб, программ и компонентов операционной системы. Этот параметр устанавливается по умолчанию, и его применение рекомендуется для компьютеров, которые поддерживают предотвращение выполнения данных и настроены должным образом.
   - **Включить DEP для всех программ и служб, кроме выбранных ниже** (Turn on DEP for programs except those I select). Применяет возможность DEP ко всем программам, за исключением указанных пользователем программ. При выборе этой опции для добавления исключенных из нее программ нужно нажать кнопку **Добавить** (Add), а затем в окне навигации по файловой системе указать исполняемый файл программы, подлежащей исключению. Таким образом, возможность предотвращения исполнения будет применяться ко всем программам, за исключением тех, которые указаны в списке.
4. Нажмите кнопку **OK**, чтобы применить настройки.

Вкладка *Дополнительно*: переменные среды

Настройка пользовательских и системных переменных среды выполняется с помощью диалогового окна **Переменные среды** (Environment Variables), показанного на рис. 2.17.

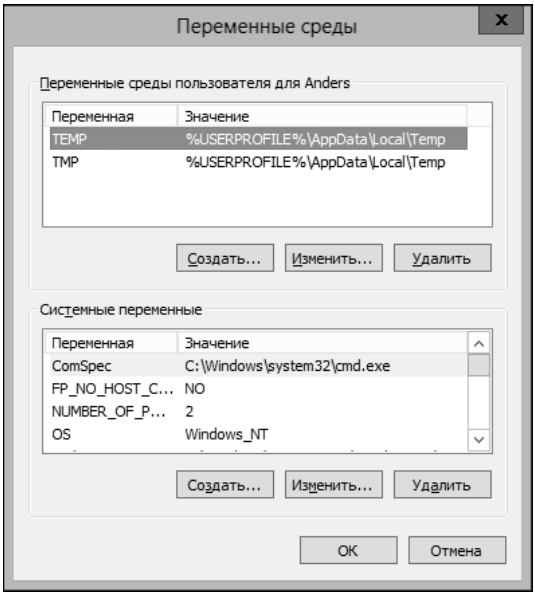


Рис. 2.17. Диалоговое окно **Переменные среды** для настройки пользовательских и системных переменных среды

Это диалоговое окно можно открыть следующим образом:

1. В Панели управления щелкните по ссылке категории **Система и безопасность** (System and Security) и в открывшемся списке элементов этой категории выберите ссылку **Система**.
2. В левой панели окна **Система** щелкните по ссылке **Дополнительные параметры системы** (Advanced system settings).
3. На вкладке **Дополнительно** открывшегося диалогового окна **Свойства системы** нажмите кнопку **Переменные среды**.

Примечание

Другой, более быстрый, способ открытия этого окна — это открыть окно **Свойства системы**, выполнив команду `systempropertiesadvanced` в поле поиска панели **Приложения**, а затем на вкладке **Дополнительно** этого окна нажать кнопку **Переменные среды**.

Создание переменной среды

Созданные или модифицированные системные переменные среды начинают действовать после перезагрузки компьютера, а пользовательские — после следующего входа данного пользователя в систему.

Переменную среды можно создать, выполнив следующую процедуру:

1. Откройте диалоговое окно **Переменные среды** одним из описанных ранее способов.
2. Нажмите кнопку **Создать** (New) под полем **Переменные среды пользователя** (User variables) или под полем **Системные переменные** (System variables) в зависимости от типа создаваемой переменной среды. Откроется диалоговое окно **Новая пользовательская переменная** (New User Variable) или **Новая системная переменная** (New System Variable) соответственно.
3. Введите имя и значение переменной в соответствующие поля, а затем нажмите кнопку **OK**, чтобы сохранить ее.

Практический совет

Путь к исполняемому файлу команд задается посредством переменной среды `PATH`. Редактирование этой переменной рассматривается в *разд. "Управление списком путей к командам" главы 8*.

Дополнительная информация

Профили пользователей содержат информацию о глобальных пользовательских параметрах и конфигурации. Они создаются при первом входе пользователя на локальный компьютер или домен и отличаются от локальных и доменных учетных записей. Профиль пользователя содержит среду рабочего стола, чтобы она была одной и той же при каждом входе пользователя в систему. Профили пользователей подробно рассматриваются в *главе 11 "Managing Existing User and Group Accounts"* книги "Windows Server 2012 Pocket Consultant"[1].

На компьютерах домена переменные среды можно создавать с помощью редактора управления групповыми политиками (Group Policy Management Editor) в узле **Настройка** (Preferences) посредством следующей процедуры:

1. В редакторе управления групповыми политиками откройте для редактирования объект групповой политики. Для настройки параметров компьютера разверните узел **Конфигу-**

[1] William R. Stanek. Windows Server 2012 Pocket Consultant. — Microsoft Press, 2012.

рация компьютера\Настройка\Конфигурация Windows (Computer Configuration\Preferences\Windows Settings) и выберите узел **Среда** (Environment). Для настройки параметров пользователя разверните узел **Конфигурация пользователя\Настройка\ Конфигурация Windows** (User Configuration\Preferences\Windows Settings) и выберите узел **Среда** (Environment).

2. Щелкните на узле **Среда** правой кнопкой мыши, выберите в контекстном меню команду **Создать** (New), а затем команду **Переменные среды** (Environment Variable). Откроется диалоговое окно **Новые свойства среды** (New Environment Properties).
3. В списке **Действие** (Action) выберите опцию **Создать** (Create). Далее выберите опцию **Пользовательская переменная** (User Variable) или **Системная переменная** (System Variable), чтобы создать пользовательскую или системную переменную соответственно.
4. В поля **Имя** и **Значение** введите имя и значение переменной соответственно.
5. Для управления способом применения настройки используются опции на вкладке **Общие параметры** (Common). Как правило, новую переменную нужно создать только один раз. В таких случаях устанавливается флажок **Применить один раз и не применять повторно** (Apply once and do not reapply).
6. Нажмите кнопку **OK**, чтобы сохранить настройку. При следующем обновлении политики элемент настройки будет применен должным образом к объекту групповой политики, для которого он был определен.

Редактирование переменной среды

Переменную среды можно редактировать, используя следующую процедуру:

1. Откройте диалоговое окно **Переменные среды** одним из описанных ранее способов.
2. Выберите требуемую переменную в поле **Переменные среды пользователя** или **Системные переменные**.
3. Нажмите кнопку **Изменить** (Edit) под полем **Переменные среды пользователя** или под полем **Системные переменные** (System variables) в зависимости от типа выбранной переменной среды. Откроется диалоговое окно **Изменение пользовательской переменной** (Edit User Variable) или **Изменение переменной среды** (Edit System Variable) в зависимости от типа выбранной переменной.
4. Введите новое значение переменной в поле **Значение переменной** (Variable value) и нажмите кнопку **OK**.

На компьютерах домена переменные среды можно редактировать с помощью редактора управления групповыми политиками в узле **Настройка** посредством следующей процедуры:

1. В редакторе управления групповыми политиками откройте для редактирования объект групповой политики. Для настройки параметров компьютера разверните узел **Конфигурация компьютера\Настройка\Конфигурация Windows** и выберите узел **Среда**. Для настройки параметров пользователя разверните узел **Конфигурация пользователя\Настройка\Конфигурация Windows** и выберите узел **Среда**.
2. Щелкните на узле **Среда** правой кнопкой мыши, выберите в контекстном меню команду **Создать**, а затем команду **Переменные среды**. Откроется диалоговое окно **Новые свойства среды**.
3. В списке **Действие** выберите **Обновить** (Update), чтобы обновить переменную, или **Заменить** (Replace), чтобы удалить, а затем снова создать ее. Далее выберите опцию

Пользовательская переменная или **Системная переменная**, чтобы создать пользовательскую или системную переменную соответственно.

4. В поле **Имя** и **Значение** введите имя и значение обновляемой переменной соответственно.
5. Для управления способом применения настройки используются опции на вкладке **Общие параметры**. Как правило, новую переменную нужно создать только один раз. В таких случаях устанавливается флажок **Применить один раз и не применять повторно**.
6. Нажмите кнопку **OK**, чтобы сохранить настройку. При следующем обновлении политики элемент настройки будет применен должным образом к объекту групповой политики, для которого он был определен.

Удаление переменной среды

Переменные среды можно удалять в диалоговом окне **Переменные среды**, выбрав требуемую переменную, а затем нажав кнопку **Удалить**. На компьютерах домена переменные среды можно удалять с помощью редактора управления групповыми политиками посредством следующей процедуры:

1. В редакторе управления групповыми политиками откройте для редактирования объект групповой политики. Для настройки параметров компьютера разверните узел **Конфигурация компьютера\Настройка\Конфигурация Windows** и выберите узел **Среда**. Для настройки параметров пользователя разверните узел **Конфигурация пользователя\Настройка\Конфигурация Windows** и выберите узел **Среда**.
2. Далее выполните одно из следующих действий.

   - Если элемент настройки для переменной уже существует, откройте окно свойств этой переменной, дважды щелкнув на ее имени. В списке **Действие** выберите опцию **Удалить**. На вкладке **Общие параметры** установите требуемую опцию, например **Применить один раз и не применять повторно**, а затем нажмите кнопку **OK**.
   - Если элемент настройки для переменной, которую нужно удалить с компьютеров, не существует, его нужно создать одним из вышеописанных методов. Обязательно выберите опцию **Удалить** в списке **Действие**, а также выберите требуемые опции на вкладке **Общие**.

Вкладка *Дополнительно*: загрузка и восстановление

Параметры загрузки и восстановления системы настраиваются в диалоговом окне **Загрузка и восстановление** (Startup and Recovery) (рис. 2.18).

Это диалоговое окно можно открыть следующим образом:

1. В Панели управления щелкните по ссылке категории **Система и безопасность** и в открывшемся списке элементов этой категории выберите ссылку **Система**.
2. В левой панели окна **Система** щелкните по ссылке **Дополнительные параметры системы**.
3. Наконец, в открывшемся окне **Свойства системы** перейдите на вкладку **Дополнительно** и в разделе **Загрузка и восстановление** этой вкладки нажмите кнопку **Параметры**, вследствие чего откроется диалоговое окно **Загрузка и восстановление**.

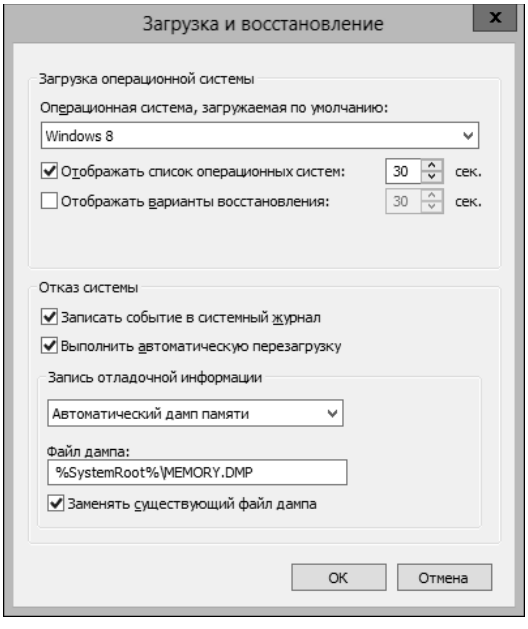


Рис. 2.18. Диалоговое окно **Загрузка и восстановление**

Примечание

Другой, более быстрый, способ открытия данного окна — это открыть окно **Свойства системы**, выполнив команду `systempropertiesadvanced` в поле поиска панели **Приложения**, а затем в области **Загрузка и восстановление** вкладки **Дополнительно** этого окна нажать кнопку **Параметры**.

Настройка параметров загрузки

Область **Загрузка операционной системы** (System startup) диалогового окна **Загрузка и восстановление** содержит параметры управления загрузкой операционной системы. На компьютере с несколькими операционными системами ОС для загрузки по умолчанию выбирается в раскрывающемся списке **Операционная система, загружаемая по умолчанию** (Default operating system). Флажки под этим списком задают параметры, используемые диспетчером загрузки Windows.

При запуске компьютера с несколькими операционными системами по умолчанию в течение 30 секунд отображается меню выбора операционной системы для загрузки. Предоставляемое по умолчанию время для выбора операционной системы для загрузки можно изменить одним из следующих способов:

- задать немедленную загрузку операционной системы по умолчанию, сбросив флажок **Отображать список операционных систем** (Time to display list of operating systems);
- оставить этот флажок установленным и задать другое время, в течение которого отображать список выбора операционных систем для загрузки.

Обычно на большинстве систем это время можно установить в пределах 3—5 с. Этого времени достаточно, чтобы пользователь смог выбрать требуемую операционную систему, и в то же время оно короткое, чтобы не задерживать процесс загрузки.

При загрузке системы в режиме восстановления можно отображать список вариантов восстановления. Как и в случае с вариантами загрузки, имеются два способа настроить загруз-

ку восстановления. Можно не предлагать вариантов восстановления и задать немедленную загрузку компьютера, сбросив флажок **Отображать варианты восстановления** (Time to display recovery options when needed), или же отображать доступные варианты в течение определенного времени. В последнем случае флажок нужно установить и задать время для отображения опций восстановления.

Настройка параметров восстановления

В областях **Отказ системы** (System failure) и **Запись отладочной информации** (Write debugging information) диалогового окна **Загрузка и восстановление** задаются параметры восстановления системы. Эти параметры восстановления позволяют задавать действия, которые можно предпринять в случае неисправимого системного сбоя (также называется *остановом по ошибке*). В области **Отказ системы** доступны следующие опции восстановления.

- **Записать событие в системный журнал** (Write an event to the system log). Установка этого флажка задает протоколирование ошибки в системном журнале, что позволяет администраторам впоследствии попытаться выяснить ее причины, просмотрев запись с помощью средства просмотра событий.
- **Выполнить автоматическую перезагрузку** (Automatically restart). При установке этого флажка после неисправимого сбоя система пытается перезагрузиться.

> ***Примечание***
>
> Установка автоматической перезагрузки не всегда является хорошим подходом к восстановлению. Иногда желательно вместо перезагрузки остановить систему, чтобы внимательно исследовать ее. При перезагрузке же этот факт будет известен лишь при просмотре системных журналов или если администратор окажется в это время рядом с системой.

Параметры группы **Запись отладочной информации** позволяют выбрать тип отладочной информации для записи в файл дампа, которую затем можно использовать для диагностирования причины отказа. Доступны следующие опции:

- **Нет** (None) — дамп не сохраняется;
- **Малый дамп памяти** (Small memory dump) — в файл дампа записывается содержимое физического сегмента памяти, в котором произошла ошибка. Размер записываемого сегмента — 256 Кбайт;
- **Дамп памяти ядра** (Kernel memory dump) — в файл дампа записывается содержимое области физической памяти, используемой ядром Windows. Объем записываемых данных зависти от размера ядра Windows;
- **Полный дамп памяти** (Complete memory dump) — в файл дампа записывается содержимое всей физической памяти. Размер файла зависит от объема используемой физической памяти, вплоть до полного объема установленной памяти компьютера;
- **Автоматический дамп памяти** (Automatic memory dump) — объем записываемой в файл дампа информации определяется автоматически Windows.

При выборе любого типа дампа памяти нужно указать расположение файла, в который его выполнять. По умолчанию для малого дампа памяти используется файл *%SystemRoot%*\Minidump, а для дампов других типов — файл *%SystemRoot%*\Memory.dmp. Кроме этого, обычно также следует установить флажок **Заменять существующий файл дампа** (Overwrite any existing file), чтобы при новой ошибке останова файл дампа содержал данные только для этой ошибки.

Рекомендации

Для создания файла дампа система должна быть правильно сконфигурирована. В частности, файл подкачки должен быть достаточного размера и расположен на системном диске (что задается в настройках виртуальной памяти на вкладке **Дополнительно**). Кроме этого диск, на котором сохраняется файл дампа, также должен иметь достаточно свободного пространства, чтобы вместить этот файл. В случае дампа памяти ядра объем свободного дискового пространства, требуемого для файла дампа, составляет 35—50% от объема оперативной памяти. Например, если в системе установлено 16 Гбайт оперативной памяти, то для файла дампа памяти ядра требуется 6—8 Гбайт свободного дискового пространства.

Вкладка *Защита системы*

Вкладка **Защита системы** (System Protection) диалогового окна **Свойства системы** (рис. 2.19) содержит параметры для управления восстановлением системы.

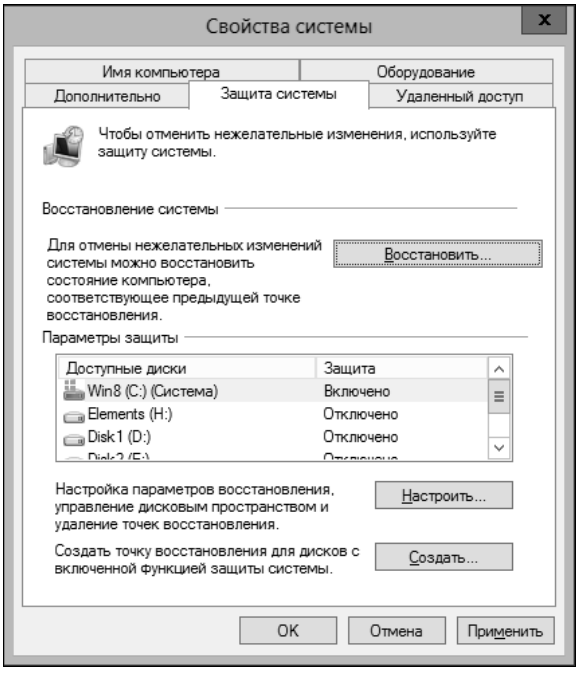


Рис. 2.19. Вкладка **Защита системы**

Получить доступ к этой вкладке можно следующим способом:

1. В Панели управления щелкните по ссылке категории **Система и безопасность** и в открывшемся списке элементов этой категории выберите ссылку **Система**.
2. В левой панели окна **Система** щелкните по ссылке **Защита системы** (System protection).
3. В открывшемся диалоговом окне **Свойства системы** выберите вкладку **Защита системы**.

Другой способ добраться к этой вкладке — выполнить команду `systempropertiesprotection` в поле поиска панели **Приложения**, в окне **Выполнить**, командной строке или оболочке Windows PowerShell.

В отличие от Windows 7, параметры восстановления Windows 8 не содержат отдельной опции восстановления предыдущих версий файлов. Вместо этого предыдущие версии личных

файлов создаются с помощью резервного копирования посредством утилиты **История файлов**. В последующих разделах рассматривается работа со средством **Восстановление системы** и его настройка. Точки восстановления и резервное копирование истории файлов для восстановления системы *см. в главе 10*.

Практический совет

Файловые серверы Windows Server 2012 обладают функциональностью **Предыдущие версии**. Предыдущие версии файлов получаются с теневых копий для сетевых папок. Окно свойств сетевой папки будет иметь вкладку **Предыдущие версии** (Previous Versions). Эта вкладка используется для восстановления предыдущих версий файлов данной сетевой папки.

Принцип работы защиты системы

При включенной защите системы компьютер периодически создает снимки системной конфигурации. Эти снимки называются *точками восстановления* (restore points). В число отслеживаемых параметров системной конфигурации входят параметры Windows и список установленных программ. В случае проблем с запуском или работой компьютера вследствие изменения конфигурации системы с помощью точки восстановления ее можно восстановить ко времени одного из снимков системы. Например, допустим, что после установки нового пакета обновлений для Office система, которая до этого работала как часы, начинает давать сбои и приложения Office отказываются запускаться. Удаление пакета обновлений не помогает, но есть еще одно средство — восстановление системы, посредством которого систему можно восстановить до состояния, в котором она находилась до установки пакета обновлений.

Примечание

В функциональности восстановления системы используются разные типы точек восстановления. Один тип, *системная контрольная точка* (system checkpoint), создается операционной системой через постоянные промежутки времени. Другой тип, *точка восстановления установки или обновления*, создается автоматически операционной системой при установке приложений или обновлений. Еще один тип, *ручная точка восстановления*, создается вручную пользователями. Администраторам следует рекомендовать своим пользователям создавать ручные точки восстановления перед тем, как выполнять операции, которые могут затронуть нормальное функционирование системы.

Возможность защиты системы применима к отдельным дискам и должна быть включена для дисков, содержащих критические приложения и системные файлы. По умолчанию защита системы включена только для системного диска, а для других дисков может быть включена вручную. Если для определенного диска защита системы не включена, изменения в конфигурации системы для этого диска не отслеживаются, вследствие чего, в случае проблем, восстановление системной конфигурации для этого диска будет невозможным.

Примечание

Для всех дисков с включенной защитой системы точки восстановления создаются ежедневно. Предыдущие версии файлов не сохраняются, как часть точек восстановления тома, созданных автоматически или вручную. Для создания предыдущих версий файлов следует использовать средство резервного копирования **История файлов**.

Настройка восстановления системы

Настройка функциональности восстановления системы осуществляется на вкладке **Защита системы** диалогового окна **Свойства системы**. Процессом, ответственным за отслеживание изменений в конфигурации системы и приложениях, является служба **Теневое копиро-**

вание тома[1] (Volume Shadow Copy). Эта служба настраивается на автоматический запуск и исполняется под системной учетной записью LocalSystem. Если эта служба не исполняется или не настроена должным образом, функциональность восстановления системы не будет работать, как следует.

Защита системы сохраняет системные контрольные точки для всех отслеживаемых дисков и требует, по крайней мере, 300 Мбайт свободного дискового пространства на системном диске для хранения точек восстановления. Кроме этого, функциональность защиты системы резервирует дополнительное место на диске для точек восстановления по мере надобности, вплоть до всей емкости жесткого диска; но это пространство всегда доступно пользователям и приложениям, т. к. защита системы освобождает его по мере необходимости. В случае недостатка свободного пространства для надобностей защиты системы, операционная система затирает предыдущие точки восстановления, освобождая таким образом дисковое пространство для записи новых точек восстановления.

Объем дискового пространства для надобностей защиты системы можно задавать вручную. По умолчанию для хранения точек восстановления защита системы резервирует, по крайней мере, 1% от полного объема диска. Например, на жестком диске объемом в 930 Гбайт защита системы по умолчанию резервирует 9,3 Гбайт под файлы точек восстановления.

Процедура настройки защиты системы для дисков следующая:

1. В Панели управления щелкните по ссылке категории **Система и безопасность** и в открывшемся списке элементов этой категории выберите ссылку **Система**.
2. В левой панели окна **Система** щелкните по ссылке **Защита системы**.
3. Выберите в списке **Параметры защиты** (Protection settings) диск, для которого требуется настроить защиту системы, а затем нажмите кнопку **Настроить** (Configure). Откроется диалоговое окно **Защита системы** (System Protection) для выбранного диска (рис. 2.20).
4. Установите один из следующих переключателей.
   - **Включить защиту системы** (Turn on system protection). Установка этого переключателя включает возможность создания точек восстановления для диска, и настоятельно рекомендуется для системных дисков, чтобы обеспечить восстановление системы в случае сбоя.
   - **Отключить защиту системы** (Disable system protection). Установка этого переключателя отключает защиту системы для данного диска. Эта опция не рекомендуется для системных дисков, т. к. не обеспечивает возможности восстановления компьютера к прежнему состоянию.
5. Для включенной защиты системы с помощью ползунка **Максимальное использование** (Max Usage) можно задать максимальный объем дискового пространства для хранения файлов точек восстановления. По заполнению выделенного объема диска защита системы удаляет старые точки восстановления, чтобы освободить место под новые.
6. Выполнив все требуемые настройки, нажмите кнопку **OK**, чтобы сохранить их. (При установленном переключателе отключения защиты системы Windows удаляет все ранее созданные точки и запрашивает подтверждение для этого. Если действительно требуется

[1] В версиях Windows, предшествующих Windows Vista, эта служба называлась **Службой восстановления системы**.

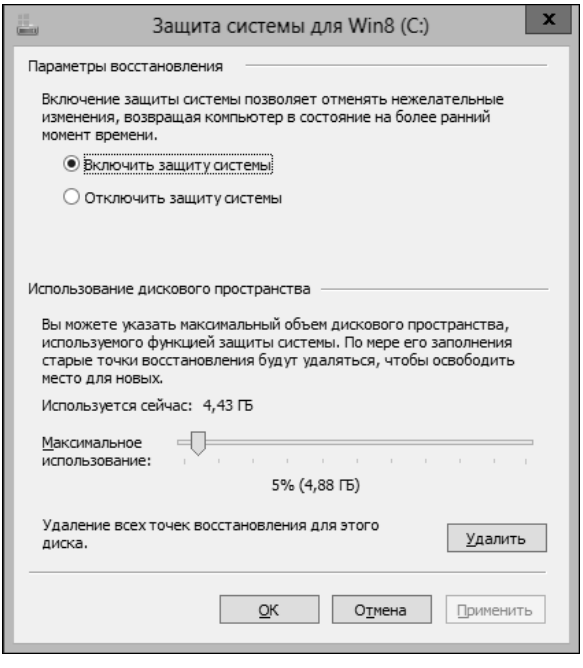


Рис. 2.20. Диалоговое окно для настройки защиты системы для диска

отключить защиту системы, нажмите кнопку **Да** в окне запроса. По завершению удаления данных точек восстановления нажмите кнопку **Закрыть**.)

При полной уверенности, что система находится в стабильном состоянии, можно удалить все точки восстановления, чтобы освободить дисковое пространство или предотвратить непреднамеренное применение пользователями одной из точек восстановления. Для этого нужно выполнить следующую процедуру:

1. В Панели управления щелкните по ссылке категории **Система и безопасность** и в открывшемся списке элементов этой категории выберите ссылку **Система**.
2. В левой панели окна **Система** щелкните по ссылке **Защита системы**.
3. Выберите в списке **Параметры защиты** диск, для которого требуется настроить защиту системы, а затем нажмите кнопку **Настроить**.
4. В открывшемся диалоговом окне **Защита системы** нажмите кнопку **Удалить** (Delete), в следующем диалоговом окне нажмите кнопку **Продолжить** (Continue), чтобы подтвердить намерение удалить точки восстановления. Повторите шаги 3 и 4 для других дисков, если требуется.
5. По завершению удаления данных восстановления нажмите кнопку **Закрыть**.

Вкладка *Удаленный доступ*

На вкладке **Удаленный доступ** (Remote) диалогового окна **Свойства системы** выполняется настройка параметров запросов удаленного помощника и подключений к удаленному рабочему столу. Эти параметры и их настройка рассматриваются в *разд. "Управление удаленным доступом к рабочим станциям" главы 7*.

Конфигурирование параметров управления питанием

Параметры управления питанием следят за поведением компьютера в различных режимах потребления электроэнергии, таких как работа от сети или от батарей. Хотя все компьютеры должны быть настроены на экономию электроэнергии, управление электропитанием на ноутбуках помогает сбалансировать быстродействие и потребление электроэнергии. В некоторых случаях необходимо увеличить время отклика и понизить производительность ноутбука, чтобы продлить время работы от батарей. В других случаях может быть допустимым средний уровень производительности при среднем времени работы от батарей, или же необходимо получить максимальную производительность независимо от того, как это повлияет на время работы батареи.

Ключевые аспекты энергопотребления контролируются посредством схем управления питанием, которые представляют собой наборы параметров, следящих за потреблением электроэнергии. Для компьютера может существовать несколько схем управления питанием, но только одна из них может быть задействованной в любой момент времени. Кроме схем управления питанием, для большинства компьютеров предустановлены действия, которые следует выполнять при нажатии кнопки питания и кнопки перехода в спящий режим, а для ноутбуков — при закрытии крышки. Обычно закрытие крышки ноутбука переводит его в спящий режим, длительное нажатие кнопки питания выключает компьютер, а нажатие кнопки перехода в спящий режим переводит его в спящий режим. Но с помощью общесистемных параметров электропитания можно настроить кнопку питания и поведение при выходе из режима сна для удовлетворения требований индивидуальных пользователей или групп пользователей.

Управление параметрами электропитания из командной строки

Операционная система Windows 8 содержит утилиту Power Configuration (powercf.exe) для управления параметрами электропитания из командной строки. Выполнение команды `powercfg /?` выводит на экран список параметров этой утилиты. В число наиболее часто употребляемых параметров входят следующие:

- `-a` — выводит список всех доступных режимов сна компьютера и причину, по которой определенный режим сна не поддерживается;
- `-d [guid]` — удаляет схему управления электропитанием, заданную идентификатором GUID;
- `-devicequery all devices verbose` — выводит на экран подробную информацию о поддержке режимов электропитания для всех устройств компьютера. При исполнении этой команды рекомендуется направить ее вывод в файл, т. к. этот вывод довольно объемистый;
- `-energy` — выполняет проверку системы на наличие основных проблем конфигурации, устройств и батарей, связанных с эффективностью энергопотребления и временем работы от батареи, и создает отчет о результатах проверки в текущей рабочей папке;
- `-h` — включает/выключает возможность гибернации;
- `-l` — выводит список сконфигурированных на компьютере схем управления питанием по имени и идентификатору GUID;

- `-q [guid]` — выводит содержимое схемы управления питанием, заданной идентификатором GUID. Если идентификатор GUID не указан, выводится содержимое активной схемы электропитания;
- `-requests` — перечисляет все запросы питания для драйверов устройств. При наличии запросов питания для дисплеев, ожидающих выполнение, эти запросы предотвращают автоматическое выключение дисплеев. При наличии запросов питания для любых устройств, включая дисплеи, ожидающих выполнения, эти запросы предотвращают автоматический переход компьютера в спящий режим;
- `-s [guid]` — активирует в системе схему управления электропитанием с указанным идентификатором GUID;
- `-x [параметр] [значение]` — задает указанное значение для указанного параметра в активной схеме управления электропитанием.

> ***Примечание***
>
> По умолчанию в компьютерах под управлением Windows 8 вместо гибернации применяется гибридный режим сна. Прежде чем настраивать режим гибернации, следует определить его поддержку компьютером. Также параметры для команды `powercfg` можно задавать с использованием дефиса (-) либо косой черты (/). Оба эти знака абсолютно равносильны; предпочтение одного из них другому может определяться такими факторами, как размещение на клавиатуре.

В листинге 2.1 приводится пример вывода, возвращаемого командой `powercfg -l`.

Листинг 2.1. Пример вывода команды `powercfg -l`

```
Существующие схемы управления питанием (* — активные)
-----------------------------------
GUID схемы питания: 381b4222-f694-41f0-9685-ff5bb260df2e (Сбалансированный)
GUID схемы питания: 8c5e7fda-e8bf-4a96-9a85-a6e23a8c635c (Высокая производительность)
GUID схемы питания: a1841308-3541-4fab-bc81-f71556f20b4a (Экономия энергии)
GUID схемы питания: Cld97820-3148-42a9-a587-75d618a9bb2b (Graphics Dept)*
```

В листинге 2.1 активная схема электропитания помечена звездочкой. По этому выводу можно определить, что данный компьютер имеет четыре схемы управления питанием и активной является схема **Graphics Dept**.

Для настройки схем управления электропитанием или модифицирования параметров питания с помощью утилиты Powercfg эту утилиту нужно запустить с правами администратора. Если для параметра требуется указать идентификатор GUID, самым легким способом узнать его будет выполнить команду `powercfg -l` (с правами администратора), а затем скопировать значение для соответствующей схемы управления электропитанием. Например, чтобы установить в качестве схемы по умолчанию схему **Сбалансированный** (см. листинг 2.1), следует выполнить команду:

```
powercfg -s 381b4222-f694-41f0-9685-ff5bb260df2e
```

Определить поддерживаемые компьютером режимы электропитания можно с помощью команды `powercfg -a`. Пример результата исполнения этой команды показан в листинге 2.2.

Листинг 2.2. Пример результата исполнения команды `powercfg -a`

```
В данной системе доступны следующие состояния спящего режима:
    Ждущий режим (S1 S3)
    Гибернация
```

```
    Гибридный спящий режим
    Быстрый запуск

Следующие состояния спящего режима недоступны в данной системе:
    Ждущий режим (S2)
      Системное встроенное ПО не поддерживает ждущий режим.

    Ждущий режим (подключенный)
      Системное встроенное ПО не поддерживает ждущий режим.
```

В случае проблем с переходом компьютера в спящий режим или режим гибернации с помощью команды `powercfg -a` можно попытаться определить причину такой проблемы. Если выяснится, что микропрограммное обеспечение компьютера не поддерживает определенный режим, то в некоторых случаях проблему можно устранить, обновив его версией, поддерживающей требуемый режим. Может оказаться, что устройство, не поддерживающее определенного режима энергопотребления, вызывает проблемы в работе компьютера. В таком случае это устройство можно попытаться удалить и заменить его совместимым устройством.

Оценить конфигурацию энергопотребления компьютера и совместимость устройств можно с помощью команды `powercfg -energy`. Результатом выполнения этой команды является отчет о диагностике эффективности энергопотребления, который сохраняется как файл energy-report.html. Отчет содержит результаты анализа соответствия устройств схемам управления питанием. В нем приводится список устройств, не поддерживающих должным образом управление энергопотреблением и описание проблем совместимости. Например, если устройство USB не переходит должным образом в ждущий режим, информация о вызываемых этим фактом ошибках вместе с информацией о конфигурации устройства отображается в отчете. А если возможность управления питанием была отключена в связи с проблемой совместимости, это также отражается в отчете. Например, если аппаратное обеспечение системы не поддерживает режим ASPM PCI Express, вследствие чего эта возможность была отключена, это обстоятельство будет указано в отчете. В отчете также предоставляются предупреждения и дополнительная информация об устройствах и совместимости, включая подробности о поддерживаемых режимах сна и возможностях процессора по управлению энергопотреблением.

> ***Практический совет***
>
> Для ноутбуков в отчете предоставляется важная информация о заряде и времени работы от батарей. Если срок службы батареи подходит к концу или уже истек, это можно будет определить по тому обстоятельству, что время работы от такой батареи будет ограничено, и в сведениях о батарее будет указано, что батарея не заряжается до своей расчетной емкости. Таким образом, будет известно, что батарею ноутбука требуется заменить.

Подробную информацию о поддержке каждым устройством системы режимов энергопотребления можно найти с помощью следующей команды:

```
powercfg -devicequery all_devices_verbose > power.txt
```

где `power.txt` — это имя файла в текущем рабочем каталоге, в который будет перенаправлен и сохранен вывод этой команды.

Настроив утилиту Windows PowerShell для удаленной работы, в ней можно исполнять команду `powercfg` на удаленных компьютерах. Для этого создайте текстовый файл computers.txt, введите в него имена удаленных компьютеров (каждое в новой строке), а затем сохраните этот файл. После этого откройте Windows PowerShell с правами администратора и выполните в ней следующие команды:

```
$comp = get-content c:\computers.txt
$s = new-pssession -computername $comp
invoke-command -session $s { powercfg.exe -energy }
```

Здесь `c:\computers.txt` обозначает путь к файлу computers.txt. Измените этот путь в соответствии с расположением этого файла в конкретном случае. В результате выполнения этих команд на каждом компьютере, указанном в файле computer.txt, будет создан файл energy-report.html в каталоге по умолчанию для пользователя, чья учетная запись используется для доступа к этому компьютеру. Чтобы избежать неудобства получения отчета с каждого компьютера, все отчеты можно сохранить на сетевом диске, называя каждый из них по имени компьютера, для которого он создается. Команды для создания отчетов таким образом приводятся в листинге 2.3.

Листинг 2.3. Сценарий для сохранения файлов отчетов на сетевом диске

```
$comp = get-content c:\computers.txt
$s = new-pssession -computername Scomp
invoke-command -session $s { powercfg.exe -energy -output
 "\\fileserver46\data\Senv:computername.html"}
```

В данном случае отчет для каждого компьютера сохраняется на сетевом диске \\fileserver46\data под именем, созданным на основе значения переменной среды `computername`. Обратите внимание, что при работе с консолью Windows PowerShell задаваемые в ней команды ссылаются на исполняемые файлы, поэтому имя команды нужно указывать вместе с расширением exe.

Работа со схемами управления питанием

На мобильных вычислительных устройствах область извещений панели задач содержит значок **Электропитание**. Щелчок по этому значку открывает окно, в котором указывается состояние батареи и используемая в данный момент схема управления питанием. Щелчок по любой из ссылок в этом диалоговом окне открывает окно **Электропитание** (Power Optionss). Большинство конфигураций Windows 8 имеют три основные схемы управления питанием.

- **Сбалансированная** (Balanced). Данная схема балансирует энергопотребление компьютера и производительность системы. При дополнительной нагрузке на процессор энергопотребление повышается, а при снижении нагрузки снижается и энергопотребление. Эта схема управления питанием применяется по умолчанию. Ее рекомендуется применять, когда система используется для работы с разнообразными приложениями, включая как умеренно ресурсоемкие в графическом отношении приложения, такие как Microsoft PowerPoint, так и приложения, не являющиеся таковыми, например Microsoft Word и Outlook.
- **Высокая производительность** (High performance). Применение этой схемы оптимизирует производительность компьютера за счет времени работы от батарей. Эта схема всегда обеспечивает удовлетворение всех требований питания при использовании ресурсоемких в графическом плане рабочих приложений или приложений мультимедиа, таких как компьютерные игры. Эту схему рекомендуется применять в тех случаях, когда производительность играет главную роль, а пользователи работают в основном с ресурсоемкими графическими приложениями или приложениями, выполняющими сложные математические вычисления. Обратите внимание на то, что для отображения этой схемы

может потребоваться щелкнуть по ссылке **Показать дополнительные схемы** (Show additional plans).

- **Экономия энергии** (Power saver). Эта схема предназначена для понижения энергопотребления компьютера. При использовании этой схемы скорость работы процессора понижается, чтобы продлить время работы от батарей. Эта схема рекомендуется для пользователей, которые работают в основном с приложениями, не потребляющими большого объема графических ресурсов, например Word или Outlook.

Параметры схем управления электропитанием разделены на две общие категории: основные и дополнительные. Основные параметры питания управляют уменьшением яркости или отключением экрана и переходом компьютера в спящий режим. Важно отметить, что мобильные устройства имеют два набора параметров питания: один для работы от батарей, а другой для работы от сети. Настройку параметров каждого из этих наборов можно выполнять независимо друг от друга. Например, можно установить уменьшение яркости экрана после двух минут бездействия при работе от батарей или после пяти при работе от сети.

Расширенные параметры питания позволяют с точностью задать время отключения компонентов компьютера, а также настроить их производительность. Состав расширенных параметров зависит от конфигурации компьютера и включает следующие параметры.

- **Батарея / Уровень резерва батареи** (Battery / Reserve battery level). Задает остаточный процент емкости батареи, при котором активируется режим энергосбережения. Обычно, по умолчанию для этого параметра задается значение 7%. Это означает, что когда уровень заряда батареи понизится до 7% от полного заряда, компьютер перейдет в режим энергосбережения. Хотя этому параметру можно присвоить любое значение, в большинстве случаев наилучшим будет уровень резерва батареи в диапазоне от 5 до 18%.
- **Параметры фона рабочего стола / Показ слайдов** (Desktop background settings / Slide show). Определяет, доступен или приостановлен показ слайдов в качестве фона рабочего стола. Значение по умолчанию — **Доступно** (Available). При установке значения **Приостановлено** (Paused) показ слайдов для фона рабочего стола будет отключен.
- **Экран / Отключать экран через** (Display / Turn off display after). Задает отключение экрана компьютера после определенного периода бездействия и длительность этого периода с целью экономии заряда батареи. Присвоение этому параметру значения **Никогда** (Never) отключает эту возможность. Длительность периода бездействия компьютера устанавливается счетчиком.
- **Жесткий диск / Отключать жесткий диск через** (Hard disk / Turn off hard disk after). Задает отключение жестких дисков компьютера после определенного периода бездействия и длительность этого периода с целью экономии заряда батареи. Присвоение этому параметру значения **Никогда** (Never) отключает эту возможность, т. е. жесткие диски никогда не будут отключаться, независимо от того, сколько времени компьютер остается неактивен. Длительность периода бездействия компьютера устанавливается счетчиком, отображающимся при щелчке по значению параметра. Значение счетчика можно быстро прокручивать вверх или вниз, нажав и удерживая соответствующую стрелку счетчика. При прокрутке счетчика вниз после единицы устанавливается значение **Никогда**. Значение можно также вводить в поле счетчика. При вводе 0 параметру присваивается значение **Никогда**.
- **Параметры мультимедиа / При воспроизведении видео** (Multimedia settings / When playing video). Задет режим оптимизации энергопотребления при воспроизведении видео. При значении этого параметра **Оптимизация качества видео** (Optimize video quality) будет применяться наилучшее качество воспроизведения. При значении **Оптимизация** (Balanced) будет применяться сбалансированный подход с несколько пони-

женным качеством воспроизведения в целях энергосбережения. А при значении **Оптимизация энергосбережения** (Optimize power settings) уровень качества воспроизведения устанавливается для активного энергосбережения.

- **Параметры мультимедиа / При общем доступе к мультимедиа** (Multimedia settings / When sharing media). Задает действие при воспроизведении мультимедиа с данного компьютера другим компьютером или устройством. При значении этого параметра **Разрешить компьютеру переходить в режим отсутствия** (Allow the computer to enter away mode) компьютер не будет переходить в спящий режим, когда предоставляет мультимедиа для других компьютеров или устройств. При значении **Разрешить компьютеру переходить в спящий режим** (Allow the computer to sleep) компьютер может переходить в спящий режим после определенного периода бездействия независимо от того, что он предоставляет мультимедиа для других компьютеров или устройств. А если значение этого параметра равно **Запретить переход из состояния простоя в спящий режим** (Prevent idling to sleep), компьютер будет переходить в спящий режим при предоставлении мультимедиа для других компьютеров или устройств, только если это сделает пользователь.
- **PCI Express / Управление питанием состоянием связи** (PCI Express / Link State Power Management). Задает режим энергосбережения для применения с устройствами PCI Express, подключенными к компьютеру. Доступные значения — **Откл.**, **Умеренное энергосбережение**, **Максимальное энергосбережение** (Off, Moderate power savings, Maximum power savings).
- **Кнопки питания и крышка / Действие кнопки питания** (Power buttons and lid / Power button action). Задает действие при длительном нажатии кнопки питания компьютера. Доступные значения: **Действие не требуется**, **Сон**, **Гибернация Завершение работы** (Do nothing, Sleep, Hibernate, Shut down).
- **Кнопки питания и крышка / Действие кнопки спящего режима** (Power buttons and lid / Sleep button action). Задает действие по умолчанию для кнопки перехода в спящий режим. Этот параметр используется для замены действия по умолчанию компьютера. Доступные значения: **Действие не требуется**, **Сон**, **Гибернация** (Do nothing, Sleep, Hibernate). Но, несмотря на наличие значения параметра в списке, оно не может быть присвоено, если компьютер его не поддерживает.
- **Управление питанием процессора / Максимальное состояние процессора** (Processor power management / Maximum processor state). Задает максимальную производительность процессора компьютера. Для энергосбережения и продления времени работы от батареи значение этого параметра можно понизить. Но понижение уровня производительности процессора напрямую сказывается на времени отклика и скорости вычислений. Хотя понижение уровня производительности процессора до 50% или ниже от максимального может значительно понизить быстродействие и время отклика, в то же самое время это может значительно повысить уровень энергосбережения.
- **Управление питанием процессора / Минимальное состояние процессора** (Processor power management / Minimum processor state). Задает минимальный уровень производительности процессора компьютера. Чтобы повысить уровень энергосбережения и продлить время работы от батареи, значение этого параметра можно понизить. Но понижение уровня производительности процессора напрямую сказывается на времени отклика и скорости вычислений. Например, при значении этого параметра 5% как время отклика, так и обработка данных будут медленными, но зато уровень энергосбережения будет высоким. При значении 50% достигается баланс между временем отклика и производительностью и энергосбережением. А значение 100% максимизирует время отклика и производительность при полном отсутствии энергосбережения.

- **Управление питанием процессора / Политика охлаждения системы** (Processor power management / System cooling policy). Задает приоритет для повышения скорости вентилятора и понижения скорости процессора. Если этому параметру присвоено значение **Пассивный** (Passive), замедляется процессор, прежде чем повышается скорость вентилятора, а если **Активный** (Active) — скорость вентилятора повышается перед замедлением процессора.
- **Имя плана / Требовать введения пароля для пробуждения** (Plan name /Require a password on wakeup). Задает, запрашивать ли пароль при выходе компьютера из спящего режима. Доступные значения: **Да** или **Нет**. Для компьютеров членов домена этому параметру присвоено значение **Да**, и изменять его можно только посредством групповой политики.
- **Сон / Разрешить гибридный спящий режим** (Sleep / Allow hybrid sleep). Задает тип режима сна: режим сна для Windows 8 или режим сна, используемый в предыдущих версиях Windows. Допустимые значения: **Вкл./Выкл.** (On/Off). В гибридном спящем режиме компьютер находится в состоянии низкого энергопотребления, пока пользователь не возобновит работу с компьютером. При работе от батареи ноутбуки и планшеты, находящиеся в спящем режиме, продолжают потреблять ток, хоть и очень небольшой. Если батарея ноутбука, находящегося в спящем режиме, разряжается до критического уровня, текущее состояние компьютера сохраняется на жесткий диск, а компьютер полностью выключается. Это конечное состояние похоже на состояние гибернации, которое использовалось в Windows XP.
- **Сон / Разрешить таймеры пробуждения** (Sleep / Allow wake timers). Включает или отключает использование временных событий для вывода компьютера из спящего режима. При значении **Отключить** (Disable) компьютер в режиме сна на временные события не реагирует, а при значении **Включить** (Enable) временные события могут выводить компьютер из режима сна.
- **Сон / Гибернация после** (Sleep / Hibernate after). Задает переход компьютера в режим гибернации после определенного периода бездействия и длительность этого периода с целью экономии заряда батареи. При переходе компьютера в режим гибернации на жесткий диск компьютера записывается снимок рабочей среды пользователя и текущей системной рабочей среды. Когда компьютер выводится из режима гибернации, пользовательская и системная среда восстанавливаются в оперативной памяти из сохраненных на диск снимков. Этот параметр обычно не применяется в Windows 8, т. к. стандартной реакцией на период простоя является переход в спящий режим. Присвоение этому параметру значения **Никогда** (Never) отключает эту возможность. Длительность периода бездействия компьютера перед переходом в режим гибернации устанавливается счетчиком.
- **Сон / Сон после** (Sleep / Sleep after). Задает переход компьютера в режим сна после определенного периода бездействия и длительность этого периода с целью экономии заряда батареи. Присвоение этому параметру значения **Никогда** (Never) отключает эту возможность. Длительность периода бездействия компьютера перед переходом в режим сна устанавливается счетчиком.
- **Параметры USB / Параметр временного отключения USB-порта** (USB Settings / USB selective suspend setting). Задает возможность временного выборочного отключения USB-портов. Если этому параметру присвоено значение **Запрещено** (Disabled), выборочное временное отключение USB-устройств не применяется, а если присвоено значение **Разрешено** (Enabled), то, наоборот, применяется.
- **Параметры адаптера беспроводной сети / Режим энергосбережения** (Wireless Adapter Settings / Power Saving Mode). Задает режим энергосбережения для адаптеров беспро-

водной сети, подключенных к компьютеру. Доступные значения: **Максимальная производительность**, **Минимальное энергосбережение**, **Среднее энергосбережение**, **Максимальное энергосбережение** (Maximum Performance, Low Power Saving, Medium Power Saving, Maximum Power Saving).

Как можно видеть, расширенные параметры питания позволяют управлять всеми аспектами электропитания. По сути, разница между схемами управления электропитанием определяется разницей в значениях расширенных параметров. Например, тогда как схема **Высокая производительность** обеспечивает производительность, позволяя процессору всегда работать при 100-процентном энергопотреблении, схемы **Экономия энергии** и **Сбалансированный** понижают уровень энергопотребления посредством настройки энергопотребления процессора в диапазоне от минимум 5 процентов до максимум 100%.

Важным аспектом конфигурации схем управления электропитанием является настройка их на отключение компонентов после определенного периода простоя. Последовательное отключение компонентов позволяет последовательный переход компьютера во все более глубокий спящий режим. При полном переходе компьютера в спящий режим все компоненты с управляемым питанием отключены, вследствие чего уровень потребления электроэнергии компьютером значительно снижается. Когда компьютер выходит из спящего режима, питание компонентов, таких как монитор и жесткий диск, восстанавливается, а также восстанавливается рабочая среда пользователя. Спящий режим следует настраивать таким образом, чтобы при работе компьютера от батареи переход в спящий режим выполнялся после сравнительно короткого периода простоя, около 20—30 минут.

Так как компьютер может иметь несколько схем управления питанием, каждую схему можно оптимизировать под обстоятельства использования ноутбука в определенное время. Можно создать несколько схем управления питанием для разных ситуаций. Для работы дома или в офисе для ноутбука может требоваться другая конфигурация управления питанием, чем когда он используется для презентаций. В одном случае может быть желательным настроить ноутбук на экономный режим энергопотребления при работе от батарей, а в другом может быть необходимым обеспечить постоянную работу жесткого диска и адаптера беспроводной сети.

Выбор и оптимизация схем управления питанием

Хотя для компьютера может существовать несколько схем управления питанием, только одна из них может быть задействованной в любой данный момент времени. Выбрать или оптимизировать схему электропитания для компьютера можно следующим способом:

1. В Панели управления щелкните по ссылке категории **Система и безопасность** и в открывшемся списке элементов этой категории выберите ссылку **Электропитание**.
2. Как показано на рис. 2.21, схема управления питанием задается выбором в списке требуемой схемы.
3. Чтобы настроить выбранную схему управления электропитанием, щелкните по ее ссылке **Настройка плана электропитания** (Change plan settings). В результате откроется диалоговое окно **Изменение параметров схемы** (Edit Plan Settings) (рис. 2.22). Обратите внимание, что для мобильных устройств это окно содержит отдельные параметры для питания от батареи и от сети.
4. Для мобильных устройств в раскрывающемся списке **Затемнить дисплей** (Dim the display) укажите период простоя, после которого следует уменьшить яркость экрана. Чтобы отключить эту возможность, установите для этого параметра значение **Никогда**.

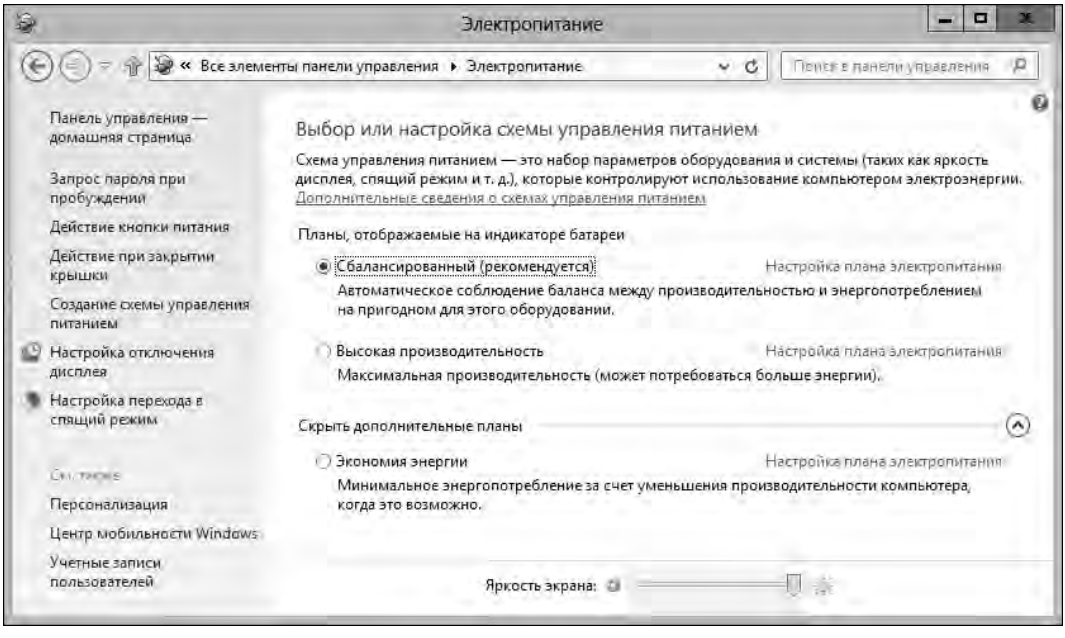


Рис. 2.21. Выбор схемы управления электропитанием

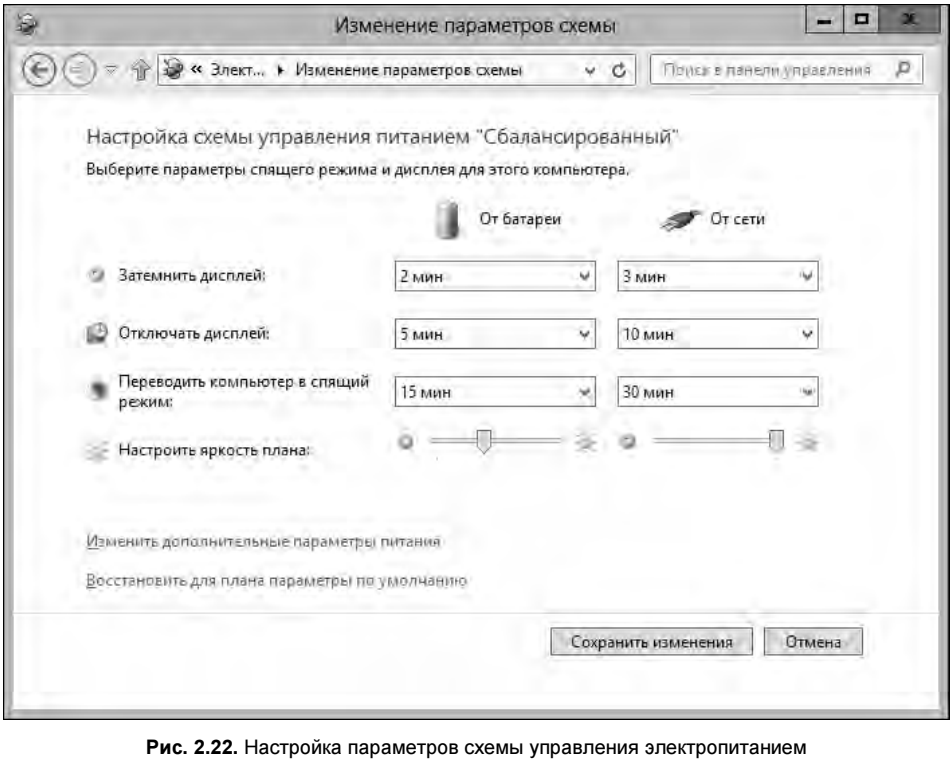


Рис. 2.22. Настройка параметров схемы управления электропитанием

5. В раскрывающемся списке **Отключать дисплей** (Turn off the display) задайте период бездействия, после которого следует отключать экран компьютера. Чтобы отключить возможность перехода в отключения дисплея, установите для этого параметра значение **Никогда**.
6. В раскрывающемся списке **Переводить компьютер в спящий режим** (Put the computer to sleep) установите период простоя, после которого компьютер следует переводить в спящий режим. Чтобы отключить возможность перехода в спящий режим, установите для этого параметра значение **Никогда**.
7. Для настройки дополнительных параметров электропитания щелкните по ссылке **Изменить дополнительные параметры питания** (Change advanced power settings). В открывшемся диалоговом окне **Электропитание** (Power Options) (рис. 2.23) установите требуемые значения дополнительных параметров, а затем нажмите кнопку **OK**, чтобы сохранить и применить выполненные настройки.

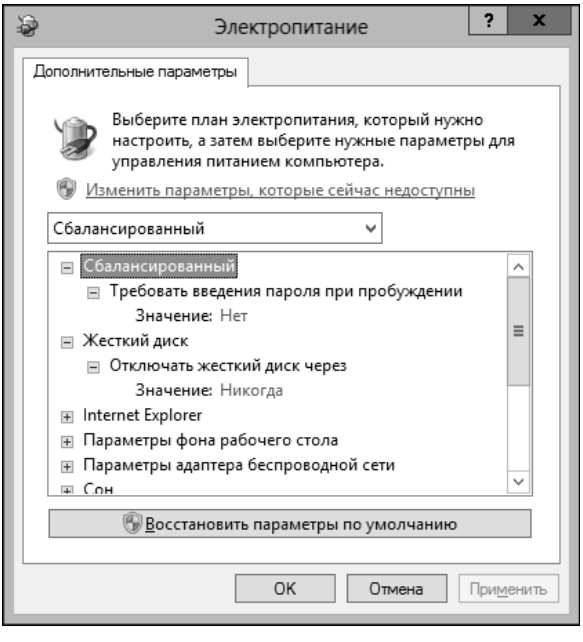


Рис. 2.23. Диалоговое окно **Электропитание** для настройки дополнительных параметров управления питанием

8. Если в окне **Изменение параметров схемы** были изменены значения параметров, сохраните их, нажав кнопку **Сохранить изменения** (Save changes).

На компьютерах домена схемы управления электропитания можно изменять с помощью редактора управления групповыми политиками в узле **Настройка** посредством следующей процедуры:

1. В редакторе управления групповыми политиками откройте для редактирования требуемый объект групповой политики. Для настройки параметров компьютера разверните узел **Конфигурация компьютера\Настройка\Параметры панели управления** и выберите узел **Электропитание**. Для настройки параметров пользователя разверните узел **Конфигурация пользователя\Настройка\Параметры панели управления** и выберите узел **Электропитание**.

2. Щелкните правой кнопкой мыши по узлу **Электропитание**, выберите в контекстном меню команду **Создать**, а затем щелкните на опции **Схема управления питанием (Windows 7 и выше)** (Power Plan (At least Windows 7)). Откроется диалоговое окно **Новые свойства схемы управления питанием (Windows 7 и выше)** (New Power Plan (At least Windows 7)).
3. Для обновления параметров схемы электропитания в списке **Действие** выберите опцию **Обновить** (Update), а чтобы удалить схему и создать ее заново согласно требуемым параметрам — опцию **Заменить** (Replace).
4. Выберите в списке требуемую схему электропитания, например, **Сбалансированная**.
5. Чтобы сделать схему активной, установите ее флажок **Задать в качестве текущей схемы управления электропитанием** (Set as the active power plan).
6. Настройте схему управления питанием, установив требуемые значения доступных для нее параметров.
7. Выполнив все требуемые настройки, нажмите кнопку **OK**, чтобы сохранить их. При следующем обновлении политики элемент настройки будет применен должным образом к объекту групповой политики, для которого он был определен.

Создание схем управления электропитанием

В дополнение к стандартным схемам управления электропитанием, поставляемым с Windows 8, можно создавать пользовательские схемы. Создать схему управления электропитанием можно следующим образом:

1. В Панели управления щелкните по ссылке категории **Система и безопасность** и в открывшемся списке элементов этой категории выберите ссылку **Электропитание**.
2. В левой панели открывшегося окна **Электропитание** щелкните по ссылке **Создание схемы управления питанием** (Create a power plan). Откроется окно **Создание схемы управления питанием** (Create a Power Plan) (рис. 2.24).
3. Для предварительной установки значений параметров схемы питания выберите стандартную схему, наиболее отвечающую требованиям создаваемой, например, **Сбалансированный**.
4. Введите описательное название схемы в соответствующее поле, а затем нажмите кнопку **Далее**. Откроется окно **Изменение параметров схемы**.
5. Для мобильных устройств в раскрывающемся списке **Затемнить дисплей** укажите период простоя, после которого следует уменьшить яркость экрана. Чтобы отключить эту возможность, установите для этого параметра значение **Никогда**.
6. В раскрывающемся списке **Отключать дисплей** задайте период бездействия, после которого следует отключать экран компьютера. Чтобы отказаться от возможности отключения дисплея, установите для этого параметра значение **Никогда**.
7. В раскрывающемся списке **Переводить компьютер в спящий режим** установите период простоя, после которого компьютер следует переводить в спящий режим. Чтобы отключить возможность перехода в спящий режим, установите для этого параметра значение **Никогда**.
8. Задав все требуемые настройки, нажмите кнопку **Создать**. Теперь в дополнение к стандартным схемам управления питанием окно **Электропитание** будет содержать созданную схему, которая автоматически задается в качестве активной. Первоначальная актив-

ная схема теперь находится в разделе под заголовком **Показать дополнительные схемы**, и отобразить ее можно, щелкнув по этой ссылке или круглой кнопке со стрелкой справа от нее.

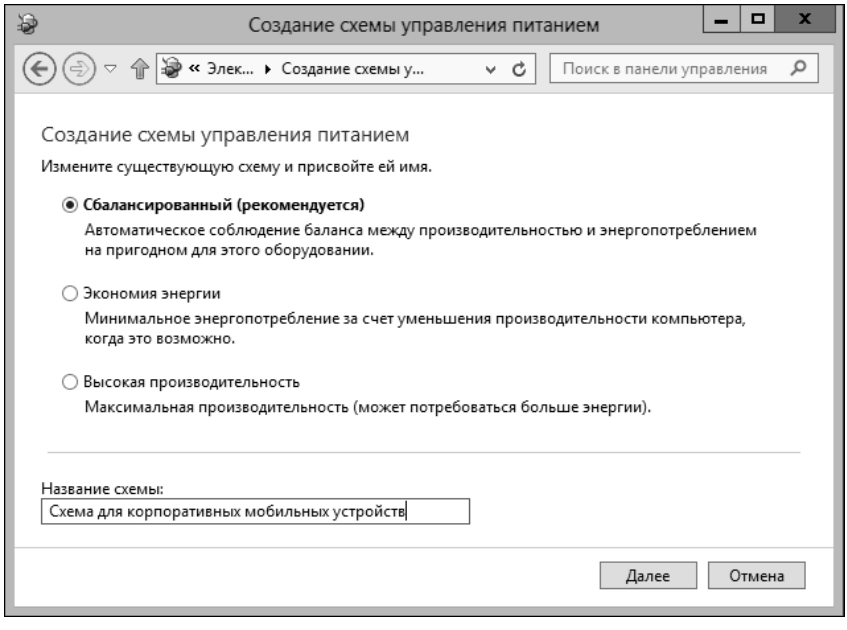


Рис. 2.24. Окно для создания схемы управления электропитанием

9. Созданная схема устанавливается активной по умолчанию. Щелкните по ссылке **Настройка плана электропитания этой схемы**, чтобы отобразить страницу **Изменение параметров схемы**, а затем по ссылке **Изменить дополнительные параметры питания**, чтобы отобразить окно **Электропитание** для настройки дополнительных параметров.
10. Настроив дополнительные параметры электропитания, нажмите кнопку **OK**, чтобы сохранить и применить их.

На компьютерах домена схемы управления электропитанием можно создавать с помощью редактора управления групповыми политиками в узле **Параметры** посредством следующей процедуры:

1. В редакторе управления групповыми политиками откройте для редактирования требуемый объект групповой политики. Для настройки параметров компьютера разверните узел **Конфигурация компьютера\Настройка\Параметры панели управления** и выберите узел **Электропитание**. Для настройки параметров пользователя разверните узел **Конфигурация пользователя\Настройка\Параметры панели управления** и выберите узел **Электропитание**.
2. Щелкните правой кнопкой мыши по узлу **Электропитание**, выберите в контекстном меню команду **Создать**, а затем щелкните по опции **Схема управления питанием (Windows Vista и выше)**. Откроется диалоговое окно **Добавление нового элемента схемы управления питанием**.
3. В списке **Действие** выберите опцию **Создать**. Для предварительной установки значений параметров схемы питания выберите стандартную схему, наиболее отвечающую требо-

ваниям создаваемой. Выбрав требуемую базовую схему, введите название создаваемой схемы в соответствующее поле.

4. Выберите в списке требуемую схему электропитания, например, **Сбалансированная**.
5. Чтобы сделать схему активной, установите ее флажок **Задать в качестве текущей схемы управления электропитанием**.
6. Настройте схему управления питанием, установив требуемые значения доступных для нее параметров.
7. Выполнив все требуемые настройки, нажмите кнопку **OK**, чтобы сохранить их. При следующем обновлении политики элемент настройки будет применен должным образом к объекту групповой политики, для которого он был определен.

Настройка общесистемных параметров кнопки питания и парольной защиты при выходе из спящего режима

Общесистемные параметры для управления электропитанием позволяют настроить действия при нажатии кнопки питания и парольную защиту при выходе из спящего режима для всех пользователей компьютера. Допустимые действия, которые можно задать для кнопки питания, — завершение работы, переход в режим гибернации или переход в спящий режим. Парольная защита заключается в настройке компьютера на запрос пароля при выходе из спящего режима, чтобы разблокировать экран.

Настроить общесистемные параметры можно таким образом:

1. В Панели управления щелкните по ссылке категории **Система и безопасность** и в открывшемся списке элементов этой категории выберите ссылку **Электропитание**.
2. В левой панели открывшего окна **Электропитание** щелкните по ссылке **Действие кнопок питания** (Choose what the power buttons do).
3. В открывшемся окне **Системные параметры** (System Settings) выберите в списке **Действие при нажатии кнопки питания** (When I press the power button) действие, которое требуется выполнять при нажатии кнопки питания, — **Действие не требуется**, **Сон**, **Гибернация**, **Завершение работы**. Но, несмотря на наличие значения параметра в списке, оно не может быть присвоено, если компьютер его не поддерживает.
4. В списке **При нажатии кнопки сна** (When I press the sleep button) выберите действие, которое требуется выполнять при нажатии кнопки перехода в спящий режим, — **Действие не требуется**, **Сон** или **Гибернация**. Опять же, несмотря на возможное наличие значения параметра в списке, оно не может быть присвоено, если компьютер его не поддерживает.
5. Если доступен параметр **Действие при закрытии крышки** (When I close the lid), установите и его значение — **Действие не требуется**, **Сон**, **Гибернация** или **Завершение работы**. Опять же, несмотря на возможное наличие значения параметра в списке, оно не может быть присвоено, если компьютер его не поддерживает.
6. Если опции для параметров кнопок питания и парольной защиты недоступны, нужно щелкнуть по ссылке **Изменение недоступных в данный момент параметров** (Change settings that are currently unavailable).
7. Чтобы задать требование пароля при выходе компьютера из спящего режима, нужно установить переключатель **Запрашивать пароль** (Require a password). Рекомендуется воспользоваться этой возможностью, чтобы обеспечить безопасность системы.

8. В разделе **Параметры завершения работы** (Shutdown settings) установите флажок **Включить быстрый запуск**, чтобы при выключении компьютера сохранять системную информацию в файл на системном диске. Этот файл затем считывается при запуске компьютера, чтобы ускорить процесс загрузки. При перезагрузке компьютера быстрый запуск не применяется.
9. В этом же разделе установите другие флажки, которые следует отображать при нажатии кнопки завершения работы Windows 8.
10. Установив требуемые настройки, нажмите кнопку **Сохранить изменения**, чтобы применить их.

Управление параметрами питания посредством настроек политик

Групповая политика содержит настройки для управления параметрами питания. Для их настройки требуется последовательно развернуть узлы политики **Конфигурация компьютера\Административные шаблоны\Система\Управление электропитанием** (Computer Configuration\Administrative Templates\System\Power Management). Узел **Управление электропитанием** содержит следующие вложенные узлы.

- **Параметры кнопок** (Button Settings). Содержит политики для настройки действий при нажатии кнопки питания и кнопки перехода в спящий режим и закрытия крышки при работе от батареи и от сети. Эти же параметры управляют действиями кнопки завершения работы на экране задач, который открывается при нажатии комбинации клавиш <Ctrl>+<Alt>+<Delete>.
- **Параметры жесткого диска** (Hard Disk Settings). Содержит политики для настройки отключения жестких дисков при питании от батареи и от сети.
- **Параметры уведомлений** (Notification Settings). Содержит политики для управления уведомлениями и действиями при низком уровне заряда батареи.
- **Параметры спящего режима** (Sleep Settings). Содержит политики для настройки состояний спящего режима для разрешенных устройств и приложений.
- **Параметры дисплея и видео** (Video and Display Settings). Содержит политики для настройки действий для экрана, яркости экрана и показа слайдов в качестве фона рабочего стола при питании от батареи и от сети.

Чтобы применить параметр политики, включите ее, а затем выберите требуемое действие.

Посредством групповой политики можно также задать активную схему управления электропитанием. Метод работы с политиками управления электропитанием зависит от того, какую схему питания следует применить — схему по умолчанию, обновленную стандартную или созданную и настроенную самостоятельно. Настроить все компьютеры, которые следуют определенной политике, на использование одной из схем управления питанием по умолчанию можно следующим образом:

1. В редакторе управления групповыми политиками откройте требуемый объект групповой политики и последовательно разверните узлы **Конфигурация компьютера\Административные шаблоны\Система\Управление электропитанием**.
2. В правой панели дважды щелкните на политике **Выбрать текущую схему управления питанием** (Select an active power plan).
3. В открывшемся одноименном окне установите переключатель **Включить**, а затем в списке **Текущая схема управления питанием** (Active Power Plan) выберите одну из сле-

дующих доступных схем: **Автомат** (Automatic), **Высокая производительность** (High Performance), **Экономия электроэнергии** (Power Saver). Для значения **Автомат** Windows 8 в большинстве случаев применяет схему управления **Сбалансированный**.

4. Выполнив все требуемые настройки, нажмите кнопку **OK**, чтобы сохранить их.

Настроить все компьютеры, которые следуют определенной политике, на использование одной из обновленных стандартных или созданных и настроенных самостоятельно схем управления питанием можно следующим образом:

1. В редакторе управления групповыми политиками откройте требуемый объект групповой политики и последовательно разверните узлы **Конфигурация компьютера\Административные шаблоны\Система\Управление электропитанием**.
2. В правой панели дважды щелкните на политике **Указать пользовательскую текущую схему управления питанием** (Specify a custom active power plan)
3. В открывшемся одноименном окне установите переключатель **Включить**. В текстовое поле **Пользовательская текущая схема управления питанием (GUID)** (Custom Active Power Plan (GUID)) введите идентификатор GUID требуемой схемы.
4. Нажмите кнопку **OK**, чтобы сохранить изменения.

> ***Совет***
>
> Узнать идентификатор GUID схемы управления электропитанием можно, выполнив команду `powercfg -l` в командной строке с правами администратора. Исполнение этой команды выводит список схем управления электропитанием, сконфигурированных на компьютере.

Использование уведомлений и настройка действий по уведомлениям

Политики уведомлений определяют подачу сигнала тревоги или вывод предупреждающего сообщения мобильным устройством, когда заряд его батареи понижается до определенного уровня. Для мобильных устройств можно настроить три уровня уведомлений.

- **Уведомление о низком заряде батареи** (Low battery alarm). Это уведомление оповещает пользователя о низком уровне заряда батареи. Состояние низкого уровня заряда активируется по умолчанию, когда уровень заряда батареи составляет 10% от ее полной емкости. Например, для батареи, время работы которой при полном заряде составляет 8 часов, 10% оставшегося заряда равно около 48 минутам работы.
- **Уведомление о почти полной разрядке батареи** (Critical battery alarm). Это уведомление оповещает пользователя о том, что заряд батареи на исходе. Состояние почти полной разрядки батареи активируется по умолчанию, когда уровень заряда батареи составляет 3% или меньше от ее полной емкости. Например, для батареи, время работы которой при полном заряде составляет 8 часов, 3% оставшегося заряда равно около 14 минутам работы.
- **Уведомление о резервном уровне заряда батареи** (Reserve battery alarm). Это уведомление оповещает пользователя о том, что используется резерв заряда батареи. Состояние резерва заряда активируется по умолчанию, когда уровень заряда батареи составляет 1% от ее полной емкости. Например, для батареи, время работы которой при полном заряде составляет 8 часов, 1% оставшегося заряда равен около 5 минутам работы.

Действия уведомления низкого и почти полного разряда позволяют задать конкретное действие, которое следует предпринять системе при понижении заряда до соответствующего

уровня. Возможные действия включают завершение работы компьютера, переход в спящий режим или в режим гибернации. Начиная с Windows Vista, извещения низкого уровня заряда батареи можно отключать, установив политику **Отключить уведомление о низком заряде батарей** (Turn off low batter user notification). В Windows 8 было добавлено уведомление для оповещения о резервном уровне заряда батарей. Так как при настройке разных уровней уведомления во внимание принимаются разные соображения, то каждое из этих уведомлений рассматривается отдельно в последующих разделах.

Настройка уведомления и действий низкого заряда батареи

Как упоминалось ранее, уведомление низкого заряда батареи предупреждает о низком уровне энергоресурсов системы. При переходе в состояние низкого энергопотребления система оповещает пользователя об этом либо только текстовым сообщением, либо текстовым сообщением со звуковым сигналом. В некоторых случаях может иметь смысл вдобавок вместо выдачи предупреждения настроить компьютер на дополнительное действие — переход в режим ожидания.

Настроить уведомления и действия для низкого уровня заряда батареи можно следующим образом:

1. В редакторе объектов уровня зарядки групповой политики откройте требуемый объект групповой политики и последовательно разверните узлы **Конфигурация компьютера\Административные шаблоны\Система\Управление электропитанием** и выберите в последнем подузел **Параметры уведомлений**.
2. В правой панели дважды щелкните на политике **Действие уведомления о низком заряде батарей** (Low battery notification action). В открывшемся одноименном окне установите переключатель **Включить** и выберите требуемое действие, например, **Сон**. Нажмите кнопку **OK**, чтобы сохранить настройку.
3. Чтобы задать уровень активирования уведомления, в правой панели дважды щелкните на политике **Уровень уведомления о низком заряде батарей** (Low battery notification level). В открывшемся одноименном окне установите переключатель **Включить** и с помощью счетчика **Уровень уведомления о низком заряде батарей** задайте уровень заряда батарей для срабатывания уведомления. Нажмите кнопку **OK**, чтобы сохранить настройки.

> ***Совет***
>
> Устанавливаемый по умолчанию уровень уведомления о низком заряде батарей основан на полном заряде батареи и обычно составляет 10% от полного заряда. Для большинства систем этого достаточно. Но автор обнаружил, что для некоторых систем, особенно систем с батареей низкого качества, это значение слишком низкое, и требуется 12—15%. С другой стороны, на системах с низким энергопотреблением или с двумя батареями значение по умолчанию слишком высокое. В таких случаях его следует откорректировать таким образом, чтобы оповещать пользователя, когда оставшегося заряда достаточно, скажем, для 20 мин работы.

Настройка уведомлений и действий почти полной разрядки батареи

Целью уведомлений о почти полной разрядке батареи является обеспечение перехода системы в соответствующий режим работы перед тем, как батарея полностью разрядится. При переходе в состояние почти полной разрядки батареи система оповещает об этом пользователя, а затем переходит в спящий режим. В спящем режиме компоненты компьютера с управляемым энергопотреблением отключаются с целью понижения энергопотребления.

Но на перевод компьютера в режим сна лучше настроить уведомления низкого заряда батареи, а уведомления о почти полной разрядке батареи настроить на перевод компьютера в режим гибернации или выключение. Такой подход к конфигурации уведомлений улучшает управление энергопотреблением и содействует сбережению состояния системы перед тем, как батарея полностью разрядится.

Настроить действия уведомления о почти полной разрядке батареи можно следующим способом:

1. В редакторе объектов групповой политики откройте требуемый объект групповой политики и последовательно разверните узлы **Конфигурация компьютера\Административные шаблоны\Система\Управление электропитанием** и выберите в последнем подузел **Параметры уведомлений**.
2. В правой панели дважды щелкните на политике **Действие уведомления о почти полной разрядке батарей** (Critical battery notification action). В открывшемся одноименном окне установите переключатель **Включить** и выберите требуемое действие, например, **Гибернация** или **Завершение работы**. Нажмите кнопку **OK**, чтобы сохранить настройки.
3. Чтобы задать уровень активирования уведомления, в правой панели дважды щелкните на политике **Уровень уведомления о почти полной разрядке батарей** (Critical battery notification level). В открывшемся одноименном окне установите переключатель **Включить** и с помощью счетчика **Уровень уведомления о почти полной разрядке батарей** задайте уровень заряда батарей для срабатывания уведомления. Нажмите кнопку **OK**, чтобы сохранить настройки.

> ***Совет***
>
> Устанавливаемый по умолчанию уровень уведомления о почти полной разрядке батарей основан на полном заряде батареи и обычно составляет 3% от полного заряда. В большинстве случаев этого достаточно. Но если планируется переводить компьютер в режим гибернации или выключать его, это значение рекомендуется уменьшить. Также следует принять во внимание емкость батарей. В случае большой емкости значение по умолчанию обычно завышено, а в случае малой оно может быть недостаточно высоким. Уведомление почти полной разрядки батарей рекомендуется настраивать таким образом, чтобы его действие активировалось, когда оставшегося заряда достаточно на 6—8 мин работы.

Настройка уведомления резервного уровня заряда батарей

Уведомление резервного заряда батареи оповещает пользователя о том, что используется резерв заряда батареи. Настроить уведомление резервного заряда батареи можно следующим образом:

1. В редакторе объектов групповых политик откройте требуемый объект групповой политики и последовательно разверните узлы **Конфигурация компьютера\Административные шаблоны\Система\Управление электропитанием** и выберите в последнем подузел **Параметры уведомлений**.
2. Чтобы задать уровень активирования уведомления, в правой панели дважды щелкните политику **Уровень уведомления резервной батареи** (Reserve battery notification level). В открывшемся одноименном окне установите переключатель **Включить** и с помощью счетчика **Уровень уведомления резервной батареи** установите уровень заряда батарей для срабатывания уведомления. Нажмите кнопку **OK**, чтобы сохранить настройки.

ГЛАВА 3

Настройка рабочего стола и пользовательского интерфейса

Администраторам часто приходится помогать пользователям с настройкой их рабочих столов и пользовательских параметров. Операционная система Windows 8 располагает многими возможностями для настройки рабочего стола и экрана. Умелое применение этих возможностей приносит значительную пользу, а неумелое способно вызвать проблемы, для устранения которых пользователь будет вынужден обращаться за помощью к администратору. В связи с этим в данной главе рассматривается настройка и диагностирование:

- параметров компьютера, панели задач и панели инструментов;
- тем и фона рабочего стола;
- индивидуализированного содержимого рабочего стола;
- экранных заставок;
- вида и параметров экрана.

Оптимизация параметров компьютера

Экран **Параметры** компьютера и связанные страницы предназначены для предоставления легкого доступа к параметрам, широко применяемый для настройки пользовательского интерфейса и метода использования приложений. Открыть экран **Параметры** компьютера можно одним из следующих способов:

- на устройствах с сенсорным интерфейсом проведите пальцем справа к центру экрана, коснитесь кнопки **Параметры**, а затем — **Изменение параметров компьютера**;
- на устройствах с традиционным вводом нажмите комбинацию клавиш <Windows>+<I>, а затем выберите пункт **Изменение параметров компьютера**.

На рис. 3.1 показан пример экрана **Параметры**. Переход между страницами экрана осуществляется щелчком по имени требуемой страницы. Каждый пользователь, вошедший в систему под индивидуальным именем, имеет отдельный набор параметров.

В следующих разделах этой главы обсуждаются ключевые области операционной системы, которые можно настраивать, используя эти страницы и параметры. Но следует иметь в виду, что в зависимости от используемого вычислительного устройства конкретные страницы и параметры могут быть разными.

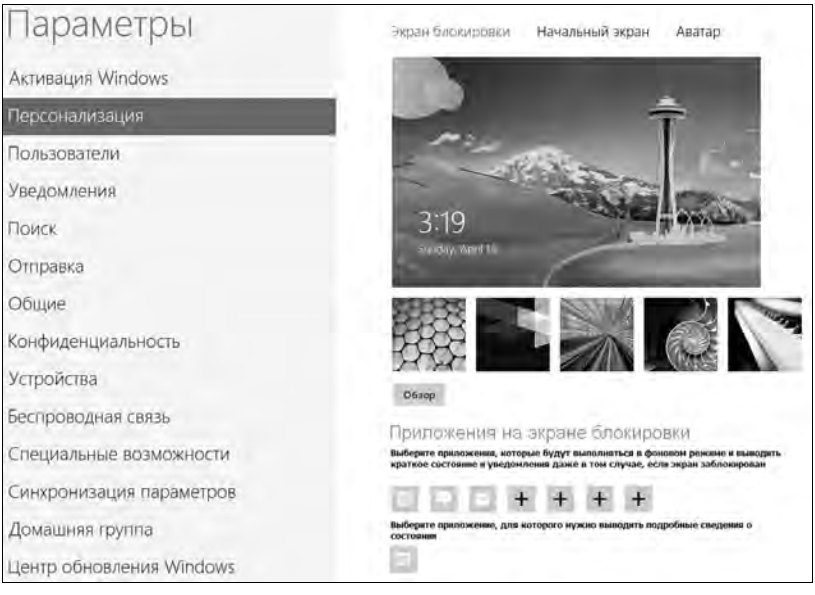


Рис. 3.1. Экран **Параметры** компьютера для настройки пользовательского интерфейса

Примечание

В этом разделе применяется термин "приложения рабочего стола" (desktop apps), в противоположность традиционным программам, запускающимся с рабочего стола. Дополнительную информацию о приложениях рабочего стола *см. в главе 8*.

Страница *Персонализация*

Страница **Персонализация** применяется для настройки экрана блокировки, экрана **Пуск** и аватара учетной записи. Переход между этими областями конфигурации выполняется щелчком по соответствующему названию.

Настройка экрана блокировки

Для экрана блокировки можно выбрать изображение фона, щелкнув по миниатюре одного из предлагаемого изображения. Чтобы выбрать другое изображение, нажмите кнопку **Обзор**, а затем с помощью предоставленных средств навигации по файловой системе компьютера выберите требуемое изображение.

Некоторые приложения рабочего стола, называющиеся приложениями экрана блокировки, могут исполняться в фоновом режиме и быстро выводят информацию о своем статусе и другие извещения даже при заблокированном экране. Обычно приложения сообщений, почты и календаря настроены на такой режим работы по умолчанию. Но и другие программы, установленные на компьютере, также, возможно, имеют функциональность для отображения своего состояния и вывода сообщений на экран блокировки. Такие приложения можно добавить на экран блокировки, щелкнув по одному из значков "плюс" в разделе **Приложения на экране блокировки** (Lock screen apps) и выбрав в открывшемся списке требуемое приложение рабочего стола. Чтобы удалить приложение экрана блокировки, щелкните по его значку и в открывшемся списке выберите опцию **Не выводить здесь краткие сведения о состоянии** (Don't show quick status here).

Некоторые приложения рабочего стола, такие как Календарь и Погода, могут выводить подробные сведения на экран блокировки, но обычно активным может быть только одно такое приложение. Это приложение обозначается значком под текстом "Выберите приложение, для которого нужно выводить подробные сведения о состоянии" (Choose an app to display detailed status). Если такое приложение еще не было выбрано, то можно щелкнуть на значке "плюс" и выбрать в открывшемся списке требуемое приложение рабочего стола. Чтобы удалить приложение с выводом подробных сведений о состоянии, щелкните по его значку и в открывшемся списке выберите опцию **Не показывать подробное состояние на экране блокировки** (Don't show detailed status on the lock screen).

Персонализация экрана *Пуск* и аватара учетной записи

Персонализация экрана **Пуск** заключается в выборе стиля и цвета его фона. Для этого щелкните по одному из значков стиля в виде больших квадратов. Выбор цвета фона осуществляется щелчком по соответствующему квадрату меньшего размера в горизонтальной линейке цветов или же перемещением ползунка по этой линейке.

Для аватара можно использовать любое изображение. По умолчанию используется силуэт человека. Чтобы поместить другое изображение, нажмите кнопку **Обзор**, а затем с помощью предоставленных средств навигации по файловой системе компьютера выберите требуемое изображение.

Если к компьютеру подключена камера, изображение для аватара можно создать, щелкнув на значке **Камера**, а затем выполнить предлагаемые инструкции.

Страница *Пользователи*

Страница **Пользователи** в основном применяется для управления учетной записью текущего пользователя. Если вход в систему был выполнен с учетной записью Microsoft, предоставляется опция переключения на вход в систему с локальной учетной записью, и наоборот.

В разделе **Параметры входа** (Sign-in options) можно создать графический пароль для текущего пользователя (если это разрешено в групповой политике). Также можно потребовать ввода пароля при выходе компьютера из спящего режима.

Для рабочих или домашних групп имеются две дополнительные опции входа. В частности, можно изменить пароль текущего пользователя, а также создать или изменить PIN-код. Дополнительную информацию по работе с учетными записями пользователя *см. в главе 7*.

Страница *Уведомления*

Многие приложения могут выдавать уведомления, управление которыми осуществляется на странице **Уведомления**. В частности, применяются следующие элементы управления верхнего уровня:

- **Показывать уведомления приложений** (Show app notifications) — определяет вывод уведомлений приложениями на экран **Пуск** и на рабочий стол;
- **Выводить уведомления приложений на экране блокировки** (Show app notifications on the lock screen) — определяет вывод уведомлений приложениями на экран блокировки;
- **Воспроизводить звуки уведомления** (Play notification sounds) — задает воспроизведение звуков при выводе уведомлений.

Щелчок по элементу управления включает или выключает соответствующее действие. В списке ниже также можно включить или выключить вывод уведомлений для отдельных приложений.

Страницы *Поиск*, *Отправка* и *Общие*

На странице **Поиск** (Search) настраивается способ работы функциональности поиска. Операционная система Windows 8 ведет журнал поисков, с помощью которого можно определить наиболее часто затребованные приложения и выводить их в числе первых результатов поиска, а также сохранять результаты поиска для вывода предлагаемых вариантов при следующих поисках. С помощью опций журнала поиска эти функциональности можно изменить или удалить текущее содержимое журнала поиска.

При поиске приложений рабочего стола, кроме поиска приложений, Windows также выполняет поиск данных, хранящийся в этих приложениях. Определенные приложения, такие как Почта, Музыка, Фотоальбом и Новости, настроены для поиска; также предоставлена возможность включать и отключать возможность поиска для каждого отдельного приложения рабочего стола, щелкнув по значку требуемого приложения.

Также определенные приложения могут быть настроены для быстрого предоставления общего доступа к фотографиям, документам и прочим файлам. Настройка общего доступа к документам осуществляется на странице **Отправка** (Share). Операционная система Windows отслеживает такие приложения и может отображать их в списке очередности. По умолчанию этот список может содержать до пяти приложений рабочего стола. Изменить количество приложений в списке можно, выбрав в раскрывающемся списке **Элементы в списке** (Items in list) необходимое число. Список сбрасывается нажатием кнопки **Очистить список** (Clear list).

Определенные приложения, такие как Почта и Люди, настроены для автоматического предоставления общего доступа. Возможность предоставления общего доступа можно контролировать отдельно для каждого приложения, щелкнув по значку требуемого приложения.

Приложения рабочего стола могут использовать местонахождение, имя и аватар пользователя. Применяемые для этого параметры можно настроить на странице **Конфиденциальность** (Privacy), щелкнув по значку требуемого типа информации, чтобы включить или отключить возможность ее использования в приложениях рабочего стола.

Совет

На странице **Общие** в разделе **Переключение приложений** (App switching) можно контролировать возможность переключения между недавно применявшимися приложениями рабочего стола. Когда эта возможность включена, Windows 8 ведет журнал недавно используемых приложений. Содержимое этого журнала можно очистить, нажав кнопку **Удалить журнал** (Delete history).

Страница *Синхронизация параметров*

Текущие пользователи, владельцы учетной записи Microsoft, могут контролировать синхронизацию параметров между устройствами на странице **Синхронизация параметров** (Sync your settings). Синхронизировать можно следующие параметры:

- пользовательские параметры на странице **Персонализация**;
- параметры рабочего стола для тем, панели инструментов и др.;
- пароли входа для некоторых приложений, веб-сайтов, сетей и домашних групп;
- параметры специальных возможностей (Ease of Access) и настройки языка;
- настройки журнала и закладки браузера;
- другие параметры для Проводника Windows, мыши и т. п.

Опция **Синхронизация параметров на этом компьютере** (Sync settings on this PC) контролирует возможность синхронизации на высшем уровне. Сброс этой опции отключает воз-

можность синхронизации всех параметров для устройств. Чтобы разрешить синхронизацию некоторых или всех параметров, эту опцию нужно включить.

При разрешенной синхронизации параметры для синхронизации между устройствами задаются посредством опций раздела **Синхронизируемые параметры** (Settings to sync). Операционная система Windows 8 может определить использование тарифного подключения, например, к сотовой сети. На странице синхронизации параметров имеется возможность контролировать синхронизацию параметров по тарифному подключению вообще, а также для ситуаций, когда тарифное подключение работает в режиме роуминга.

Работа с приложениями автозапуска и рабочего стола

В операционной системе Windows элементы рабочего стола и приложения автозапуска имеют ярлыки, способ использования которых зависит от их местонахождения исходного элемента, на который указывает ярлык. Например, чтобы запускать приложения автозапуска для всех пользователей, можно создать ярлык, указывающий на папку *%SystemDrive%*\ ProgramData\Microsoft\Windows\Главное меню\Программы\Автозагрузка. Теперь эти приложения будут запускаться автоматически при локальном входе в систему любого пользователя. А чтобы запускать приложения автозапуска для определенного пользователя, можно создать ярлык, указывающий на папку *%UserProfile%*\AppData\Roaming\Microsoft\Windows\ Главное меню\Программы\Автозагрузка.

Создание ярлыков для приложений автозапуска, рабочего стола и других элементов

Ярлыки пользователя для обычных приложений и приложений автозапуска, а также для папок можно создавать в требуемом месте в Проводнике Windows, выполнив вход в систему. С помощью групповой политики можно создавать ярлыки для обычных приложений, приложений автозапуска и для других объектов в элементе **Ярлыки** узла **Параметры**. Эти ярлыки применяются автоматически ко всем пользователям и компьютерам, которые обрабатывают соответствующий объект групповой политики.

Настроить ярлыки посредством узла **Настройка** можно так:

1. В редакторе управления групповыми политиками откройте для редактирования требуемый объект групповой политики. Для настройки параметров компьютера разверните узел **Конфигурация компьютера\Настройка\Конфигурация Windows** и выберите узел **Ярлыки**. Для настройки параметров пользователя разверните узел **Конфигурация пользователя\Настройка\Конфигурация Windows** и выберите узел **Ярлыки**.
2. Щелкните правой кнопкой мыши по узлу **Ярлыки**, выберите в контекстном меню команду **Создать**, а затем — **Ярлык**. Откроется диалогового окно свойств для создаваемого ярлыка (рис. 3.2).
3. В раскрывающемся списке **Действие** выберите требуемую опцию: **Создать**, **Обновить** или **Заменить**. Затем установите другие параметры, как рассмотрено ранее в этом разделе.
4. Для управления способом применения настройки задаются опции на вкладке **Общие**. Часто действия, выполняемые ярлыком, требуется запускать только один раз. В таких случаях устанавливается флажок **Применить один раз и не применять повторно**.

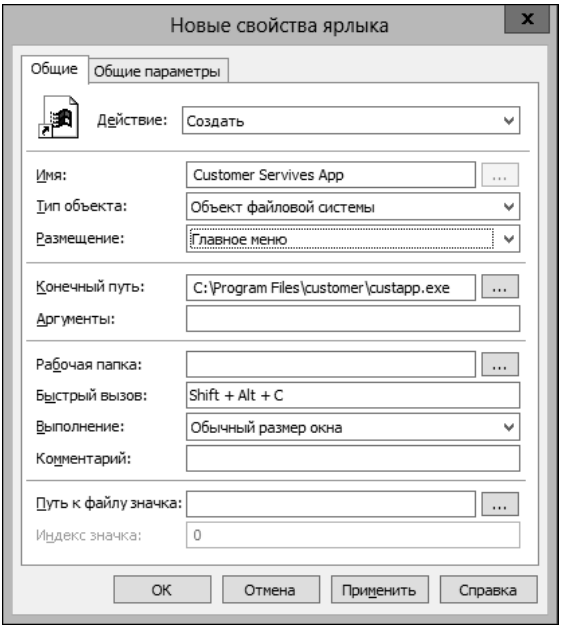


Рис. 3.2. Окно свойств ярлыка, создаваемого посредством групповой политики

5. Нажмите кнопку **OK**, чтобы сохранить настройки. При следующем обновлении политики элемент настройки будет применен должным образом к объекту групповой политики, для которого он был определен.

Раскрывающийся список **Размещение** (Location) содержит перечень специальных папок, которые можно использовать с ярлыками (табл. 3.1).

Таблица 3.1. *Специальные папки, используемые с ярлыками*

Папка	**Назначение**
AllUsers\Рабочий стол (AllUser\Desktop)	Ярлыки приложений рабочего стола для всех пользователей
AllUsers\Избранное (AllUsers\Explorer Favorites)	Закладки IE для всех пользователей
AllUsers\Программы (AllUsersPrograms)	Опции меню программ для всех пользователей
AllUsers\Главное меню (AllUsers\Start Menu)	Опции меню **Пуск** для всех пользователей
AllUsers\Автозагрузка (AllUsers\Startup)	Приложения автозапуска для всех пользователей
Рабочий стол (Desktop)	Ярлыки рабочего стола для определенного пользователя
Избранное Internet Explorer (Explorer Favorites)	Избранное IE для определенного пользователя
Ссылки Internet Explorer (Explorer Links)	Ссылки IE для определенного пользователя
Сетевое окружение (MyNetworkPlaces)	Ярлыки сетевого окружения для определенного пользователя

Таблица 3.1 *(окончание)*

Папка	Назначение
Программы (Programs)	Опции меню программ для определенного пользователя
Панель быстрого запуска (QuickLaunchToolbar)	Папка панели инструментов с ярлыками для определенного пользователя
Недавние (Recent)	Ярлыки последних применяемых документов для определенного пользователя
Отправить (SendTo)	Ярлыки меню **Отправить** для определенного пользователя
Главное меню (StartMenu)	Ярлыки меню **Пуск** для определенного пользователя
Автозагрузка (Startup)	Приложения автозапуска для определенного пользователя

Ярлыки могут указывать на локальные и сетевые файлы, а также на удаленные интернет-ресурсы. Ярлыки для локальных или сетевых файлов называются *ярлыками-ссылками* (link-shortcuts), а ярлыки для удаленных интернет-ресурсов — *URL-ярлыками* (URL shortcuts).

Ярлыки-ссылки обычно применяются для запуска приложений или открытия документов, а не для доступа к удаленным ресурсам посредством браузера. По этой причине свойства ярлыков-ссылок отличаются от свойств UTL-ярлыков. В табл. 3.2 приводятся названия свойств ярлыков ссылок, их краткие описания и примеры значений.

Таблица 3.2. *Свойства ярлыков-ссылок*

Свойство	Описание	Пример значения
Аргументы (Arguments)	Аргументы для передачи приложению, запускаемому посредством ярлыка	C:\Приступая_к_работе.doc
Комментарии (Comments)	Описательный комментарий для ярлыка	Открывает документ "Приступая к работе"
Путь к файлу значка (Icon File Path)	Задает расположение значка ярлыка. Если не установлено, используется значок по умолчанию	C:\Program Files\ InternetExplorer\Iexplore.exe
Индекс значка (Icon Index)	Задает позицию индекса значка ярлыка. Так как немногие приложения имеют несколько индексированных значков, значение индекса почти всегда равно 0	0
Размещение (Location)	Задает место, где нужно расположить ярлык	Рабочий стол
Имя (Name)	Задает имя ярлыка	Приступая к работе
Выполнение (Run)	Задает стиль окна приложения, запускаемого ярлыком. Доступные стили — **Обычный размер окна** (Normal Window), **Свернутое в значок** (Minimized) и **Развернутое на весь экран** (Maximized)	Обычный размер окна
Быстрый вызов (Shortcut Key)	Задает последовательность клавиш (hotkeys) для активирования ярлыка. Это свойство применимо только с ярлыками рабочего стола и опциями меню **Пуск**	<Alt>+<Shift>+<Z>
Рабочая папка (Start In)	Задает рабочую папку приложения, запускаемого ярлыком	C:\Working

Таблица 3.2 *(окончание)*

Свойство	Описание	Пример значения
Конечный путь (Target Path)	Задает путь исполняемого файла	*%WinDir%*\Notepad.exe
Тип объекта (Target Type)	Задает тип создаваемого ярлыка. Доступные значения **— Объект файловой системы** (File system Object) для ярлыков ссылок, **URL-адрес** (URL) для ярлыков URL **и Объект оболочки** (Shell Object) для ярлыков оболочки Проводника	Объект файловой системы

Если для ярлыка задано неправильное свойство или свойство, неподдерживаемое приложением, на которое указывает ярлык, возможно, что ярлык не будет создан. А если все-таки создан будет, то, скорее всего, не станет работать так, как ожидает пользователь. В таком случае следует создать ярлык повторно.

Одним из наиболее полезных свойств ярлыка является свойство **Аргументы** (Arguments). Посредством его можно передавать аргументы в запускаемое ярлыком приложение. Используя это свойство, можно создать ярлык, который запускает Microsoft Word и открывает определенный документ. Для этого в свойстве **Конечный путь** (Target Path) нужно указать путь к исполняемому файлу MS Word, а в свойстве **Аргументы** — путь и имя документа, который нужно открыть.

Для ярлыков меню или рабочего стола можно задать комбинацию клавиш быстрого вызова, нажатие которой активирует ярлык. Определение комбинации клавиш быстрого вызова должно содержать, по крайней мере, одну клавишу-модификатор (modifier key) и одну клавишу-указатель (designator key). Доступны следующие клавиши-модификаторы:

- ALT — клавиша <Alt>;
- CTRL — клавиша <Ctrl>;
- SHIFT — клавиша <Shift>.

Можно задавать любую комбинацию клавиш-модификаторов, например, <Alt>+<Ctrl> или <Shift>+<Ctrl>, но комбинация не должна повторять комбинации клавиш, используемые для других ярлыков. В качестве клавиш-указателей можно использовать клавиши букв (A—Z) и цифр (0—9), а также клавиши <End>, <Home>, <Page Up> и <Page Down>. Вот пример комбинации клавиш: <Shift>+<Alt>+<G>.

Приложения обычно имеют значок по умолчанию, который используется в качестве значка для ярлыка данного приложения. Например, для значка ярлыка для Internet Explorer по умолчанию используется значок самой программы Internet Explorer. Для значков ярлыков документов в большинстве случаев по умолчанию служит значок их соответствующих приложений.

С помощью свойства **Путь к файлу значка** (Icon Location) ярлыку можно присвоить значок, отличающийся от значка по умолчанию. Обычно, место нахождения значка соответствует имени приложения, например, Iexplore.exe или notepad.exe, а значение индекса значка равно 0. В таком случае операционная система должна найти исполняемый файл ярлыка. Если исполняемый файл отсутствует по указанному пути, задать значок не получится. По этой причине в обязательном порядке следует ввести полный путь к исполняемому файлу.

В качестве папки по умолчанию для приложения служит текущая рабочая папка. Эти папка используется при первом открытии или сохранении файла.

Ярлыки URL открывают интернет-документы, используя соответствующие приложения. Например, веб-страницы открываются в браузере по умолчанию, таком как Internet Explorer.

Для ярлыков URL не применимы свойства **Аргументы**, **Рабочая папка**, **Выполнение** и **Комментарии**.

Добавление и удаление приложений автозапуска

Установленными администратором или пользователями приложениями, которые исполняются в фоновом режиме, можно управлять посредством папки **Автозагрузка**. Программы автозапуска, которые доступны только текущему пользователю, размещаются в папке **Автозагрузка**, которая находится в профиле данного пользователя (*%UserProfile%*\AppData\Roaming\Microsoft\Windows\Главное меню\Программы), а программы автозапуска, которые доступны для всех пользователей, находятся в папке **Автозагрузка** в профиле для всех пользователей (*%SystemDrive%*\ProgramData\Microsoft\Windows\Главное меню\Программы).

Чтобы добавить или удалить программы автозапуска для всех пользователей, следуйте этой процедуре:

1. В Проводнике откройте скрытую папку *%SystemDrive%*\ProgramData\Microsoft\Windows\Главное меню. Чтобы отображать скрытые объекты файловой системы, в Проводнике выберите меню **Представление** и на ленте этого меню установите флажок **Скрытые элементы** (Hidden items).
2. В папке **Главное меню** откройте папку **Программы**, а в ней — папку **Автозагрузка**.
3. Теперь можно добавлять и удалять программы автозапуска для всех пользователей. Для добавления программы автозапуска создайте для нее ярлык в папке **Автозагрузка**, а для удаления — удалите ее ярлык из этой папки.

Для добавления или удаления программы автозапуска для определенного пользователя применяется следующая процедура:

1. Выполните вход в систему с учетной записью пользователя, для которого нужно управлять приложениями автозапуска. В Проводнике откройте скрытую папку *%UserProfile%*\AppData\Roaming\Microsoft\ Windows\Главное меню.
2. В папке **Главное меню** откройте папку **Программы**, а в ней — папку **Автозагрузка**.
3. Теперь можно добавлять и удалять программы автозапуска для данного пользователя. Для добавления программы автозапуска создайте для нее ярлык в папке **Автозагрузка**, а для удаления — удалите ее ярлык из этой папки.

> ***Примечание***
>
> Технически для управления программами автозапуска определенного пользователя выполнять вход в систему с учетной записью этого пользователя не обязательно, но это значительно облегчает задачу. Если выполнить вход в систему с учетной записью требуемого пользователя невозможно, откройте папку Пользователи на системном диске, а в ней — папку профиля требуемого пользователя. Имена папок профилей пользователей соответствуют именам их учетных записей.

С помощью настроек групповой политики можно задавать приложения для автоматического запуска при входе пользователя в систему, создавая соответствующие ярлыки в папках AllUsers\Автозагрузка и Автозагрузка. В папке AllUsers\Автозагрузка задаются приложения, автоматически запускаемые для всех пользователей, которые выполняют вход в систему, а в папке Автозагрузка — приложения автозапуска для текущего пользователя.

Для нового созданного ярлыка приложения автозапуска в большинстве случаев нужно задать только такие свойства, как **Имя**, **Тип объекта**, **Размещение** и **Конечный путь**. Иногда еще может потребоваться указать рабочую папку для приложения или задать параметры запуска.

Приложение автозапуска удаляется выбором в меню **Действие** опции **Удалить**.

Настройка панели задач

Панель задач предоставляет быстрый доступ к часто запрашиваемой информации и приложениям. Поведение и свойства панели задач можно модифицировать разными способами, основные из которых рассматриваются в этом разделе.

Основные сведения о панели задач

Панель задач является наименее ценимой областью рабочего стола Windows. Несмотря на ежедневное интенсивное использование этой панели для доступа практически ко всем аспектам работы с операционной системой Windows, пользователи и администраторы склонны обходить вниманием ее настройку. А ведь если пользователи часто испытывают трудности с доступом к возможностям Windows или с исполнением приложений, им можно помочь в этом, настроив панель задач под их работу. Несколько панелей инструментов, из которых состоит панель задач Windows, могут послужить пользователю многими разными способами.

Иногда можно значительно повысить производительность, просто добавив часто используемый объект на панель задач. Например, большинство людей тратит много времени на поиск и чтение документов. Они просматривают веб-сайты или сайты корпоративных сетей в поисках самой свежей информации. Для поиска каждого из таких документов часто применяется отдельный подход, а для открытия запускают отдельное приложение, такое как Microsoft Word, Excel, PowerPoint и т. п. Но добавив в панель задач панель **Адрес**, можно получить прямой доступ к документам и запускать требуемое для их открытия приложение автоматически. Все, что для этого нужно сделать — это ввести путь документа и нажать клавишу <Enter>. Со временем журнал панели **Адрес** накапливает адреса документов, с которыми ранее работал пользователь, и это облегчает задачу нахождения требуемой пользователем информации.

Закрепление ярлыков на панели задач

Операционная система Windows 8 не имеет панели быстрого запуска. Вместо этого она позволяет закреплять ярлыки часто используемых программ непосредственно на панели задач в любое время при работе в экране **Пуск**. Для этого нужно просто щелкнуть правой кнопкой мыши на объекте и на панели меню внизу экрана выбрать опцию **Закрепить на панели задач** (Pin to taskbar). Закрепленный на панели задач ярлык можно разместить в требуемом месте, перетаскивая его мышью. Чтобы удалить ярлык с панели задач, щелкните на нем правой кнопкой мыши и в контекстном меню выберите команду **Изъять программу из панели задач** (Unpin this program form taskbar).

Изменение размера и положения панели задач

По умолчанию панель задач расположена внизу вдоль экрана и имеет высоту в один значок. Если панель задач не закреплена, ее можно разместить вдоль любой стороны экрана и изменить размер как требуется. Чтобы разместить панель задач на другой стороне экрана, просто перетащите ее мышью к требуемой стороне. В процессе перетаскивания панель задач остается на прежнем месте, пока указатель мыши не пройдет большую часть пути к новому месту; тогда панель задач отображается уже там, и кнопку мыши можно отпустить. Чтобы изменить ширину панели задач, разместите указатель мыши над ее кромкой, чтобы он принял форму двунаправленной стрелки, после чего нажмите левую кнопку мыши и перетащите край панели задач вверх или вниз (или вправо/влево, если панель расположена у бокового края рабочего стола).

Автоматическое скрытие, закрепление и управление отображением панели задач

Отображением панели задач можно управлять несколькими способами. Прежде всего, можно включить возможность автоматического скрытия панели задачи, когда она не используется. Затем панель задач можно закрепить, чтобы ее нельзя было перемещать или изменять ее размеры. Кроме этого, панель задач можно настроить на отображение в конкретном месте с определенным внешним видом. Разместив панель задач в требуемом месте и установив необходимый размер, ее следует закрепить, чтобы пользователи случайно не сбили ее настройки.

Для настройки панели задач следуйте этой процедуре:

1. Щелкните правой кнопкой мыши на панели задач и в контекстном меню выберите команду **Свойства** (Properties).
2. На вкладке **Панель задач** (Taskbar) открывшегося окна **Свойства панели задач** (Taskbar Properties) выберите требуемые параметры внешнего вида панели задач. В частности, здесь можно закрепить панель задач, включить функциональность автоматического скрытия, а также задать использование маленьких значков.
3. В списке **Положение панели задач на экране** (Taskbar location on screen) можно задать расположение панели задач вдоль одной из сторон рабочего стола — внизу, слева, справа или вверху.
4. В списке **Кнопки панели задач** (Taskbar buttons) задается способ отображения значков и их меток на панели задач. При выборе опции **Всегда группировать, скрывать метки** (Always combine, hide labels) значки принимают форму квадратов, названия их программ на значках не отображаются, а значки одного типа (например, несколько открытых документов Word) группируются под одним значком. При выборе опции **Группировать при заполнении панели задач** (Combine when taskbar is full) значки принимают прямоугольную форму, на них отображаются названия их программ, и значки одинакового типа группируются под одним значком только при заполнении панели задач. Опция **Никогда не группировать** (Never combine) подобна предшествующей опции, только в этом случае значки одного типа никогда не группируются.
5. Выполнив требуемые настройки, нажмите кнопку **OK**, чтобы сохранить их.

> ***Совет***
>
> Возможность закрепления панели задач является одним из самых полезных параметров настройки. Закрепление настроенной панели задач полезно тем, что пользователи будут испытывать меньше проблем, возникающих вследствие случайного изменения ее параметров. К тому же, пользователи могут в любое время изменить настройки панели задач преднамеренно. Для этого нужно просто щелкнуть на панели задач правой кнопкой мыши и в контекстном меню выбрать команду **Закрепить панель задач** (Lock the taskbar).

Управление программами в области уведомлений

Область уведомлений, или системный лоток, представляет собой крайнюю правую область панели задач, в которой размещаются системные часы и значки уведомлений приложений. Двумя стандартными значками уведомлений являются значки для Центра поддержки и Центра управления сетями и общим доступом. При наведении указателя мыши на значок в области уведомлений отображается всплывающая строка (или окно), содержащая информацию о состоянии приложения или компонента значка. Для управления приложением, представленным значком в области уведомлений, щелкните правой кнопкой мыши на его знач-

ке, в результате чего откроется контекстное меню для данного приложения. Опции этого меню будут различными для разных приложений; большинство из них предоставляет доступ к основным операциям управления приложением.

Область уведомлений можно оптимизировать, настроив параметры отображения системных значков (часов, регулятора громкости, Центра управления сетями и общим доступом) и значков приложений.

Управление отображением значков в области уведомлений

Область уведомлений может содержать как системные значки, так и значки приложений. Значки приложений помещаются в область уведомлений по нескольким причинам. Некоторые программы, такие как Центр поддержки, управляются самой операционной системой, и их значки периодически отображаются в области уведомлений, когда имеются уведомления от этих приложений. Другие типы программ, такие как антивирусные приложения, настраиваются для автоматического запуска, после чего исполняются в фоновом режиме. Отображением значков программ часто можно управлять с помощью средств настройки, предоставляемых их соответствующими приложениями, но Windows 8 предоставляет общий интерфейс для управления отображением значков в области уведомлений для каждого отдельного приложения, помещающего значок в эту область.

Управление отображением значков в области уведомлений осуществляется посредством следующей процедуры:

1. Щелкните правой кнопкой мыши на панели задач и в контекстном меню выберите команду **Свойства**.
2. На вкладке **Панель задач** открывшегося диалогового окна **Свойства панели задач** щелкните по ссылке **Настроить** (Customize) справа от надписи **Область уведомлений**

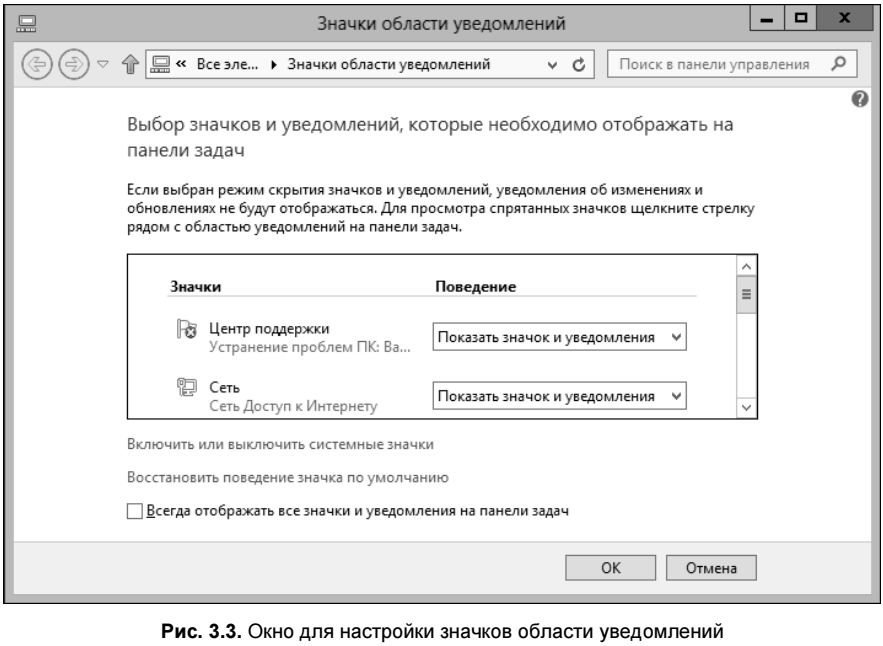


Рис. 3.3. Окно для настройки значков области уведомлений

(Notification area). Откроется окно **Значки области уведомлений** (Notification Area Icons), подобное показанному на рис. 3.3.

3. Для отображения всех значков и их уведомлений установите флажок **Всегда отображать все значки и уведомления на панели задач** (Always show all icons and notifications on the taskbar). Пропустите все следующие шаги.
4. Для индивидуальной настройки значков и уведомлений сбросьте флажок **Всегда отображать все значки и уведомления на панели задач**. Индивидуальная настройка значков и уведомлений осуществляется следующим образом. Каждый элемент в левой колонке списка, расположенного в центре окна, имеет раскрывающийся список в правой колонке, содержащий следующие опции:
   - **Скрыть значок и уведомления** (Hide icon and notifications) — никогда не отображать значок и уведомления;
   - **Показать только уведомления** (Only show notifications) — отображаются только уведомления;
   - **Показать значок и уведомления** (Show icon and notifications) — всегда отображать значок и уведомления.
5. Настроив все значки, закройте оба диалоговых окна, нажав их кнопки **OK**.

Оптимизация панелей инструментов

На панели задач можно разместить несколько панелей инструментов. Наиболее знакомым для большинства пользователей примером панели инструментов будет панель быстрого запуска, которая имелась в предыдущих версиях Windows, но в Windows 8 ее функциональность исполняет панель задач. Кроме этого, панель задач Windows 8 может содержать несколько системных панелей инструментов, а также панели инструментов, создаваемые пользователями.

Отображение панелей инструментов

На панели задач можно размещать следующие панели инструментов.

- **Адрес.** Эта панель инструментов содержит поле **Адрес** для ввода URL или другого адреса содержимого, к которому требуется получить доступ, в Интернете, локальной сети или на локальном компьютере. После ввода полного пути к объекту запускается приложение по умолчанию для открытия данного типа файла.
- **Ссылки.** Дубликат папки **Ссылки** меню **Избранное** в Internet Explorer. Чтобы добавить ссылки на папки, веб-страницы и другие ресурсы на эту панель инструментов, перетащите мышью туда ее ярлык. Чтобы удалить ссылку, щелкните ее правой кнопкой и в контекстном меню выберите пункт **Удалить**. При выводе запроса на подтверждение удаления нажмите кнопку **Да**.
- **Рабочий стол.** Предоставляет доступ ко всем ярлыкам на локальном рабочем столе, чтобы не сворачивать окна приложений для получения доступа к ним.
- **Сенсорная клавиатура.** Предоставляет быстрый доступ к экранной клавиатуре.

Для отображения или скрытия отдельных панелей инструментов применяется следующая процедура: щелкните правой кнопкой мыши на панели задач, выберите в контекстном меню пункт **Панели** и во вложенном меню щелкните на требуемой панели инструментов. Щелчок по панели инструментов включает или отключает ее отображение на панели задач, в зависимости от ее текущего состояния.

Совет

По умолчанию на большинстве панелей инструментов отображаются их названия. Отображение названий можно отключить, щелкнув на панели инструментов правой кнопкой мыши и сбросив в контекстном меню флажок **Показать заголовок** (Show title). Но если панель задач закреплена, этот флажок будет недоступен, и сначала нужно сбросить флажок **Закрепить панель задач** в контекстном меню панели задач.

Создание пользовательских панелей инструментов

Кроме предоставляемых системой панелей инструментов, на панели задач можно размещать пользовательские панели инструментов. Они создаются на основе папок, а их элементы отображают содержимое папок. Администраторы наиболее часто создают панели инструментов для сетевых папок. Например, может быть необходимым предоставить всем пользователям доступ к сетевой папке CorpData, содержащей корпоративную информацию, или папке UserData, содержащей пользовательскую информацию. В таком случае можно создать панель инструментов для этих ресурсов и поместить ее на панель задач. Теперь, когда пользователям нужно открыть одну из этих папок, они могут сделать это, просто щелкнув по соответствующему значку на панели инструментов.

Пользовательскую панель инструментов можно создать таким способом:

1. Щелкните правой кнопкой мыши на панели задач, выберите в контекстном меню пункт **Панели**, а во вложенном меню — **Создать панель инструментов** (New toolbar). Откроется диалоговое окно **Новая панель инструментов — Выбор папки** (New Toolbar — Choose a folder), похожее на диалоговое окно для открытия файла.
2. С помощью этого средства перемещения по файловой системе выберите папку для использования в качестве основы панели инструментов, а затем нажмите кнопку **Выбор папки** (Select Folder). Выбранная папка будет представлена панелью инструментов со своим названием на панели задач. Ярлыки, вставляемые в пользовательскую панель инструментов, автоматически попадают и в ее базовую папку. Соответственно, удаляемые с панели ярлыки также удаляются из ее базовой папки.

Примечание

Что касается пользовательских панелей инструментов, с ними как в том анекдоте о хорошей и плохой новости. Хорошая новость состоит в том, что большинство пользователей находят их полезными. Плохая же новость заключается в том, что если пользователь удалит такую панель инструментов, чтобы поместить ее обратно, нужно будет снова выполнить весь процесс ее создания.

Работа с темами рабочего стола

Темы рабочего стола представляют собой комбинации рисунков фона, наборов звуков, значков и других элементов, позволяющих персонализировать рабочий стол в частности и рабочую среду вообще. Администраторы, как правило, ненавидят темы, пользователи же, наоборот, излишне увлекаются ими. В этом разделе мы рассмотрим, как применять темы и настраивать их с помощью отдельных опций, а также как удалять их.

Применение и удаление тем

Операционная система Windows 8 позволяет применять различные темы, некоторые из них поставляются вместе с этой операционной системой.

Применить схему можно посредством следующей процедуры:

1. Щелкните правой кнопкой мыши на свободной области рабочего стола и в контекстном меню выберите команду **Персонализация** (Personalize). Откроется одноименное окно (рис. 3.4).

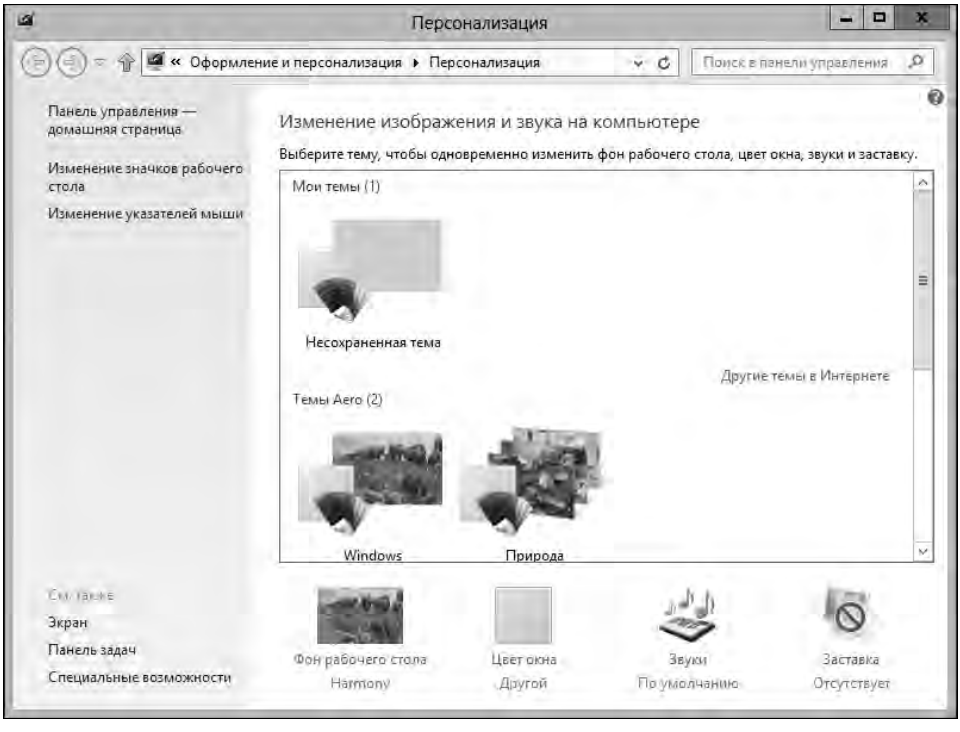


Рис. 3.4. Окно **Персонализация** для настройки тем, фона рабочего стола, параметров экрана и т. п.

2. Выберите из списка требуемую тему. Кроме доступных на компьютере тем, можно устанавливать темы с веб-сайта Microsoft. Для этого щелкните по ссылке **Другие темы в Интернете** (Get more themes online), чтобы открыть этот веб-сайт в браузере. Выберите на сайте понравившуюся тему, щелкните по ссылке **Download** и в диалоговом окне запроса нажмите кнопку **Сохранить**. В IE, чтобы выбрать папку для сохранения темы, щелкните на треугольничке справа от кнопки, выберите во вложенном меню опцию **Сохранить как** и укажите требуемую папку. По завершению загрузки нажмите кнопку **Открыть папку** и установите загруженную тему, дважды щелкнув на ее значке. Теперь эта тема доступна для применения в разделе **Мои темы** консоли **Персонализация**.
3. В нижней части окна **Персонализация** предоставляются опции для настройки отдельных аспектов выбранной темы, таких как рисунок фона рабочего стола, цвет окна и звуки. Чтобы изменить какой-либо из этих элементов темы, щелкните мышью по требуемой ссылке.

Исходная тема рабочего стола восстанавливается следующим образом:

1. Щелкните правой кнопкой мыши по свободной области рабочего стола и в контекстном меню выберите опцию **Персонализация**.
2. В разделе **Темы Aero** выберите тему **Windows**.

Подсказка

Темы управляются службой **Темы**, поэтому, если нужно отключить темы, не изменяя их конфигурацию, например при диагностировании какой-либо проблемы, это можно сделать, остановив эту данную службу. Одним из быстрых способов сделать это будет выполнение команды `net stop themes` в консоли командной строки, открытой с правами администратора. Запуск службы **Темы** осуществляется выполнением команды `net start themes` в консоли командной строки, открытой с правами администратора.

Настройка и сохранение тем

Применение определенной темы к рабочему столу изменяет несколько разных его аспектов. Обычно пользователям нравится общий эффект темы, но какой-либо из ее аспектов может вызывать возражения. Чтобы исправить это, можно изменить те детали темы, которые вызывают нарекания пользователя, и сохранить модифицированную тему, чтобы ее можно было применять в будущем без дополнительных настроек.

Управление темами осуществляется посредством окна **Персонализация**, для открытия которого нужно щелкнуть правой кнопкой мыши по свободной области рабочего стола и в контекстном меню выбрать одноименную опцию. В окне **Персонализация** можно выполнять настройку следующих параметров тем.

- **Заставка.** Чтобы установить или изменить экранную заставку, щелкните на значке **Заставка**. В открывшемся диалоговом окне **Параметры экранной заставки** выберите требуемую заставку или опцию **Нет**, чтобы убрать ее, и нажмите кнопку **OK**, чтобы сохранить и применить настройку.
- **Звуки.** Чтобы изменить звуковую схему темы, щелкните на значке **Звуки**. На вкладке Звуки открывшего диалогового окна выберите в раскрывающемся списке **Звуковая схема** (Sound Scheme) требуемый набор звуков для программных и системных событий. Чтобы восстановить звуковую схему по умолчанию, выберите опцию **По умолчанию**, а чтобы отключить звуки темы — опцию **Без звука** (No sounds). Нажмите кнопку **OK** для сохранения настроек. При отключении звуковой схемы темы следует обратить внимание на возможность отключения опции **Проигрывать мелодию запуска Windows** (Paly Windows startup sound), сбросив для этого соответствующий флажок.
- **Указатели мыши.** Чтобы изменить указатели мыши, щелкните по ссылке **Изменение указателей мыши** (Change mouse pointers) в правой панели окна. На вкладке **Указатели** открывшегося диалогового окна **Свойства: Мышь** в списке **Схема** выберите требуемый набор указателей мыши. Нажмите кнопку **OK**, чтобы сохранить настройки.
- **Фон рабочего стола.** Чтобы изменить рисунок фона рабочего стола, щелкните по ссылке **Фон рабочего стола** (Desktop background). В списке **Расположение изображения** (Picture location) укажите одно из стандартных хранилищ рисунков или же нажмите кнопку **Обзор**, чтобы выбрать папку с рисунком с помощью диалогового окна для просмотра файловой системы **Обзор папок** (Browse For Folder). Рисунок для фона можно также выбрать из содержимого папки *%SystemRoot%*\Web\Wallpaper, в которой по умолчанию хранятся стандартные рисунки рабочего стола Windows 8. Выберите требуемое изображение, укажите способ его расположения в списке **Положение изображения** (Picture position), а затем нажмите кнопку **Сохранить изменения** (Save changes).
- **Цвет окна.** Чтобы изменить цвет границ системных окон и панели задач, щелкните по ссылке **Цвет**. Выберите требуемый цвет и нажмите кнопку **Сохранить изменения**.

Удаление пользовательских схем

Дополнительные темы, устанавливаемые пользователями, могут занимать много места на диске. Удалить схему и связанные с ней файлы, чтобы освободить дисковое пространство, можно с помощью следующей процедуры:

1. Щелкните правой кнопкой мыши по свободной области рабочего стола и в контекстном меню выберите команду **Персонализация**.
2. В разделе **Мои темы** щелкните правой кнопкой мыши на теме, которую нужно удалить, а затем нажмите всплывшую кнопку **Удалить тему**. Файл определения темы и связанные с темой файлы мультимедиа будут удалены.

> ***Совет***
>
> По умолчанию файлы определения стандартных тем Windows находятся в папке *%WinDir%*\Resources\Themes, а пользовательских тем — в папке профиля пользователя. Чтобы определить занимаемый темами объем дискового пространства, выясните объем, занимаемый этими папками с их содержимым. Файлы тем не следует удалять вручную, а применять для этого только что описанную процедуру.

Оптимизация среды рабочего стола

Окна открытых программ и папок располагаются на рабочем столе. Расположение этих окон можно организовать разными способами, щелкнув правой кнопкой мыши на пустой области панели задач и выбрав в контекстном меню одну из команд: **Расположить окна каскадом** (Cascade windows), **Расположить окна стопкой** (Show windows stacked) или **Расположить окна рядом** (Show Windows side by side). А выбор опции **Показать рабочий стол** (Show the desktop) сворачивает все окна и отображает рабочий стол. Когда все окна свернуты, вместо команды **Показать рабочий стол** меню содержит команду **Показать все окна** (Show open windows), выбор которой восстанавливает все окна к их прежнему состоянию.

На рабочем столе можно размещать файлы, папки и ярлыки. Любые файлы или папки, сохраненные на рабочем столе, отображаются на нем. Также, перетащенный мышью на рабочий стол из окна Проводника файл или папка остаются на рабочем столе. Чтобы поместить ярлык для файла или папки на рабочий стол, щелкните правой кнопкой мыши на объекте, выберите в контекстном меню команду **Отправить** (Send to), а во вложенном меню — **Рабочий стол (создать ярлык)** (Desktop (create shortcut)).

Кроме рассмотренных основных способов, Windows 8 предоставляет много других методов оптимизации среды рабочего стола. Например, в качестве фона рабочего стола можно установить корпоративный логотип или другой символ. Это может быть особенно полезным для подменных ноутбуков, для которых можно создать, например, логотип наподобие "Подменный ноутбук технологического отдела". Или же можно с помощью гаджетов Windows добавить пользовательское содержимое непосредственно на рабочий стол.

Установка фона рабочего стола

Windows 8 содержит несколько наборов изображений для фона рабочего стола (так называемые *обои*), поименованных и распределенных по папкам, в которых хранятся файлы этих изображений. Эти наборы хранятся в папке *%WinDir%*\Web\Wallpaper, каждый в своей папке. Например, изображения в папке Природа отображаются в наборе фоновых изображений **Природа**.

В качестве изображений обоев можно использовать изображения форматов BMP, GIF, JPEG, DIB и PNG. Изображение одного из этих форматов, добавленное в любую из вложенных папок папки *%WinDir%*\Web\Wallpaper становится частью этого набора изображений обоев. Также можно сформировать собственный набор обоев, создав в корневой папке *%WinDir%*\Web\Wallpaper свою папку и заполнив ее изображениями допустимого формата.

Установить изображение фона рабочего стола можно следующим образом:

1. Щелкните правой кнопкой мыши по свободной области рабочего стола и в контекстном меню выберите команду **Персонализация**. В открывшемся окне щелкните по ссылке **Фон рабочего стола**. Откроется окно **Фоновый рисунок рабочего стола** (Desktop Background), пример которого показан на рис. 3.5.

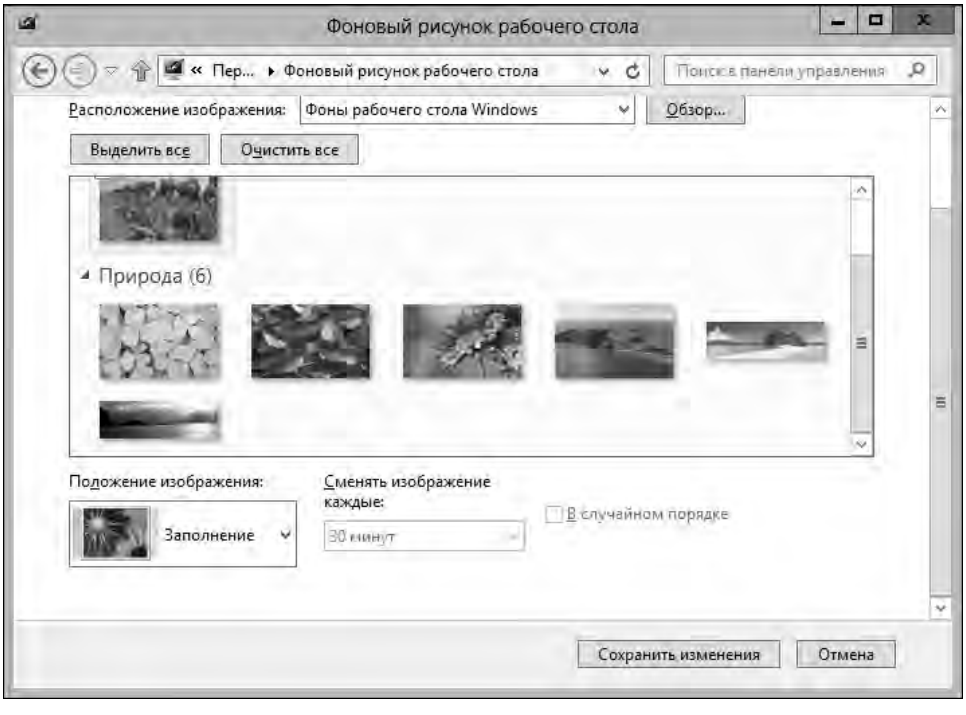


Рис. 3.5. Окно для установки фона рабочего стола

2. В раскрывающемся списке **Расположение изображения** выберите, например, опцию **Фоны рабочего стола Windows**. В большой панели окна отобразятся доступные наборы фоновых изображений, в данном примере это наборы **Windows** и **Природа**.
3. Щелкните на изображении, которое требуется установить в качестве фона. Вместо изображения из стандартных наборов можно выбрать любое отвечающее требованиям изображение, хранящееся на локальном или сетевом диске. Для выбора такого изображения нажмите кнопку **Обзор**.
4. Выбрав требуемое изображение, задайте способ его размещения, выбрав одну из опций в раскрывающемся списке **Положение изображения**. Изображение можно разместить:

   - **По центру** (Center) — изображение размещается в центре рабочего стола. Область рабочего стола, не заполненная изображением, заполняется текущим цветом рабочего стола;

- **Заполнение** (Fill) — фон рабочего стола заполняется изображением; стороны изображения могут обрезаться;
- **По размеру** (Fit) — изображение подгоняется по размеру рабочего стола с сохранением соотношения сторон. Этот вариант хорош для фотографий и больших изображений, которые нельзя искажать растягиванием;
- **Растянуть** (Stretch) — изображение растягивается, чтобы заполнить рабочий стол. Соотношение сторон выдерживается насколько это возможно, но изображение может быть растянуто по высоте до краев рабочего стола;
- **Замостить** (Tile) — фон покрывается несколькими изображениями исходного размера. Может быть интересным выбором для небольших изображений и значков.

5. Выбрав требуемое фоновое изображение рабочего стола, сохраните настройку, нажав кнопку **Сохранить изменения**.

Работа со стандартными значками рабочего стола

По умолчанию на рабочем столе отображается только Корзина. Двойной щелчок по значку Корзины открывает ее окно, в котором можно просмотреть объекты, предназначенные для удаления. Чтобы безвозвратно удалить содержимое Корзины, выберите меню **Управление** (Manage) Корзины, а затем в панели инструментов щелкните по значку **Очистить корзину** (Empty Recycle Bin). Для управления использованием Корзины выберите меню **Управление**, а затем щелкните по значку **Свойства корзины**. Откроется диалоговое окно **Свойства: Корзина**, в котором для каждого несъемного жесткого диска задается отдельная Корзина в виде папки. Для каждого диска можно задать максимальный размер Корзины или же указать немедленное удаление файлов, без промежуточного помещения их в Корзину.

Кроме Корзины, на рабочий стол можно добавить следующие стандартные значки.

- **Компьютер.** Двойной щелчок по значку **Компьютер** открывает окно, предоставляющее доступ к жестким и съемным дискам компьютера. Щелчок по этому значку правой кнопкой мыши и выбор в контекстном меню команды **Управление** открывает консоль **Управление компьютером** (Computer Management). Контекстное меню значка **Компьютер** также содержит опции для подключения и отключения сетевых папок.
- **Панель управления.** Двойной щелчок по значку **Панель управления** открывает окно Панели управления, предоставляющее доступ к средствам конфигурации и управления системой.
- **Сеть.** Двойной щелчок по значку **Сеть** открывает окно, предоставляющее доступ к сетевым ресурсам локальной сети. Контекстное меню значка **Сеть**, открываемое щелчком правой кнопки мыши, содержит, среди прочих, опции для подключения и отключения сетевых папок.
- **Файлы пользователя.** Значок папки текущего пользователя; имеет вид полуоткрытой папки с фигурой человека и именем текущего пользователя. Двойной щелчок по значку открывает личную папку текущего пользователя.

Добавление и удаление основных значков рабочего стола осуществляется посредством следующей процедуры:

1. Щелкните правой кнопкой мыши по свободной области рабочего стола и в контекстном меню выберите команду **Персонализация**. Откроется окно **Персонализация**.
2. В левой панели окна щелкните по ссылке **Изменение значков рабочего стола** (Change desktop icons). Откроется диалоговое окно **Параметры значков рабочего стола** (Desktop Icon Settings), пример которого показан на рис. 3.6.

Рис. 3.6. Диалоговое окно **Параметры значков рабочего стола**

3. Это диалоговое окно имеет флажок для каждого из только что рассмотренных стандартных значков рабочего стола. Для отображения значка на рабочем столе нужно установить его флажок, а сброс флажка убирает соответствующий значок с рабочего стола.
4. Установив необходимые флажки, нажмите кнопку **OK**, чтобы сохранить эти настройки.
5. Все значки рабочего стола можно отобразить или скрыть, щелкнув правой кнопкой мыши по свободной области рабочего стола, выбрав в контекстном меню команду **Вид** (View), а во вложенном меню установив или сбросив флажок **Отображать значки рабочего стола** (Show desktop items), соответственно.

Чтобы удалить значок или ярлык с рабочего стола, щелкните на нем правой кнопкой мыши и в контекстном меню выберите команду **Удалить**. При выводе запроса на подтверждение удаления нажмите кнопку **Да**. Обратите внимание, что удаление с рабочего стола значка, представляющего файл или папку, также удаляет этот файл или папку вместе с ее содержимым.

Правила работы с заставкой экрана

Заставка экрана активируется после определенного периода бездействия компьютера. Первоначально заставка экрана предназначалась для предотвращения выгорания ЭЛТ-мониторов под курсором, отображая постоянно меняющееся изображение. В настоящее время проблема выгорания мониторов больше не является актуальной, но заставки сохранились. Основной пользой, которую они приносят сейчас, является возможность автоматически заблокировать компьютер паролем.

Настройка парольной защиты для заставки

Защита компьютера паролем посредством экранной заставки предотвращает несанкционированное использование компьютера посторонними пользователями, что помогает защи-

тить как личные данные пользователя, так и интеллектуальную собственность организации. Администраторы должны в обязательном порядке обеспечить на компьютерах использование экранных заставок с включенной парольной защитой.

Включить парольную защиту на экранной заставке можно следующим образом:

1. Щелкните правой кнопкой мыши по свободной области рабочего стола и в контекстном меню выберите команду **Персонализация**.
2. Щелкните по ссылке **Заставка**, в результате чего откроется диалоговое окно **Параметры экранной заставки** (рис. 3.7).

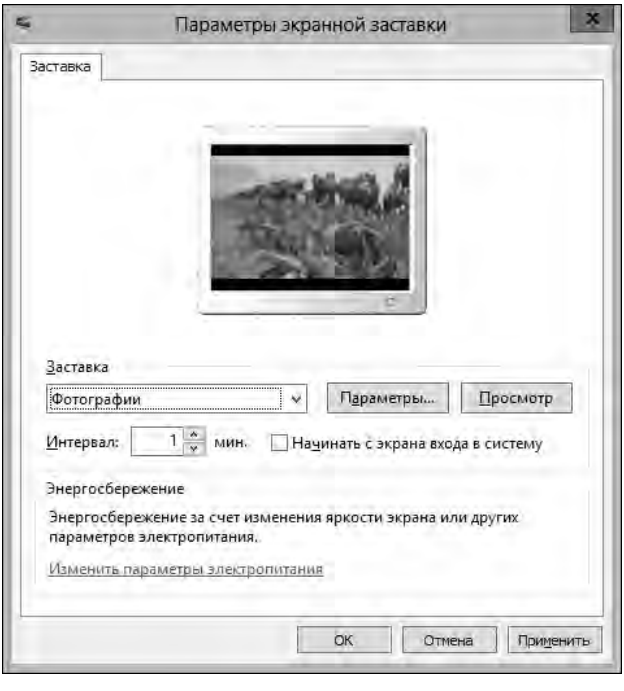


Рис. 3.7. Диалоговое окно для настройки экранной заставки и парольной защиты компьютера

3. В раскрывающемся списке **Заставка** выберите заставку. Чтобы отключить заставку, выберите **Нет** и пропустите остальные шаги.

> ***Практический совет***
>
> К сожалению, экранные заставки потребляют ресурсы компьютера, повышая как энергопотребление компьютера, так и уровень использования памяти и процессора. Некоторые заставки также повышают коэффициент использования процессора. Причиной этому является то обстоятельство, что некоторые заставки имеют очень сложный графический дизайн, и процессору требуется выполнять большой объем вычислений, чтобы постоянно обновлять изображение заставки. Несколько советов по снижению уровня использования ресурсов при исполнении заставок предоставляется в последующих разделах этой главы — *"Уменьшение уровня использования ресурсов заставками"* и *"Настройка энергосберегающих параметров для мониторов"*.

4. Установите флажок **Начинать с экрана входа в систему** (On resume, display logon screen).
5. В поле счетчика **Интервал** (Wait) установите период бездействия компьютера, после которого следует активировать заставку. Разумным значением здесь будет 10—15 минут.
6. Нажмите кнопку **OK**, чтобы сохранить настройки.

Примечание

Одной из лучших заставок является заставка **Фотографии**, которая демонстрирует изображения из папки по умолчанию **Изображения**, но можно указать любую другую папку. Скорость и порядок вывода изображений можно настраивать.

Уменьшение уровня использования ресурсов заставками

Для компьютера под управлением Windows 8, выполняющего задания в фоновом режиме или используемого в качестве сетевого сервера, не следует устанавливать сложных экранных заставок, таких как, например, движущийся объемный текст. Вместо этого желательно установить простую экранную заставку, такую как пустой экран. А для сложных экранных заставок можно настроить параметры так, чтобы уменьшить уровень использования ресурсов. Обычно такие настройки заключаются в установки низкой скорости прорисовки и частоты обновления.

Уменьшить уровень потребления ресурсов заставкой можно следующим образом:

1. Щелкните правой кнопкой мыши по свободной области рабочего стола и в контекстном меню выберите команду **Персонализация**.
2. Щелкните по ссылке **Заставка**, в результате чего откроется диалоговое окно **Параметры экранной заставки** (см. рис. 3.7).
3. Для заставки, которая использует небольшой объем ресурсов и не требует дополнительных настроек, выберите в раскрывающемся списке **Заставка** какую-либо простую заставку, например пустой экран.
4. Для более сложной заставки, такой как, например, объемный текст, нужно будет выполнить дополнительные настройки. Для этого после выбора требуемой заставки нажмите кнопку **Параметры**. В открывшемся диалоговом окне **Параметры заставки *"имя_заставки"*** установите наименьшие значения ее параметров, таких как разрешение, размер, скорость вращения и т. п., которые влияют на прорисовку или обновление заставки.
5. Установив все требуемые параметры, дважды щелкните кнопку **OK**, чтобы закрыть диалоговые окна.

Настройка энергосберегающих параметров для мониторов

Многие современные мониторы имеют энергосберегающие возможности, которые отключают монитор после определенного периода бездействия компьютера. Включение этой возможности может уменьшить потребление электричества, т. к. мониторы, особенно ЭЛТ-мониторы, в активном состоянии потребляют много электричества. На некоторых системах эта возможность может быть автоматически задействована операционной системой при ее установке. Но это зависит от правильного определения монитора операционной системой и установки всех требуемых драйверов.

Вопрос энергосбережения особенно важен в случае портативных вычислительных устройств, работающих от батарей. Настроив монитор на отключение при бездействии компьютера, можно сэкономить заряд батареи и продлить время работы от батарей.

Настроить новый режим энергосбережения монитора можно посредством следующей процедуры:

1. Щелкните правой кнопкой мыши по свободной области рабочего стола и в контекстном меню выберите команду **Персонализация**.

2. Щелкните по ссылке **Заставка**, в результате чего откроется диалоговое окно **Параметры экранной заставки** (см. рис. 3.7).
3. Щелкните по ссылке **Изменить параметры электропитания** (Change power settings). Откроется консоль **Электропитание**.
4. В левой панели консоли щелкните по ссылке **Настройка отключения дисплея** (Choose when to turn off display).
5. В открывшемся окне **Настройка параметров схемы** выберите в раскрывающемся списке **Отключать дисплей** период бездействия компьютера, после которого следует выключать монитор. Для мобильных вычислительных устройств может предоставляться два типа этого параметра — для работы от батарей и для работы от сети.
6. Нажмите кнопку **Сохранить изменения**, чтобы применить заданные параметры.

Примечание

Если монитор не поддерживает возможностей энергосбережения, то некоторые параметры могут отсутствовать. Когда компьютер настраивается в мастерской, лучше взять монитор как у пользователя или подобный и повторить процесс настройки.

Практический совет

Разумным будет отключать монитор после 15—20 минут простоя. Для офисных компьютеров рекомендуется активировать заставку примерно после 7 минут бездействия, а после 15 минут — отключать монитор. В случае мобильных устройств рекомендуется использовать 5 и 10 минут соответственно.

Модифицирование внешнего вида экрана и видеопараметров

Внешний вид и видеонастройки экрана имеют значительное влияние на восприятие пользователем рабочего стола Windows 8 и его графических элементов. Внешний вид экрана определяется параметрами окна, кнопок, цвета и шрифтов, а видеопараметры управляют разрешением экрана, качеством цвета, частотой обновления экрана, аппаратным ускорением и управлением цветом.

Настройка цвета и внешнего вида окон

Усовершенствованный интерфейс Windows Aero предоставляет такие возможности, как прозрачный фон панели задач, динамический просмотр, более плавное движение при перетаскивании окон, анимированное закрытие и открытие окон и многое другое. Как часть процесса установки, Windows 8 тестирует производительность и проверяет компьютер на соответствие основным требованиям для Windows Aero, которые включают следующее.

- Поддержку модели драйвера видеоадаптера Windows WDMM (Windows Display Driver Model). Модель WDDM 1.0 была представлена еще в Windows Vista. В Windows 7 и более поздних версиях драйверы видеоадаптера, поддерживающие модель WDDM 1.1, предоставляют повышенную производительность при одновременном понижении использования памяти каждым окном до 50%.
- Поддержка DirectX, реализованная в графическом процессоре, оснащенном минимум 128 Мбайт видеопамяти. Модель WDDM 1.1 поддерживает DirectX 11, усовершенствованную и с улучшенной производительностью версию этой технологии.

Практический совет

Определить размер видеопамяти и узнать, поддерживает ли видеоадаптер компьютера модель WDDM, можно с помощью окна **Счетчики и средства производительности**. Чтобы открыть это окно, в Панели управления в раскрывающемся списке **Просмотр** выберите опцию **Крупные значки** или **Мелкие значки**. Панель управления будет представлена в виде **Все элементы панели управления**. Теперь щелкните по ссылке **Счетчики и средства производительности** (Performance Information and Tools), в следующем окне — по ссылке видео **Отображение и печать подробных сведений о производительности компьютера и системы** (View and print detailed performance and system information). В следующем окне, **Дополнительные сведения о компьютере**, в пункте **Графика** списка **Компонент** будет указан тип видеоадаптера и уровень поддержки WDDM. Ниже в этом же окне, в разделе **Графика** расширенного списка компонентов, указываются дополнительные сведения о видеоадаптере, включая объем доступной памяти видеоадаптера и поддерживаемую версию видео DirectX.

В системах, удовлетворяющих требованиям Windows 8, по умолчанию использует рабочий стол Aero, позволяя применение расширенных видеофункциональностей, включая возможность *прикрепить* (Snap), которая позволяет, среди прочего, прикреплять окна у края экрана, и *встряхнуть* (Shake), которая позволяет временно скрыть все открытые окна, за исключением текущего активного окна. Чтобы прикрепить активное окно у правого или левого края рабочего стола, нажмите комбинацию клавиш <Win>+<→> или <Win>+<←> соответственно. Чтобы "встряхнуть" окно (т. е. оставить открытым только данное окно и скрыть все остальные), нажмите левую кнопку мыши на заголовке окна и выполните быстрое движение из стороны в сторону, а чтобы затем восстановить все скрытые окна, повторите эту операцию.

Настроить параметры цвета для экрана можно следующим образом:

1. Щелкните правой кнопкой мыши по свободной области рабочего стола и в контекстном меню выберите команду **Персонализация**.
2. На странице **Персонализация** щелкните по ссылке **Цвет окна**, вследствие чего откроется окно **Цвет и внешний вид окна** (Color and Appearance), пример которого показан на рис. 3.8.

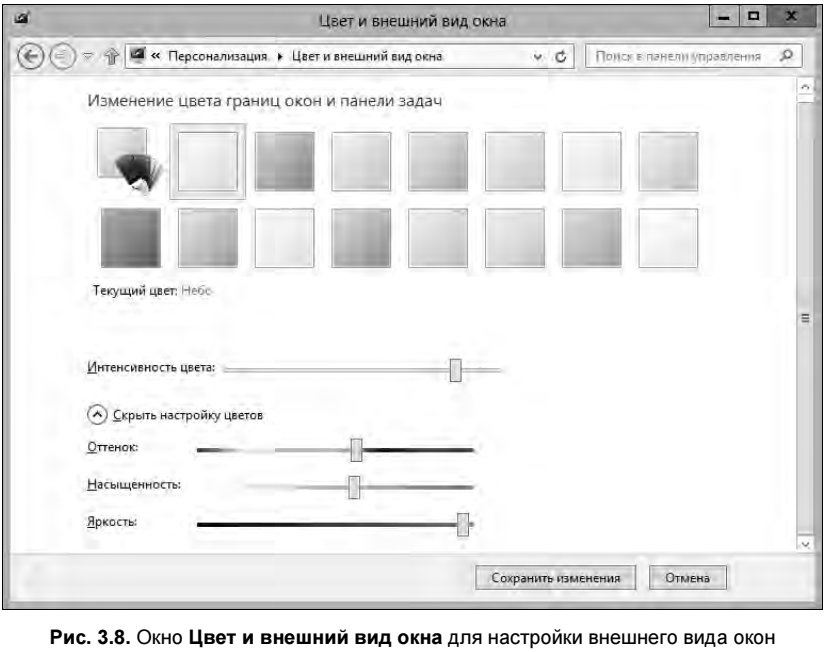


Рис. 3.8. Окно **Цвет и внешний вид окна** для настройки внешнего вида окон

3. Чтобы изменить цвет окна, щелкните на одном из квадратов требуемого цвета. Выбранный цвет можно изменить. Для этого нужно щелкнуть по ссылке **Показать настройку цветов** (Show color mixer), а затем с помощью ползунков **Оттенок** (Hue), **Насыщенность** (Saturation) и **Яркость** (Brightness) создать свой цвет.
4. С помощью ползунка **Интенсивность цвета** устанавливается интенсивность и уровень прозрачности выбранного цвета. Перемещение ползунка вправо повышает интенсивность и понижает прозрачность цвета, а перемещение влево — наоборот.
5. Добившись требуемого результата, нажмите кнопку **Сохранить изменения**, чтобы применить заданные параметры.

Для улучшения поддержки людей с нарушениями зрения Windows 8 предоставляет несколько тем специальных возможностей, включая темы **Высокая контрастность 1**, **Высокая контрастность 2**, **Контрастная белая** и **Контрастная черная**. При использовании этих тем страница **Цвет и внешний вид окна** имеет другие опции, и есть возможность изменять настройки по умолчанию для отдельных элементов окна, таких как цвет фона, цвет текста и цвет активного окна. Настройка этих элементов осуществляется следующим образом:

1. Щелкните правой кнопкой мыши по свободной области рабочего стола и в контекстном меню выберите команду **Персонализация**.
2. Щелкните по ссылке **Цвет окна** и на следующей странице установите требуемый цвет для элементов интерфейса.
3. Выполнив требуемые настройки, нажмите кнопку **Сохранить изменения**.

Оптимизация удобочитаемости дисплея

Независимо от размеров используемого ими дисплеев, будь то 19-дюймовые мониторы или 27-дюймовые панели, пользователи могут испытывать трудности с чтением текста на экране. Часто читабельность текста на экране понижается при повышении разрешения экрана, вследствие того, что текст становится меньшего размера. Чтобы понять, почему это происходит, нужно понимать термин "точек на дюйм" (dots per inch, dpi).

При распечатке документов на принтере качество печати определяется количеством точек на дюйм печати. Обычно, чем выше это отношение, тем выше качество распечатанного документа, т. к. чем больше количеств точек на дюйм, тем более четко и резко выглядят изображения и текст. Например, изображение высокого разрешения, распечатанное в натуральный размер, выглядит намного лучше при разрешении 1200×600 dpi, чем распечатанное с разрешением 300×300 dpi. То же самое происходит при масштабировании печати изображения исходного размера 2×3 дюйма, скажем, к 6×9 дюймов, вследствие меньшего количества точек на дюйм в конечном изображении.

В большинстве применяемых с компьютерами Windows мониторов по умолчанию имеют разрешение 96 dpi, и Windows 8 по умолчанию отображает все элементы пользовательского интерфейса, включая текст, с разрешением 96 dpi. При изменении разрешения экрана изменяется масштаб отображения элементов пользовательского интерфейса. Например, если для монитора с оптимальным разрешением 1920×1200 точек установить разрешение 800×600 точек, элементы пользовательского интерфейса будут выглядеть большими и зернистыми, т. к. 800×600 пикселов отображаются на площади, оптимизированной под 1920×1200 пикселов (сравните с растягиванием изображения 2×3 дюйма к размеру 6×9 дюймов).

Обычно оптимальное разрешение монитора можно определить, умножив ширину и высоту его экрана на 96. Например, ширина экрана 24-дюймового монитора может быть 20 дюй-

мов, а высота — 12,5 дюйма. В таком случае, оптимальное разрешение дисплея будет 1920×1200 пикселов. Но при этом разрешении экрана отображаемые на нем текст и элементы пользовательского интерфейса могут выглядеть маленькими, вследствие чего нужно будет выполнить определенные настройки, чтобы улучшить читаемость. Одним из подходов к выполнению таких настроек будет использование средств приложений. Например, в текстовом редакторе MS Word размер текста можно увеличить до удобочитаемого размера с помощью элемента управления **Масштаб**.

Операционная система Windows позволяет изменять размер текста для определенных элементов пользовательского интерфейса, включая текст заголовков диалоговых окон, меню, окон сообщений, заголовков цветовых палитр, значков и всплывающих подсказок. Увеличивая или уменьшая размер текста определенной части пользовательского интерфейса, можно повысить удобочитаемость. Параметры размера текста можно настраивать отдельно для каждой учетной записи компьютера. Настройка размера текста для элементов пользовательского интерфейса выполняется следующим образом:

1. В панели инструментов щелкните по ссылке **Оформление и персонализация** (Appearance and Personalization). На следующей странице в разделе **Экран** щелкните по ссылке **Изменение размеров текста и других элементов** (Make text and other items larger or smaller).
2. В следующем окне в разделе **Изменение только размера текста** (Change only the text size) в раскрывающемся списке выберите требуемый элемент интерфейса, например **Меню**.
3. Далее, в поле счетчика установите размер текста, необходимый для этого элемента интерфейса. Вдобавок текст можно сделать полужирным, установив соответствующий флажок.
4. Повторите шаги 2 и 3 для всех элементов пользовательского интерфейса. Задав все требуемые параметры, нажмите кнопку **Применить**.
5. Чтобы выполненные настройки вошли в действие, нужно выйти из системы, а затем снова войти в нее.

Операционная система Windows также позволяет увеличивать размер текста и других элементов к одному из выбранных масштабов. Масштабирование можно настраивать отдельно для каждой учетной записи компьютера, выполняется это следующим образом:

1. В панели инструментов щелкните по ссылке **Оформление и персонализация**. На следующей странице в разделе **Экран** щелкните по ссылке **Изменение размеров текста и других элементов**.
2. Стандартные опции позволяют устанавливать масштаб 100% (масштаб по умолчанию), 125 или 150%.
3. Кроме этого, доступна опция установки любого масштаба от 100 до 500%. Для этого нужно щелкнуть по ссылке **Пользовательские параметры изменения размера** (Custom sizing options) и, перемещая бегунок вправо, установить требуемый масштаб.
4. Чтобы выполненные настройки вошли в действие, нужно выйти из системы, а затем снова войти в нее.

Важно!

Если установить масштаб больше, чем 200%, размер элементов интерфейса и текста может быть настолько большим, что работать с компьютером будет невозможно, вплоть до того, что нереально будет открыть панель инструментов, чтобы устранить проблему. В случае такого развития событий выполните команду `dpiscaling` в командной строке или в поле поиска панели **Приложения**. Это откроет страницу **Экран** напрямую, где можно будет установить правильный масштаб.

Практический совет

Если вследствие установки определенного масштаба текст в каком-либо приложении становится размытым или вообще нечитаемым, масштабирование для этого приложения можно отключить. Для этого щелкните правой кнопкой мыши по значку приложения и в контекстном меню выберите команду **Properties**, а затем на вкладке **Совместимость** страницы свойств приложения установите флажок **Отключить масштабирование изображения при высоком разрешении экрана** (Disable display scaling on high DIP settings).

Настройка видеопараметров

Видеопараметры управляют разрешением экрана, качеством цвета, частотой обновления экрана, аппаратным ускорением и управлением цветом. В этом разделе рассматривается, как обеспечить правильное определение видеоадаптера и монитора операционной системой Windows 8, а также оптимизация различных видеопараметров.

Получение сведений о текущем видеоадаптере и мониторе

На всех компьютерах устанавливаются драйверы монитора и видеоадаптера. Драйвер монитора сообщает Windows о возможностях монитора, а драйвер видеоадаптера — о возможностях этого оборудования.

От корректности используемой компьютером информации о видеоадаптере и мониторе зависит правильность видеовывода. В зависимости от того, какую модель используемых в системе видеоадаптера и монитора обнаружит Windows 8, операционная система устанавливает разные драйверы для этих аппаратных компонентов. Эти драйверы играют очень важную роль в определении доступных и правильных для данной системы параметров разрешения экрана, глубины цвета и частоты обновления экрана. Если видеоадаптер и монитор не определены и не настроены должным образом, Windows 8 не сможет использовать их возможности.

Текущие настройки видеоадаптера или монитора могут быть неправильными по разным причинам. В одних случаях Plug and Play не может определить устройство и использует для него общий драйвер. В других случаях устройство определяется неправильно, например, как другой модели. В таком случае устройство может работать с установленным для него драйвером, но некоторые возможности будут недоступны.

Получить информацию о текущих настройках монитора и видеоадаптера компьютера можно следующим образом:

1. Щелкните правой кнопкой мыши по свободной области рабочего стола и в контекстном меню выберите команду **Разрешение экрана** (Screen Resolution).
2. Откроется одноименное окно (рис. 3.9), где в поле **Дисплей** перечислены текущие определенные мониторы. Разрешение и ориентация монитора указаны в соответствующих полях. Если в поле **Дисплей** указан неправильный монитор, или если требуется получить более подробные сведения о мониторе, *см. разд. "Обновление драйвера монитора" далее в этой главе*.
3. Выберите в списке **Дисплей** требуемый монитор, а затем щелкните по ссылке **Дополнительные параметры** (Advanced settings). На вкладке **Adapter** открывшегося окна представлена информация о текущем видеоадаптере. Если здесь указан неправильный адаптер, или если требуется получить дополнительные сведения о драйвере видеоадаптера, *см. разд. "Изменение драйвера видеоадаптера" далее в этой главе*.
4. Последовательно нажмите кнопку **OK**, чтобы закрыть все окна.

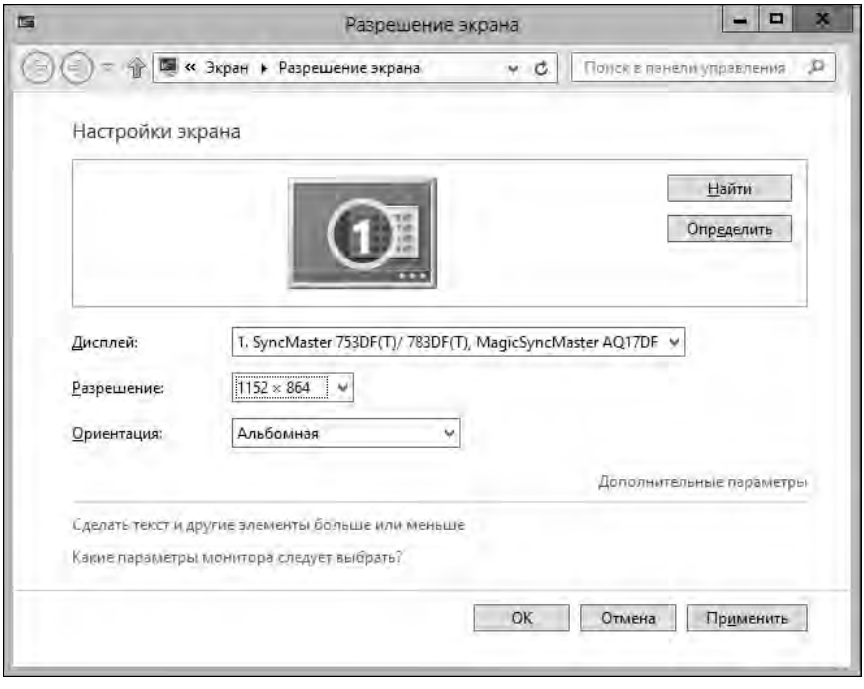


Рис. 3.9. Окно **Разрешение экрана**

Изменение драйвера видеоадаптера

Если при просмотре информации о драйвере видеоадаптера, как описано в предыдущем разделе, было обнаружено, что драйвер не соответствует установленному на компьютере видеоадаптеру, можно попробовать установить другой драйвер. Например, если указано, что установлен общий видеодрайвер S3, в то время как в действительности на компьютере установлен видеоадаптер NVIDIA GeForce, следует заменить установленный видеодрайвер соответствующим установленному видеоадаптеру.

Чтобы удостовериться в правильности предоставляемой информации о драйвере видеоадаптера, необходимо знать, какой видеоадаптер установлен в действительности. Узнать это можно разными способами: в документации о системе, у других администраторов или же у членов команды технической поддержки, среди которых обычно всегда есть кто-либо, знающий, какой видеоадаптер установлен на определенном типе компьютера. Если определить изготовителя и модель видеоадаптера такими способами не представляется возможным, есть еще несколько других подходов. Если текущие настройки работают, как следует, можно просто оставить все как есть. Или же можно попробовать определить изготовителя и модель видеоадаптера одним из следующих способов.

- Выключите питание компьютера, а затем снова включите. Не выполняйте перезагрузку компьютера, так как некоторые компьютеры не проходят полную инициализацию при перезагрузке. Сразу же после включения компьютера смотрите на экран: во многих случаях первое, что выводится на экран при включении компьютера — это информация о видеоадаптере.
- Выключите компьютер, снимите левую боковую крышку и попробуйте найти информацию о производителе и модели на самой плате адаптера. Плату видеоадаптера можно определить по подключенному к ней кабелю монитора.

- Если же видеоадаптер интегрирован в материнскую плату (т. е. отдельной платы видеоадаптера нет), попробуйте найти на ней чип с видеоинформацией или же посетите веб-сайт производителя материнской платы и попытайтесь получить требуемую информацию там.

Определив производителя и модель видеоадаптера, попробуйте найти драйверы для него на веб-сайте производителя. Обычно новые видеоадаптеры поставляются с компакт-диском с драйверами. Если такой диск сохранился, запустите программу установки и установите драйверы. Если диск содержит драйверы, но программа установки отсутствует, драйверы нужно будет установить вручную.

Когда все готово для установки драйвера, это процедура выполняется следующим образом:

1. Щелкните правой кнопкой мыши по свободной области рабочего стола и в контекстном меню выберите команду **Разрешение экрана**.
2. Если к компьютеру подключено несколько мониторов, что означает наличие больше одного видеоадаптера, выберите в списке **Дисплей** монитор, подключенный к видеоадаптеру, для которого нужно заменить драйвер.
3. Щелкните по ссылке **Дополнительные параметры**. Со вкладки **Адаптер** открывшегося окна свойств (см. пример на рис. 3.10) спишите информацию о типе и других данных адаптера. Нажмите кнопку **Свойства**.

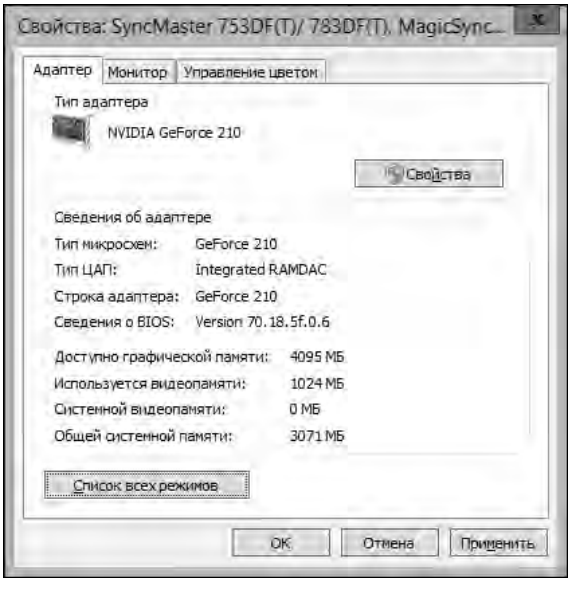


Рис. 3.10. Информация о видеоадаптере

4. В открывшемся окне свойств видеоадаптера выберите вкладку **Драйвер** и нажмите на ней кнопку **Обновить** (Update Driver). Откроется окно мастера обновления драйверов.
5. Выберите одну из предлагаемых опций поиска драйвера для установки — автоматически или вручную.
6. При автоматическом поиске Windows 8 пытается найти более новую версию драйвера и в случае успешного поиска установит его. В противном случае оставляется старый драйвер. В любом случае, по завершению процесса нажмите кнопку **Закрыть** и пропустите последующие шаги.

7. В случае поиска драйвера вручную это можно делать одним из следующих способов.
   - **Выполнить поиск драйвера на данном компьютере.** В этом случае нажмите кнопку **Обзор** и в открывшемся диалоговом окне **Обзор папок** (Browse For Folder) укажите папку для поиска драйвера, после чего нажмите кнопку **OK**. Так как по умолчанию поиск выполняется во всех вложенных папках указанной папки, указав вместо папки диск, можно выполнить поиск по всему этому диску. Если не требуется выполнять поиск во вложенных папках, сбросьте флажок **Включая вложенные папки** (Include subfolders).
   - **Выбрать драйвер для установки.** Чтобы указать драйвер, который следует установить, выберите опцию **Выбрать драйвер из списка уже установленных драйверов** (Let me pick from the list of device drivers on my computer). Откроется страница мастера со списком совместимых устройств. Выберите в этом списке устройство, соответствующее вашему видеоадаптеру. Чтобы просмотреть список всех возможных устройств, сбросьте флажок **Только совместимые устройства** (Show compatible hardware). В таком случае откроются две панели: одна — со списком производителей видеоадаптеров, вторая — с моделями. Выберите в первом списке производителя вашего видеоадаптера, а потом во втором списке — модель видеоадаптера.
8. Выбрав таким образом требуемый драйвер, продолжите процесс установки, нажав кнопку **Далее**. По завершению операции установки драйвера нажмите кнопку **Закрыть**. Если мастер не может найти требуемый драйвер, необходимо раздобыть таковой и повторить процедуру установки. Следует иметь в виду, что в некоторых случаях, чтобы активировать новоустановленный драйвер, необходимо перезагрузить систему.

Обновление драйвера монитора

Общее качество видеовывода зависит от совместных возможностей видеоадаптера и монитора компьютера. Большинство компьютеров оснащено как минимум одним разъемом для подключения монитора. Наиболее распространены разъемы следующих стандартов.

- **Интерфейс HDMI[1].** Текущий цифровой стандарт для подключения видеоустройств. Интерфейс HDMI можно использовать с компьютерными мониторами, но он лучше подходит к другим видеоустройствам высшего класса. Хотя интерфейс HDMI можно приспособить к разъему стандарта DVI[2], большинство видеоадаптеров с разъемом HDMI также оснащено, по крайней мере, одним разъемом стандарта DVI.
- **Интерфейс DVI.** Цифровой стандарт для компьютерного текста и графики. Существует несколько форматов интерфейса DVI. Интерфейсы DVI-I и DVI-A можно приспособить под разъем типа VGA[3], но с интерфейсом DVI-D этого сделать невозможно. Интерфейс Dual-Link DVI[4] поддерживает мониторы высокого разрешения и требуется для некоторых дисплеев очень большого размера, чтобы обеспечить оптимальное качество изображения. Так как кабели DVI могут поддерживать более одного типа этих версий интерфейса одновременно, нужно внимательно следить за тем, чтобы использовать правильный кабель.
- **Интерфейс VGA.** Аналоговый стандарт с 15-контактным разъемом для подключения мониторов к компьютерам. Существуют 9-жильные кабели VGA, которые совместимы

[1] High-Definition Multimedia Interface — мультимедийный интерфейс высокой четкости.

[2] Digital Video Interface — цифровой видеоинтерфейс.

[3] Video Graphics Array — видеографическая матрица.

[4] Двухканальный DVI.

с 15-контактными разъемами. Мониторы с таким разъемом встречаются все еще часто, но, если возможно, рекомендуется использовать разъемы DVI и HDMI.

Примечание

Монитор может поставляться с подключенным VGA-кабелем. Если это не оптимальный тип разъема и конструкция допускает отсоединение кабеля VGA, отсоедините его.

Совет

В последнее время все большее распространение начинают получать видеоадаптеры стандарта DisplayPort. С помощью специальных переходников видеоадаптеры этого типа поддерживают подключение мониторов VGA, DVI или HDMI.

Если к компьютеру подключен монитор Plug-and-Play, Windows 8 может правильно определить его и установить нужные драйверы, но, с другой стороны, может быть установлен работоспособный драйвер, но при этом не совсем точно соответствующий данному типу и/или модели монитора. Чтобы обеспечить наилучшее качество видеоизображения, Windows 8 должна использовать драйвер, предназначенный для данного монитора. В противном случае параметры видеосигнала, такие как режим отображения, глубина цвета, частота обновления и уравнивание цветов, могут не соответствовать возможностям монитора.

Чтобы обновить драйвер монитора, следуйте такой процедуре:

1. Щелкните правой кнопкой мыши по свободной области рабочего стола и в контекстном меню выберите команду **Разрешение экрана**.
2. Если к компьютеру подключено больше одного монитора, выберите в списке **Дисплей** монитор, для которого нужно обновить драйвер.
3. Щелкните по ссылке **Дополнительные параметры**. В открывшемся окне свойств монитора выберите вкладку **Монитор**, а на ней нажмите кнопку **Свойства**.
4. В следующем окне выберите вкладку **Драйвер** и нажмите на ней кнопку **Обновить**. Откроется окно мастера обновления драйверов.
5. Далее следуйте шагам 5—8 процедуры обновления драйвера видеоадаптера, описанной ранее.

Настройка поддержки нескольких мониторов

Большинство современных видеоадаптеров может поддерживать подключение двух мониторов. Такие адаптеры можно определить по наличию нескольких разъемов для подключения монитора. К оснащенным такими адаптерами компьютерам можно подключать несколько мониторов, а затем распределить рабочий стол по этим мониторам, чтобы одновременно можно было бы видеть больше информации. Если к компьютеру подключено несколько мониторов, они представляются в виде пронумерованных прямоугольных значков на странице **Разрешение экрана**. Щелкнув по определенному значку монитора, его можно выбрать для дальнейшей работы с ним.

Если подключенный монитор не отображается в виде прямоугольника, проверьте надежность его подключения, а также убедитесь, что он включен. Затем нажмите кнопку **Найти**, и Windows должна автоматически определить его.

Если при подключении нескольких мониторов возникают затруднения с их идентификацией, нажмите кнопку **Определить**, вследствие чего на экране отобразится номер текущего монитора в виде большой цифры с белым полем и черными обводами. Если на странице **Разрешение экрана** порядок значков мониторов иной, чем расположение представляемых ими мониторов, их можно упорядочить, перетаскивая мышью, чтобы они соответствовали порядку физических мониторов.

Настроив и упорядочив мониторы, можно приступать к настройке распределения видеовывода по всем мониторам. Для этого щелкните по значку второго монитора (или выберите второй монитор в списке **Дисплей**), а затем в списке **Несколько экранов** (Multiple displays) выберите опцию **Расширить эти экраны** (Extend these displays). Обычно первый экран должен быть обозначен **В настоящее время это основной монитор** (This is currently your main display).

После первоначальной настройки нескольких мониторов в дальнейшем окно для быстрого изменения их конфигурации можно использовать комбинацию клавиш <Windows>+<P>. Ее нажатие открывает панель **Второй экран** (Second screen), на которой доступны следующие опции:

- **Только экран компьютера** (PC screen only) — использовать только основной монитор компьютера или встроенный экран ноутбука;
- **Дублировать** (Duplicate) — дублировать содержимое основного монитора компьютера или встроенного экрана ноутбука на втором мониторе;
- **Расширить** (Extend) — распределить видеовывод по двум мониторам;
- **Только второй экран** (Second screen only) — использовать только второй монитор.

Для устройств с сенсорным экраном эту панель можно открыть, проведя пальцем справа к центру экрана, щелкнув по устройству, а затем щелкнув на опции **Второй экран**.

Настройка внешнего вида экрана

Ключевыми факторами, влияющими на качество видеоизображения, являются разрешение экрана, качество цвета и частота обновления экрана. *Разрешение экрана* обозначает количество пикселов экрана. Под *качеством цвета* подразумевается количество цветов, которое можно одновременно отображать на экране. *Частота обновления* означает, сколько раз в секунду обновляется содержимое экрана.

Операционная система Windows автоматически оптимизирует видеопараметры каждого подключенного монитора, устанавливая разрешение экрана, качество цвета и частоту обновления, которые она считает наиболее подходящими для данного монитора по результатам тестирования. Обычно установленные Windows параметры работают достаточно хорошо, но они могут быть не совсем оптимальными для данного компьютера.

Например, практическое оптимальное разрешение зависит от размера монитора и от типа выполняемой на нем работы. Дизайнеры и разработчики, которым требуется много экранного пространства, предпочтут более высокое разрешение, например 1920×1200 пикселов. Это позволит им поместить на экран больший объем своей работы. А для пользователей, которые проводят бóльшую часть времени, просматривая электронную почту или редактируя текстовые документы, предпочтительней будет более низкое разрешение, например 1280×1024 пикселов. Такое разрешение позволяет пользователю легче видеть элементы изображения на экране, что понижает уровень напряжения глаз. Для широкоформатных мониторов необходимо установить такое разрешение экрана, которое подходит для широкоформатного просмотра.

Качество цвета в значительной мере зависит от установленного разрешения экрана. Хотя большинство современных видеоадаптеров может отображать 32-битовый цвет при разных разрешениях экрана, некоторые видеоплаты могут быть неспособными отображать цвет такого качества при максимальном разрешении экрана, поддерживаемом ими. Иными словами, при высоких разрешениях экрана такие видеоадаптеры могут поддерживать меньшее количество цветов. В большинстве случаев лучшее качество цветопередачи означает лучшее качество видео. Обратите внимание на тот факт, что необходимый объем видеопамяти

определяется умножением количества пикселов экрана (зависит от разрешения экрана) на количество битов на каждый пиксел (зависит от качества цвета). Таким образом, комбинация наивысшего разрешения экрана и наибольшей глубины цвета является функцией объема памяти видеоадаптера.

Разрешение экрана и глубина цвета устанавливаются следующим образом:

1. Щелкните правой кнопкой мыши по свободной области рабочего стола и в контекстном меню выберите команду **Разрешение экрана**.
2. Если к компьютеру подключено несколько мониторов, выберите в списке **Дисплей** тот монитор, для которого нужно выполнить настройки.
3. Разверните список **Разрешение**, а затем установите требуемое разрешение, например 1023×768 пикселов. Обратите внимание, что если опция **Разрешение** отображена тусклo, настройка разрешения недоступна.
4. Чтобы узнать, какие разрешения экрана поддерживают 32-битный цвет, щелкните по ссылке **Дополнительные параметры**. Выберите в открывшемся диалоговом окне вкладку **Адаптер** и нажмите на ней кнопку **Список всех режимов** (List all modes). Из списка доступных режимов запишите те, которые поддерживают 32-битный цвет.
5. Последовательно нажмите кнопку **OK**, чтобы закрыть все окна.

При достаточно высокой частоте обновления экрана человеческий глаз не воспринимает этого, но частота обновления ниже 72 Гц может иногда вызывать утомление глаз при длительной работе. Просмотреть и/или изменить частоту обновления для видеоадаптера можно таким способом:

1. Щелкните правой кнопкой мыши по свободной области рабочего стола и в контекстном меню выберите команду **Разрешение экрана**.
2. Если к компьютеру подключено несколько мониторов, выберите в списке **Дисплей** тот монитор, для которого нужно выполнить настройки.
3. Щелкните по ссылке **Дополнительные параметры**. Выберите в открывшемся диалоговом окне вкладку **Адаптер** и нажмите на ней кнопку **Список всех режимов**. Открывшееся диалоговое окно содержит список всех разрешений и соответствующей частоты обновления.
4. В окне свойств перейдите на вкладку **Монитор** и в списке **Частота обновления экрана** (Screen refresh rate) выберите требуемое значение.

> ***Осторожно!***
>
> Во многих случаях флажок **Скрыть режимы, которые монитор не может использовать** (Hide modes that this monitor cannot display) будет сброшен, чтобы его нельзя было использовать. Если же флажок можно сбросить, имейте в виду, что если частота обновления экрана превышает возможности монитора или видеоадаптера, изображение на экране может быть искаженным. Кроме этого, использование более высокой частоты обновления экрана, чем монитор может поддерживать, способно повредить монитор и/или видеоадаптер.

Профили цветов позволяют получить более реалистичные цвета для конкретных применений. Например, может быть необходимым, чтобы цвета при печати изображений как можно более точно соответствовали цветам, отображаемым на экране. В этом случае может помочь использование профиля цветов, разработанного для этой цели. Получив профиль цветов, его необходимо установить по отдельности на каждый монитор, используя следующую процедуру:

1. Щелкните правой кнопкой мыши по свободной области рабочего стола и в контекстном меню выберите команду **Разрешение экрана**. По умолчанию выбирается первый монитор. Чтобы выполнить настройку второго монитора, щелкните на его значке.

2. Щелкните по ссылке **Дополнительные параметры**. Выберите вкладку **Управление цветом** (Color management) и нажмите на ней одноименную кнопку.
3. В диалоговом окне **Управление цветом** выберите вкладку **Все профили**, содержащую сведения о текущих установленных профилях цветов. Нажмите кнопку **Добавить**.
4. С помощью диалогового окна **Установить профиль** укажите в файловой системе профиль, который нужно установить, а затем нажмите кнопку **Добавить**.
5. В окне **Управление цветом** перейдите на вкладку **Устройства**. Выберите новый профиль, а затем нажмите кнопку **Сделать профилем по умолчанию** (Set as default profile).

Если у вас нет готового профиля цветов, но вы хотите получить подобный эффект, воспользуйтесь средством **Калибровка цветов экрана**, чтобы настроить цвета экрана под свои требования. Чтобы запустить это средство, выполните в командной строке или в поле поиска панели **Приложения** команду `dccw`.

Поиск и устранение неисправностей дисплея

Как упоминалось ранее, на всех компьютерах устанавливаются драйверы монитора и видеоадаптера. Драйвер монитора сообщает Windows о возможностях монитора, а драйвер видеоадаптера — о возможностях этого оборудования.

Очевидно, что драйверы видеоадаптера и монитора играют для компьютера важную роль. При установке видеокомпонентов или обновлении компьютера нужно обеспечить установку драйверов, протестированных и доказавших свою работоспособность и надежность в вашей рабочей среде. При подозрении проблемы с драйверами обновите их, если это возможно. А при подозрении, что причиной проблемы является конфигурация компьютера, загрузите компьютер в безопасном режиме, а затем отредактируйте настройки по умолчанию.

Прежде чем приступать к углубленному диагностированию, установите, с какими программами работал пользователь. Программы, предназначенные для версий Windows более ранних, чем Windows XP, могут создавать проблемы совместимости. Закройте все исполняющиеся программы и проверьте, какой видеорежим используют приложения, подозреваемые в создании проблемы. Если для какой-либо программы требуется особый видеорежим, а переключение и выход из этого режима создают проблему, попробуйте настроить параметры совместимости, чтобы решить эту проблему. Для этого щелкните правой кнопкой мыши на значке приложения и в контекстном меню выберите команду **Properties**. В окне свойств программы перейдите на вкладку **Совместимость**. В разделе **Параметры** задайте подходящую опцию, установив соответствующий флажок, например **Использовать разрешение экрана 640 x 480** (Run in 640 x 480 screen resolution). Если вы не уверены в том, какие параметры совместимости использовать, щелкните правой кнопкой мыши на значке приложения, выберите в контекстном меню команду **Исправление неполадок совместимости** (Troubleshoot compatibility), а затем следуйте инструкциям запустившегося мастера устранения проблем совместимости.

Причиной многих проблем с монитором является некачественное подключение между монитором и видеоадаптером. Если на экране появляются разводы, цветные пятна, диагональные линии или горизонтальные полосы либо присутствуют другие подобные проблемы, первым делом следует проверить качество подключения монитора. Убедившись, что все соединения подключения в порядке, выключите монитор, оставьте его выключенным в течение минимум 10 секунд, а затем опять включите. Если проблема продолжает проявляться и есть основания полагать, что ее причиной является сам монитор, можно попробовать дополнительные диагностические мероприятия.

Мигание или дрожание изображения может быть вызвано проблемной конфигурацией или же местом размещения монитора или кабелей. Если причиной проблемы является неправильная частота обновления, установите такую частоту обновления, которая устранит эту проблему. Инструкции по установке частоты обновления *см. в разд. "Настройка внешнего вида экрана" ранее в этой главе*. Если же проблема вызвана наличием возле монитора источников электромагнитных помех, она решается перемещением в другое место кабелей и устройств, которые могут создавать эти электромагнитные помехи, включая кабели питания других устройств, большие динамики и настольные лампы. Если и это не решит проблему, проверьте, экранирован ли видеокабель, и расположите его подальше от кондиционеров, больших ламп дневного света и т. п.

Если монитор оснащен встроенными средствами управления, проверьте параметры самонастройки. Часто для этого есть отдельная кнопка, нажатие которой выполняет самонастройку монитора.

В случае разводов, цветных пятен или линий, возможно, потребуется выполнять размагничивание монитора. Эта операция состоит в удалении накопившихся магнитных полей вокруг монитора, которые могут искажать изображение. Некоторые мониторы размагничиваются выключением монитора с последующим включением, некоторые имеют специальную кнопку для этого, а некоторые совмещают обе эти возможности. Размагничивание может выполняться как физическим элементом управления (например, кнопкой) или же программными средствами монитора, доступными из его меню. В процессе размагничивания изображение на экране может временно исказиться, что является нормальным явлением. При ручном размагничивании подождите 15—20 минут, прежде чем выполнять повторное размагничивание.

Если проблема продолжает проявляться, подключите монитор непосредственно к компьютеру, т. е. уберите все удлинители, соединяющие монитор с видеоадаптером (если таковые имеются). Также снимите противобликовые экраны и другие подобные устройства, которые закрывают экран монитора. Проверьте видеокабель на наличие согнутых, сломанных или отсутствующих контактов. Хотя отсутствие некоторых контактов предусмотрено дизайном разъемов, те, к которым это не относится или согнуты, вызовут проблемы видеовывода. В случае согнутых контактов, которые можно выпрямить, выключите монитор, вытащите его шнур питания из розетки и с помощью пинцета или утконосов выпрямите их.

ГЛАВА 4

Управление микропрограммой, конфигурацией загрузки и запуском

Когда компьютер перестает загружаться или возникают фатальные сбои операционной системы, основной компонент, связанный с запуском компьютера и загрузкой операционной системы — микропрограмма — часто не принимается во внимание, как возможная причина этой проблемы. Это объясняется тем, что большинство пользователей закачивает рукава и начинает диагностировать операционную систему, забывая о микропрограмме. Проблема с этим подходом состоит в том, что многие проблемы с компьютером зарождаются в микропрограмме либо вследствие неполадок в самой микропрограмме, либо из-за неправильной ее конфигурации. Чтобы понимать, в чем заключается разница между проблемами микропрограммы и проблемами операционной системы, необходимо понимать работу процесса запуска и происходящее на каждом его этапе. Кроме этого, необходимо понимать саму микропрограмму. Приобретя эти знания, вы будете лучше подготовлены к диагностике и устранению проблемы в этих областях.

Опции микропрограммы и их значения

В процессе запуска компьютера принимают участие микропрограмма, микропрограммный интерфейс и операционная система. При запуске компьютера прежде всего исполняется микропрограмма, которая выполняет первоначальную инициализацию компьютера и предоставляет службы, позволяющие компьютеру начать загрузку операционной системы.

Микропрограмма платформы реализуется в чипсете материнской платы. Все компьютеры — будь то планшеты, настольные ПК или ноутбуки — оснащены чипсетом материнской платы. Существует много типов чипсетов, и хотя более старые чипсеты могут не обладать возможностью обновления микропрограммы, большинство новых чипсетов такую возможность имеют. Микропрограмма чипсета — совсем иное, чем интерфейс микропрограммы компьютера.

Операционная система Windows для процессорной архитектуры ARM, Windows RT (которая также называется Windows On Arm, или просто WOA), разработана с микропрограммным обеспечением платформы, которое также реализовано в чипсете материнской платы. Но в случае с устройствами Windows RT материнская плата представляет собой набор кремниевых слоев, упакованных в очень маленький форм-фактор, который называется *однокристальной системой*[1].

[1] System on Chip, SoC.

Примечание

Операционная система Windows RT представляет собой особый случай для микропрограммного обеспечения, конфигурации загрузки и запуска. Хотя в этой главе предпринимаются попытки рассмотрения некоторых аспектов Windows RT, не все, что обсуждается в этой главе, применимо к WOA.

Типы микропрограммного интерфейса и загрузочные данные

Все компьютеры имеют микропрограмму, но процесс запуска компьютера управляется интерфейсом между этой микропрограммой и операционной системой. Особенности работы интерфейса и выполняемые им задания зависят от его типа. В настоящее время наиболее распространенными являются следующие микропрограммные интерфейсы:

- интерфейс BIOS;
- интерфейс EFI;
- интерфейс UEFI.

Микропрограммный интерфейс компьютера, будь то BIOS, EFI[1] или UEFI[2], предоставляет интерфейс аппаратного уровня между аппаратными компонентами и программным обеспечением. Подобно микропрограммам чипсетов, интерфейсы BIOS, EFI и UEFI можно обновлять. В большинстве технической документации микропрограммный интерфейс компьютера называется просто *микропрограммой*[3] (firmware). Например, в документации может указываться "выполните такие и такие изменения микропрограммы" или "проверьте микропрограмму". Но в действительности, изменения выполняются в микропрограммном интерфейсе, а уже микропрограммный интерфейс осуществляет изменения в микропрограмме.

Интерфейс UEFI является как микропрограммным интерфейсом, так и промышленным стандартом. Как микропрограммный интерфейс, UEFI является модульным и не обязательно служит тем же целям или предоставляет ту же функциональность, что и интерфейс BIOS или EFI. А как стандарт, UEFI предназначен для предоставления расширяемых и тестопригодных интерфейсов. Для Windows RT интерфейс UEFI является самым нижним уровнем системы и, как и с другими "кристальными" архитектурами, интерфейс UEFI предоставляет службы, необходимые для загрузки операционной системы.

Операционная система Windows RT также поддерживает технологию TPM[4] для доверяемой загрузки и аппаратного шифрования дисков.

Также важно понимать, что интерфейсы BIOS, EFI и UEFI работают совершенно поразному. Интерфейс BIOS основан на 16-разрядной архитектуре реального времени *x*86 и изначально предназначался для приведения компьютера в рабочее состояние после включения питания. Вот почему интерфейс BIOS выполняет сопряжение микропрограммы с операционной системой и инициализацию системы.

Независимо от типа микропрограммного интерфейса, Windows 8 использует предоперационную загрузочную среду[5]. Среда загрузки представляет собой расширяемый уровень абст-

---

[1] Extensible Firmware Interface — расширяемый микропрограммный интерфейс.

[2] Unified Extensible Firmware Interface — унифицированный расширяемый микропрограммный интерфейс.

[3] Также прошивкой, микрокодом, встроенным ПО и микропрограммным ПО.

[4] Trusted Platform Module — доверенный платформенный модуль.

[5] То есть среду, используемую для управления компьютером до загрузки операционной системы.

ракции, который позволяет операционной системе работать с разными типами микропрограммных интерфейсов, не требуя создания операционной системы специально для работы с этими микропрограммными интерфейсами.

В среде загрузки запуск контролируется с помощью параметров в хранилище BCD[1].

Все компьютеры с операционной системой Windows Vista и более поздними версиями имеют хранилище BCD. Хранилище BCD также называется *реестром BCD* и содержится в файле, который так и называется — *BCD*. Размещение этого файла зависит от микропрограммы компьютера. В частности:

- на компьютерах с операционной системой на основе BIOS файл BCD расположен в папке \Boot\ активного раздела;
- на компьютерах с операционной системой на основе EFI файл BCD расположен в системном разделе EFI.

Элементы хранилища BCD определяют диспетчер загрузки, который нужно использовать при запуске, и доступные приложения загрузки. Диспетчером загрузки по умолчанию является диспетчер загрузки Windows (Windows Boot Manager). Диспетчер загрузки Windows управляет процессом загрузки и позволяет выбирать, какие загрузочные приложения следует исполнять. Приложения загрузки загружают определенную операционную систему или версию операционной системы. Например, приложением загрузки для Windows 8 является загрузчик Windows (Windows Boot Loader). Это позволяет загружать компьютеры на основе BIOS и EFI почти одинаковым способом.

Обычно в начале запуска компьютера можно нажать клавишу <F8> или <F12>, чтобы получить доступ к меню дополнительных параметров загрузки и выбрать в нем один из нескольких дополнительных режимов загрузки, включая безопасный режим (Safe Mode), ведение журнала загрузки (Enable Boot Logging) и отключение обязательной проверки подписи драйверов (Disable Driver Signature Enforcement). Эти дополнительные режимы временно изменяют способ загрузки операционной системы с целью предоставления возможностей для диагностирования и устранения неполадок. Но они не вносят постоянных изменений в конфигурацию загрузки или хранилище BCD.

Службы загрузки, службы времени исполнения и другие

Интерфейс BIOS управляет потоком предзагрузочных данных между операционной системой и подключенными устройствами, такими как видеоадаптер, клавиатура, мышь и жесткий диск. Когда система BIOS выполняет инициализацию компьютера, она сначала определяет доступность и функционирование подключенных устройств, а затем начинает загружать операционную систему.

С течением времени эти основные функциональности BIOS были расширены и сейчас включают следующие.

- **Загрузочные службы.** Коллекция интерфейсов и протоколов, присутствующих в загрузочной среде. Как минимум эти службы предоставляют загрузчик операционной системы с доступом к функциональностям платформы, требуемым для выполнения загрузки операционной системы. Эти службы также доступны для драйверов и приложений, которым требуется доступ к функциональностям платформы. Загрузочные службы прекращают свою работу после того, как управление компьютером берет на себя операционная система.

[1] Boot Configuration Data — данные конфигурации загрузки.

- **Службы времени исполнения.** Интерфейсы, предоставляющие доступ к базовому платформозависимому оборудованию, такому как таймеры, которое может быть затребованным в процессе штатной работы системы. Эти службы присутствуют при загрузке операционной системы, но продолжают функционировать после того, как операционная система прекращает работу загрузочных служб.
- **Интерфейс ACPI**[1]. Интерфейс системной платы на основе таблиц, позволяющий операционной системе реализовать управление электропитанием и конфигурацией системы.
- **Службы SMBIOS**[2]. Табличный интерфейс, требуемый спецификацией WfM[3] Baseline и применяемый для передачи платформозависимой информации операционной системе или средству управления на основе операционной системы.

Как правило, компьютеры с BIOS используют жесткие диски, которые имеют разделы MBR[4]. Чтобы освободиться от 16-разрядности BIOS, компания Intel разработала реализованный в виде микропрограммы интерфейс EFI для своих 64-разрядных процессоров Itanium. Интерфейс EFI основан на 64-разрядной архитектуре реального времени *x*64. Как и BIOS, интерфейс EFI выполняет сопряжение микропрограммы с операционной системой, инициализацию системы и другие функции. Вместе с интерфейсом EFI компания Intel также предоставила новую табличную архитектуру жестких дисков — *таблицу разделов, GUID* (GPT, GUID partition table).

Интерфейс UEFI

В то время как компания Intel начала разрабатывать интерфейс EFI, другие разработчики во всем мире начали осознавать необходимость в удалении связи между микропрограммой и архитектурой процессора. Это обстоятельство и положило начало разработке интерфейса UEFI. Спецификация UEFI 2.0 была завершена в январе 2006 г., а в апреле 2011 г. модифицирована как UEFI 2.3.1. Спецификация UEFI определяет модель сопряжения между операционной системой и микропрограммой платформы. Этот интерфейс состоит из таблиц данных, содержащих информацию о платформе, а также из функций времени загрузки и времени исполнения, доступных операционной системе и ее загрузчику. Интерфейс не зависит от архитектуры процессора. Так как интерфейс UEFI абстрагирует архитектуру микропроцессора, он может применяться на компьютерах с архитектурой *x*86, *x*64, ARM или какой-либо другой архитектурой. Как и в случае с интерфейсом EFI, на платформах с интерфейсом UEFI обычно применяются жесткие диски с разделами GPT. Но интерфейс UEFI не заменяет всю функциональность ни BIOS, ни EFI и, более того, он может служить оболочкой для BIOS или EFI.

ПРАКТИЧЕСКИЙ СОВЕТ

Спецификация UEFI 2.3.1 содержит свыше 2200 страниц. Чтобы сэкономить ваше время, далее приводится краткое изложение его основных функциональностей.

---

[1] Advanced Configuration and Power Interface — усовершенствованный интерфейс конфигурирования системы и управления энергопитанием.

[2] System Management BIOS — системное управление BIOS.

[3] Wired for Management (WFM или WfM) — термин, введенный корпорацией Intel для обозначения набора стандартов управления аппаратным обеспечением. Протоколы WFM служат для обмена информацией, содержащей данные о конфигурации компьютера, сигналы управления питанием и удаленной загрузки, между программным обеспечением управления сетями и персональными компьютерами (**http://ru.wikipedia.org/wiki/Wired_for_Management**).

[4] Master Boot Record — главная загрузочная запись.

Системный уровень абстракции интерфейса UEFI представляет собой микропрограмму, которая абстрагирует особенности реализации платформы и предоставляет базовый интерфейс для программного обеспечения высшего уровня. Интерфейс UEFI определяет как загрузочные службы, так и службы времени исполнения.

Загрузочные службы интерфейса UEFI включают, среди прочих, следующие:

- службу обработки событий, которая создает, ожидает, сигнализирует, проверяет и закрывает события; службу таймера, которая устанавливает таймеры; и службу приоритетов заданий, которая задает приоритет заданий;
- службы распределения памяти, которые выделяют или освобождают страницы памяти, получают карты распределения памяти и выделяют и освобождают память пула;
- загрузочные службы драйверной модели, которые обрабатывают протокольные интерфейсы для устройств, открывают и закрывают протокольные потоки и выполняют подключение и отключение от контроллеров;
- службы изображений, которые загружают, открывают и выгружают изображения;
- вспомогательные службы, которые устанавливают сторожевые таймеры, копируют и присваивают значения памяти, устанавливают конфигурационные таблицы, а также вычисляют циклический избыточный код.

Службы времени исполнения интерфейса UEFI включают, среди прочих, следующие:

- различные службы, которые запрашивают переменные, получают их и присваивают им значения;
- службы времени, которые получают и задают время, а также получают и задают время выхода из спящего режима;
- службы виртуальной памяти, которые выполняют отображение виртуальных адресов и преобразуют указатели памяти;
- прочие службы, которые выполняют сброс компьютера, возвращают значения счетчиков и передают информацию микропрограмме.

Интерфейс UEFI определяет архитектурно-независимые модели для изображений, загружаемых посредством EFI, путей устройств, драйверов устройств, подписывания драйверов и безопасной загрузки. Также этот интерфейс предоставляет следующие возможности:

- поддержку консоли, позволяющую осуществлять вывод простого текста и графики;
- поддержку инфраструктуры HII[1], которая описывает базовые механизмы для управления пользовательским вводом и предоставляет определения для соответствующих протоколов, функций и определений типов, помогающих абстрагировать пользовательский ввод;
- поддержку мультимедиа, обеспечивающую доступ ввода-вывода к файловым системам, файлам и устройствам мультимедиа;
- поддержку шин PCI, SCSI и iSCSI, что позволяет осуществлять доступ ввода-вывода по этим шинам, а также загрузку с устройств SCSI или ISCSI;
- поддержку шины USB, обеспечивающую доступ ввода-вывода посредством USB-контроллеров, USB-шин и USB-устройств;
- поддержку сжатия, посредством предоставления алгоритмов для сжатия и распаковки данных;

[1] Human Interface Infrastructure — инфраструктура пользовательского интерфейса.

- поддержку таблиц интерфейса ACPI[1], что позволяет устанавливать и удалять таблицы ACPI;
- поддержку виртуальной машины байтового кода EFI, обеспечивающую загрузку и исполнение драйверов устройств EFI;
- поддержку сетевых протоколов, посредством определения протокола SNP[2], среды PXE[3] и служб BIS[4]. Протокол SNP предоставляет интерфейс пакетного уровня с сетевыми адаптерами. Среда PXE применяется для доступа к сети и загрузки по сети. Службы BIS используются для сверки цифровой подписи блока данных с цифровым сертификатом с целью проверки целостности и авторизации. Среда PXE использует службы BIS для проверки полученных по сети загрузочных образов, прежде чем исполнять их;
- поддержку протоколов управляемых сетей, посредством определения протоколов MNSBP[5] и MNP[6]. Эти протоколы позволяют одновременный доступ и использование сетевых интерфейсов несколькими событийно-управляемыми драйверами и приложениями. Протокол MNSBP используется для нахождения устройств связи, поддерживаемых драйвером MNP, и для управления экземплярами драйверов протокола. Протокол MNP используется драйверами и приложениями для осуществления необрабатываемого ввода-вывода асинхронных сетевых пакетов;
- поддержку протоколов сетевой адресации, посредством определения протоколов ARPSBP[7], ARP[8], DHCPv4[9] и DHCPv6, а также привязок служб DHCPv4 и DHCPv6;
- поддержку прочих протоколов, таких как протоколы для конфигурации локальных сетей, EAP[10], TCP[11]v4 и привязка служб TCPv4, TCPv6 и привязка служб TCPv6, IPv4 и привязка и конфигурация служб IPv4, IPv6 и привязка и конфигурация служб IPv6, конфигурация IPSec и IPSec2, FTPv4 и привязка служб FTPv4, UDPv4 и привязка служб UDPv4[12], UDPv6 и привязка служб UDPv6, Multicast TFTPv4[13] и Multicast TFTPv6.

> ***Примечание***
>
> В случае Windows RT, интерфейс ACPI используется для перечисления устройств Plug-and-Play (сенсорный контроллер, дисплей и т. п.) в процессе загрузки и для управления электропитанием устройств, находящихся вне однокристальной системы. В противном случае отсутствует дерево устройств или возможность определить, какие устройства подключены к однокристальной системе или способ ее подключения.

Нужно подчеркнуть, что интерфейс UEFI не заменяет ни BIOS, ни EFI. Хотя UEFI использует разные интерфейсы для загрузочных служб и служб времени исполнения, какой-то

---

[1] Advanced System Configuration and Power Interface — усовершенствованный интерфейс конфигурирования системы и управления энергопитанием.

[2] Simple Network Protocol — простой сетевой протокол.

[3] Preboot Execution Environment — предзагрузочная среда исполнения.

[4] Boot Integrity Services — службы целостности загрузки.

[5] Managed Network Service Binding Protocol — протокол привязки служб управляемой сети.

[6] Managed Network Protocol — протокол управляемой сети.

[7] Address Resolution Protocol Service Binding Protocol — протокол привязки службы ARP.

[8] Address Resolution Protocol — протокол разрешения адресов.

[9] Dynamic Host Configuration Protocol — протокол динамической конфигурации узла.

[10] Extensible Authentication Protocol — расширяемый протокол аутентификации.

[11] Transmission Control Protocol — протокол управления передачей.

[12] User Datagram Protocol — протокол дейтаграмм пользователя.

[13] Trivial File Transfer Protocol — простой протокол передачи файлов.

микрокод платформы должен выполнять функции, которые требуются для BIOS и EFI для выполнения конфигурирования и установки системы, т. к. UEFI такие функции не предоставляет. По этой причине UEFI часто реализуется виде оболочки над традиционными BIOS и EFI, когда этот интерфейс заменяет инициализационные точки входа в BIOS или EFI.

Просмотр состояний запуска и питания

На начальной стадии запуска компьютера микропрограммный интерфейс активируют все аппаратное обеспечение, требуемое для загрузки компьютера, включая следующее:

- чипсеты материнской платы;
- процессоры и кэши процессоров;
- оперативную память;
- видео- и аудиоконтроллеры;
- несъемные диски;
- внутренние платы расширения.

После завершения этого процесса микропрограммный интерфейс передает управление компьютером операционной системе. Дальнейший ход событий определяется реализацией микропрограммного интерфейса.

- На компьютерах с BIOS и под управлением Windows XP и более ранними версиями Windows для загрузки операционной системы применяются файлы Ntldr и Boot.ini. Файл Ntldr выполняет загрузку операционной системы, а файл Boot.ini содержит параметры загрузки, включая определение загрузочных разделов. Используя параметры файла Boot.ini, можно добавлять опции для начала работы операционной системы, способы использования компонентов компьютера и функциональностей ОС.
- На компьютерах с BIOS и под управлением Windows Vista и более поздними версиями Windows для загрузки операционной системы применяются диспетчер загрузки Windows и загрузчик Windows. Диспетчер загрузки Windows выполняет инициализацию операционной системы, запуская загрузчик Windows, который в свою очередь загружает операционную систему, используя для этого информацию из хранилища BCD. Используя параметры файла BCD, можно добавлять опции для загрузки операционной системы и определять способы использования компонентов компьютера и функциональностей операционной системы.
- Для систем с процессорами Itanium для загрузки операционной системы применяются файлы Ia64ldr.efi, Diskpart.efi и Nvrboot.efi. Файл Ia64ldr.efi выполняет задачу загрузки операционной системы, файл Diskpart.efi содержит информацию о загрузочных разделах, а файлом Nvrboot.efi задаются параметры загрузки.
- На других компьютерах, в которых используется интерфейс EFI, загрузка управляется файлом Bootmgfw.efi, который затем передает управление загрузчику Windows. Параметры загрузки задаются посредством редактора хранилища BCD (Bcdedit.exe).
- Для компьютеров с UEFI загрузочные службы предоставляют уровень абстракции. В настоящее время этот уровень абстракции представляет собой оболочку над BIOS или EFI. На компьютерах с BIOS для загрузки операционной системы применяется подход на основе BIOS; на компьютерах с EFI для этого используется подход на основе EFI.
- Для компьютеров Windows RT уровень абстракции предоставляется загрузочными службами UEFI. Диспетчер загрузки Windows выполняет инициализацию операционной системы, запуская загрузчик Windows, который в свою очередь загружает операционную

систему, используя для этого информацию из хранилища BCD. Информация, требуемая для конфигурирования устройства, хранится в таблицах.

Работа с микропрограммными интерфейсами

В большинстве компьютеров при включении питания предоставляется возможность доступа к микропрограммному интерфейсу после нажатия клавиши, указанной в выводимом на экран сообщении. Обычно это клавиша <Delete> или <F2>, которую нужно удерживать нажатой в течение нескольких секунд после включения питания. Предоставляемые микропрограммными интерфейсами опции позволяют настроить функциональность аппаратного обеспечения. В частности, предоставляется возможность выполнять следующие наиболее распространенные настройки:

- регулировать яркость экрана (для мобильных вычислительных устройств);
- регулировать уровень шума жесткого диска;
- задавать количество используемых ядер процессора и их рабочую частоту;
- задавать порядок загрузки;
- изменять дату и время, хранящиеся в КМОП-памяти;
- восстанавливать значения по умолчанию параметров микропрограммного интерфейса;
- включать и отключать модульные подключаемые устройства.

Микропрограммные интерфейсы могут предоставлять основную конфигурационную информацию, включая следующие сведения:

- мощность зарядного устройства (для мобильных устройств);
- уровень заряда и состояние батареи (для мобильных устройств);
- тип матрицы и разрешение экрана (для мобильных устройств);
- версия микропрограммы;
- объем памяти;
- процессоры;
- устройства хранения данных;
- видеочипсеты.

Большинство микропрограммных интерфейсов позволяет создавать пароли администратора, пользователя и/или общие пароли, которые недоступны из операционной системы. Если установлен пароль администратора, чтобы получить доступ к изменению параметров микропрограммного интерфейса, нужно ввести этот пароль. При установленном пароле пользователя его нужно ввести, чтобы начать загрузку операционной системы. Утеря этих паролей также означает потерю доступа к настройке параметров микропрограммного интерфейса и/или загрузке операционной системы. Восстановить этот доступ можно, только выполнив сброс паролей; при этом также сбрасываются все пользовательские настройки параметров микропрограммного интерфейса.

Обновление микропрограммного интерфейса часто может разрешить проблемы с системой или добавить новые возможности этого интерфейса. С другой стороны, при отсутствии проблем с системой и сведений о каких-либо дополнительных возможностях интерфейса, которые могли бы быть полезными, обновление микропрограммного интерфейса до самой последней его версии не всегда является обязательным. Кроме этого, следует иметь в виду, что неправильное выполнение обновления микропрограммного интерфейса может повредить компьютер, вплоть до невозможности его запуска.

Исследование микропрограммных интерфейсов

Доступные в микропрограммном интерфейсе информация и опции настройки зависят от компьютера, а также типа и версии самого микропрограммного интерфейса. В основном для настольных компьютеров доступно большее число опций настройки, чем для мобильных устройств.

На момент написания этой книги одним из популярных интерфейсов являлся интерфейс Phoenix SecureCore. Этот интерфейс предоставляет несколько страниц меню с информацией и опциями настройки, включая страницы **Main** (Главная), **Advanced** (Дополнительно), **Security** (Безопасность) и **Boot** (Загрузка). На странице **Main** предоставлены основные сведения о конфигурации компьютера, включая следующие:

- системное время и дата;
- объем системной памяти;
- объем расширенной памяти;
- рабочая частота памяти, например 1333 МГц;
- тип центрального процессора, например Intel Core i5-2430;
- рабочая частота процессора, например 2,40 ГГц;
- объем памяти кэша для уровней кэша L1, L2 и L3;
- тип, модель и объем жесткого диска, например WDC WD5000BPVT-75HXZ 500 Гбайт;
- тип и модель привода оптических дисков, например PLDS DVD +/- RW DU 8A-(S1) ATAPI;
- версия системной BIOS, например A02;
- мощность адаптера сетевого питания, например 65 Вт;
- серийный номер;
- номер средства;
- наименование продукта.

На главной странице меню BIOS можно установить системную дату и время, используя предоставленные для этого параметры. На странице **Advanced** предоставляется дополнительная конфигурационная информация, позволяющая управлять важными параметрами. На этой странице можно просматривать состояния и/или устанавливать такие параметры.

- Включать или отключать возможность подключения нескольких мониторов Intel Multiple Monitor. При включенной возможности операционная система может использовать одновременно встроенный видеоадаптер и видеоадаптер расширения. При отключенной возможности может использоваться только один видеоадаптер (встроенный или адаптер расширения).
- Включать или отключать возможность Intel SpeedStep. При включенной возможности центральный процессор может работать в нескольких режимах производительности. Когда же эта возможность отключена, система не способна регулировать производительность процессора.
- Включать или отключать возможность виртуализации Intel Virtualization. Включение этой возможности позволяет монитору виртуальных машин использовать возможности виртуализации аппаратного обеспечения.
- Включать или отключать возможность Intel Turbo Boost. Когда эта возможность включена, ядра процессора работают на частоте более высокой, чем рабочая, ниже допустимых пределов температуры, тока или потребляемой мощности.

- Включать или отключать возможность USB PowerShare. Включение этой возможности позволяет использовать порт USB PowerShare для зарядки внешних устройств от батареи ноутбука даже при выключенном питании компьютера.
- Включать или отключать возможность USB Emulation. При включенной возможности микропрограмма может работать с USB-устройствами в процессе POST[1].
- Включать или отключать возможность USB Wake Status. Включение этой возможности позволяет USB-устройствам выводить компьютер из спящего режима.

На странице **Security** можно просматривать состояние пароля администратора, пользователя и жесткого диска, а также устанавливать эти пароли. Информация состояния отображает текущее состояние каждого пароля, например:

- **Supervisor Password Is: Clear**;
- **User Password Is: Clear**;
- **Hard Disk Password Status: Clear**.

Следующие конфигурационные параметры позволяют управлять паролями:

- **Set Supervisor Password** (Задать пароль администратора) — управление доступом к микропрограммному интерфейсу;
- **Set User Password** (Задать пароль пользователя) — управление доступом к компьютеру;
- **Set Hard Disk Password** (Задать пароль для жесткого диска) — управление доступом к жесткому диску.

Чтобы установить пароль, выберите требуемую команду, а затем нажмите клавишу <Enter>. Введите новый пароль и подтвердите его, введя этот же пароль в другом поле. Нажмите клавишу <Enter>, чтобы сохранить пароль.

На странице **Boot** можно просматривать и устанавливать загрузочные устройства и их приоритет. Далее приводится пример порядка загрузочных устройств, как он установлен на настольном компьютере автора выпуска фирмы Dell:

1. Жесткий диск.
2. USB-жесткий диск.
3. CD/DVD.
4. USB CD/DVD.
5. USB гибкий диск.
6. Сеть.

При включении питания компьютер пытается загрузить операционную систему с первого указанного в списке устройства. Если первое устройство не содержит приемлемой операционной системы, компьютер переходит ко второму устройству списка и т. д. Перемещение по устройствам списка выполняется нажатием клавиш <↑> и <↓>, а перемещение устройства выше или ниже в списке выполняется нажатием клавиши <+> (плюс) или <–> (минус).

На странице **Exit** предоставлено несколько опций выхода из микропрограммного интерфейса и продолжения запуска компьютера. Наиболее распространенными опциями являются следующие:

- **Exit Saving Changes** — выход с сохранением выполненных настроек;
- **Exit Saving Changes** — выход без сохранения выполненных настроек;

[1] Power-On Self Test — процедура самотестирования компьютера, выполняющаяся после включения питания и до начала загрузки операционной системы.

- **Discard Changes** — отмена выполненных настроек и продолжение работы в интерфейсе;
- **Save Changes** — сохранение выполненных настроек и продолжение работы в интерфейсе.

Каждая страница большинства микропрограммных интерфейсов предоставляет стандартный набор опций:

- **Press Fl to get help** — нажать клавишу <F1> для вызова справки;
- **Press the Up or Down Arrow key to select an item** — нажать клавишу <↑> или <↓> для перемещения по элементам списка;
- **Press Enter to select the current option on a submenu** — нажать клавишу <Enter>, чтобы выбрать текущую опцию в подменю;
- **Press the Left or Right Arrow key to select a menu page** — нажать клавишу <→> или <←> для перехода на другую страницу меню;
- **Press + or — to change values** — нажать клавишу <+> или <–>, чтобы изменить значение выбранного параметра;
- **Press F9 to apply setup defaults** — нажать клавишу <F9>, чтобы установить значения параметров по умолчанию (требуется подтверждение);
- **Press Esc to exit** — нажать клавишу <Esc>, чтобы выйти из интерфейса (при выходе предоставляется возможность сохранить выполненные настройки);
- **Press Enter to apply or execute a command** — нажать клавишу <Enter>, чтобы применить или выполнить команду;
- **Press F10 to save changes and exit the firmware interface** — нажать клавишу <F10>, чтобы сохранить настройки и выйти из микропрограммного интерфейса. (В сообщении, выводящемся при нажатии этой клавиши, уже выбрана опция **Yes**. Чтобы сохранить изменения и выйти, нужно нажать клавишу <Enter>. Чтобы отменить решение о выходе, нужно выбрать опцию **No**, нажав клавишу <Пробел>, а затем — клавишу <Enter>.)

Как можно видеть, конфигурационные опции микропрограммного интерфейса ноутбуков не такие уж и обширные. В противоположность, настольные компьютеры имеют головокружительный набор опций и подопций. Многие из этих опций, однако, будут иметь одинаковое назначение для разных компьютеров. Но так как, по большому счету, для микропрограммных интерфейсов существует ограниченное количество стандартов и соглашений, то для разных компьютеров эти опции могут иметь разные названия и значения.

Состояния энергопотребления и управление питанием

Чтобы лучше понимать аспекты аппаратного обеспечения, связанные с вопросами загрузки, давайте копнем глубже и рассмотрим интерфейс ACPI[1]. Для работы расширенных возможностей состояния энергопотребления необходимо, чтобы чипсет материнской платы, микропрограмма и операционная система поддерживали этот интерфейс. Компоненты, которые поддерживают ACPI, отслеживают состояния энергопотребления компьютера. Операционная система, поддерживающая ACPI, может создавать запросы для переключения в другой ACPI-режим, на которые микропрограммное обеспечение, поддерживающее ACPI, отвечает включением затребованного режима.

[1] Advanced Configuration and Power [management] Interface — усовершенствованный интерфейс управления конфигурированием и энергопотреблением.

Определено шесть разных состояний энергопотребления, от S0, когда все компоненты системы полностью запитаны и система находится в состоянии полной работоспособности, до S5, когда система полностью выключена. Полный список этих состояний и их краткое описание приводится в табл. 4.1.

Таблица 4.1. *Состояния энергопотребления для ACPI в микропрограмме и аппаратном обеспечении*

Состояние	Тип	Описание
S0	Включено	Система полностью запитана, находится в состоянии полной работоспособности и полностью удерживает контекст (такой как содержимое энергозависимых регистров, кэшей и оперативной памяти)
S1	Сон	Уровень энергопотребления системы ниже, чем в состоянии S0. Удерживаются все контексты аппаратного обеспечения и процессора
S2	Сон	Уровень энергопотребления системы ниже, чем в состоянии S1. Питание процессора отключено, контекст процессора и содержимое кэша утеряны
S3	Сон	Уровень энергопотребления системы ниже, чем в состоянии S2. Контексты процессора, чипсета и аппаратного обеспечения утеряны, как и содержимое кэша. Содержимое системной памяти удерживается
S4	Гибернация	Уровень энергопотребления системы ниже, чем в любом из предыдущих состояний сна. Система находится почти в выключенном состоянии. Данные контекста записываются на жесткий диск, и контекст не удерживается. Система может перезапуститься с данных контекста, сохраненных на диске
S5	Выключено	Система выключена и не удерживает никакого контекста. Для запуска системы необходима полная перезагрузка

Состояния S1, S2, S3 и S4 называются *состояниями сна*. В этих состояниях кажется, что система выключена, но в действительности, хотя ее уровень энергопотребления очень низкий, его хватает на удержание достаточного контекста аппаратного обеспечения, чтобы выполнить возврат в рабочее состояние, не требуя перезагрузки системы.

Чипсеты материнской платы поддерживают определенные состояния энергопотребления. Например, материнская плата может поддерживать состояния S0, S1, S4 и S5, но не состояния S2 и S3. В операционных системах Windows под переходом энергопотребления в состояние сна подразумевается переход системы в спящий режим или режим гибернации, а под переходом энергопотребления в состояние пробуждения имеется в виду выход системы из спящего режима или режима гибернации. Режимы сна и гибернации позволяют выполнять выключение и включение системы намного быстрее, чем с применением обычного процесса выключения и запуска.

Таким образом, компьютер выходит из спящего режима, когда он выполняет переход из состояния питания **Выключено** (S5) или из любого состояния сна (S1—S4) в состояние **Включено** (S0). А переход в спящий режим происходит, когда компьютер выполняет переход из состояния питания **Включено** (S5) в состояние **Включено** (S0) или в любое состояния сна (S1—S4). Переход из одного состояния сна непосредственно в другое состояние сна невозможен; прежде чем выполнять переход из одного состояния сна в другое, необходимо выполнить переход в состояние **Включено**.

При работе в микропрограммном интерфейсе управление интерфейсом ACPI и связанными параметрами осуществляется на странице **Advanced/Power Management** (Дополнитель-

но/Управление питанием). Возможные параметры, которые можно настраивать на этой странице, включают следующие.

- **Restore AC Power Loss или AC Recovery** (Действие после потери питания). Задает действие, которое следует предпринять после потери питания. Возможные значения: **Stay Off**, **Last State** и **Power On**. Вариант **Stay Off** (или **Power Off**) означает, что после восстановления питания система остается выключенной. Значение **Last State** восстанавливает систему до того состояния, в котором она находилась, когда произошла потеря питания. А значение **Power On** предписывает после восстановления питания выполнять простую перезагрузку системы.
- **Wake On LAN From S4/S5 или Auto Power On.** Определяет действие, которое следует предпринять, когда при выключенном питании компьютера происходит событие пробуждения, определенное в спецификации PCI Power Management. Возможные значения **Power On** (или **Enabled**) или **Power Off** (или **s**).
- **ACPI Suspend State или Suspend Mode.** Задает ждущий режим. Обычно для этого параметра доступны значения **S1** или **S2**.

> ***Примечание***
>
> Причина в указании двух стандартных имен параметров состоит в том, что на конкретном компьютере может применяться то или другое из них. Какое именно, определяется версией данной микропрограммы.

Так как компании Intel и AMD также предлагают другие технологии для сокращения времени запуска и выключения, возможно наличие других параметров питания. Примеры таких параметров для платформы Intel:

- **Enhanced Intel SpeedStep Technology** (EIST), значение которого может быть **Enabled** (включено) или **Disabled** (отключено);
- **Intel Quick Resume Technology Driver** (QRTD[1]), значение которого может быть **Enabled** (включено) или **Disabled** (отключено).

Параметр **EIST** (который также называется сокращенно просто **SpeedStep**) позволяет динамически регулировать напряжение питания и частоту ядра процессора, что помогает понизить среднее энергопотребление и тепловыделение. При включенной и задействованной возможности EIST или другой подобной возможности на странице **Система** отображаются две разные частоты процессора. Первое значение указывает заданную частоту процессора, а второе — текущую частоту, которая должна быть меньше первого значения. Если возможность EIST отключена, оба значения частоты процессора будут одинаковыми. На работу этой возможности также могут воздействовать значения дополнительных параметров в диалоговом окне **Управление питанием процессора**, открывающемся щелчком по ссылке **Изменить дополнительные параметры электропитания** окна настройки схемы электропитания. В общих словах, эту возможность не следует использовать с Windows 8 (хотя с Windows Vista она может быть полезной).

Возможность QRTD позволяет компьютерам, поддерживающим технологию Viiv, играть роль бытового электронного устройства, способного мгновенно включаться и выключаться после первоначальной загрузки. Такое поведение достигается посредством функции режима Quick Resume чипсета Intel Viiv. Нажатие кнопки питания компьютера или пульта дистанционного управления переводит компьютер в режим Quick Sleep, выход из которого в режим Quick Resume можно осуществить движением мыши, нажатием клавиши включения/выключения (если такова имеется) или нажатием кнопки **Sleep** на пульте дистанцион-

[1] Драйвер технологии Intel Quick Resume.

ного управления. Режим быстрого сна Quick Sleep отличается от стандартного спящего режима. В режиме Quick Sleep видеоадаптер компьютера прекращает отправлять данные на дисплей, звук выключается, а монитор переводится в режим низкого энергопотребления, но при этом питание подается на основные компоненты системы, такие как процессор, вентиляторы охлаждения и т. п. Эта технология изначально была разработана для версии Windows XP Media Center, и обычно ее не следует использовать с Windows 8. (Во многих случаях эта технология не будет работать с Windows Vista, и для нормального перехода в состояние сна и выхода из него эту возможность нужно будет отключить в микропрограммном интерфейсе.)

Ознакомившись в микропрограммном интерфейсе с настройками питания компьютера, также следует изучить параметры загрузки. Во многих случаях можно задавать значения следующих параметров загрузки:

- **Boot Drive Order** — порядок загрузочных устройств;
- **Boot To Hard Disk Drive** — загрузка с жесткого диска. Значение может быть **Disabled** (отключено) или **Enabled** (включено);
- **Boot To Removable Device** — загрузка компьютера со съемного носителя. Значение может быть **Disabled** (отключено) или **Enabled** (включено);
- **Boot To Network** — загрузка компьютера по сети. Значение может быть **Disabled** (отключено) или **Enabled** (включено);
- **USB Boot** — загрузка компьютера с USB-устройств флеш-памяти. Значение может быть **Disabled** (отключено) или **Enabled** (включено).

На некоторых компьютерах может просто предоставляться список загрузочных устройств, из которых можно выбрать требуемое.

Что касается параметров BIOS, их названия на конкретном компьютере могут отличаться от приведенных выше, но, в общем, должны быть довольно похожими, по крайней мере, по смыслу. Эти параметры следует оптимизировать под планируемый способ использования компьютера. Например, если используется возможность шифрования дисков BitLocker, следует включить возможность загрузки со съемных устройств (**Boot to Removable Devices**) или загрузки с USB-устройств памяти (**USB Boot**), или обе эти возможности. Это необходимо для того, чтобы при запуске компьютер мог найти носитель с ключом шифрования, который хранится на съемном носителе.

Диагностирование и решение проблем запуска

Чтобы диагностировать и устранять проблемы запуска, необходимо понимать последовательность событий, происходящих после включения питания компьютера. При нажатии кнопки питания происходит следующее:

1. Микропрограммный интерфейс выполняет проверку работоспособности узлов системы, которая называется процедурой POST *(см. предыдущий разд. "Исследование микропрограммных интерфейсов")*.
2. Далее микропрограммный интерфейс выполняет настройку компьютера, которая также называется инициализацией.
3. После этого микропрограммный интерфейс передает управление компьютером загрузчику операционной системы, который также называется диспетчером загрузки.
4. Диспетчер загрузки запускает загрузчик операционной системы (boot loader). С помощью служб микропрограммного интерфейса начальный загрузчик загружает операционную систему.

Загрузка операционной системы включает:

- загрузку (но не запуск) ядра операционной системы; обычно, это файл Ntoskrnl.exe;
- загрузку (но не запуск) уровня HAL[1]. Обычно, это файл Hal.dll;
- загрузку в память куста реестра `HKEY_LOCAL_MACHINE\SYSTEM` (с файла *%System Root%*\System32\Config\System);
- сканирование ключа реестра `HKEY_LOCAL_MACHINE\SYSTEM\Services` в поисках драйверов устройств, а затем загрузки в память (но не инициализация) драйверов, настроенных для данного класса загрузки. Драйверы также являются службами (что означает подготовку как драйверов устройств, так и системных служб);
- включение функциональности виртуальной памяти.

5. Затем загрузчик передает управление компьютером ядру операционной системы.
6. Ядро операционной системы и уровень HAL инициализируют службы Windows Executive, которые в свою очередь обрабатывают конфигурационную информацию, находящуюся в кусте `HKEY_LOCAL_ MACHINE\SYSTEM\CurrentControlSet`, а затем запускает драйверы устройств и системные службы.
7. Ядро операционной системы запускает диспетчер сеансов (Session Manager, Smss.exe), который в свою очередь:
   - инициализирует системную среду, создавая системные переменные среды;
   - запускает подсистему Win32 (файл Csrss.exe). В этом месте процесса загрузки вывод дисплея переключается с текстового режима в графический;
   - запускает диспетчер входа в систему (Windows Logon Manager, файл Winlogon.exe), который в свою очередь запускает диспетчер управления службами (Services Control Manager, файл Services.exe) и локальную систему безопасности (Local Security Authority, файл Lsass.exe) и переходит в режим ожидания входа пользователя в систему;
   - создает дополнительные требующиеся файлы подкачки;
   - по мере необходимости, выполняет отложенное переименование использующихся файлов, которые были обновлены в предыдущем сеансе.
8. Диспетчер входа в систему ожидает входа пользователя в систему. Интерфейс входа пользователя в систему и поставщик учетных данных (credential provider) получают имя пользователя и его пароль и передают эту информацию локальной системе безопасности для аутентификации.
9. Диспетчер входа в систему запускает на исполнение файл Userinit.exe и оболочку Проводника (File Explorer). Файл Userinit.exe инициализирует пользовательскую среду, создавая пользовательские переменные среды, запуская программы автозагрузки и выполняя прочие необходимые задания.

Эта последовательность событий описывает запуск компьютера от включения питания до входа пользователя в систему. Последовательность будет другой при выходе компьютера из спящего режима, режима ожидания или гибернации. Последовательность событий также будет другой при запуске операционной системы иной, чем Windows, а также при запуске версий Windows более поздних, чем Windows XP (т. е. начиная с Windows Vista).

---

[1] Hardware Abstraction Layer — уровень абстрагирования от оборудования.

Практический совет

Последовательность событий при загрузке Windows RT подобна описанной выше, но также немного отличается от нее. Службы, необходимые для загрузки этой операционной системы, предоставляются микропрограммным интерфейсом UEFI. Диспетчер загрузки Windows выполняет инициализацию операционной системы, запуская загрузчик Windows, который в свою очередь загружает операционную систему, используя для этого информацию из хранилища BCD. Затем загрузчик Windows передает управление компьютером ядру операционной системы. Ядро и уровень HAL инициализируют службы Windows Executive. Информация, требуемая для конфигурирования Windows RT, хранится в таблицах, откуда она считывается операционной системой. Для загрузки драйверов устройств и продолжения процесса загрузки, службы Windows Executive инициализирует набор маломощных последовательных шин, а затем драйверы устройств, которые поддерживают подключения к этим шинам. Теперь ядро может запустить диспетчер сеансов, который в свою очередь приводит в готовность остальную часть операционной системы.

Иногда причину проблемы при запуске операционной системы можно выяснить, определив точку нарушения нормального хода процесса запуска. В табл. 4.2 приводится поэтапное разбиение процесса запуска с указанием возможных причин проблем на каждом этапе. Номера этапов запуска не отображают никакого официального определения и предназначены только для облегчения рассмотрения этого процесса.

Таблица 4.2. *Диагностирование проблем запуска компьютера*

Этап	Название этапа	Возможная причина проблемы
1	Конфигурирование системы, самотестирование POST	Неполадка оборудования или отсутствующее устройство
2	Настройка, начальная загрузка	Конфигурация микропрограммного обеспечения, дисковая подсистема, файловая система
3	Загрузчик операционной системы, диспетчер загрузки	Данные хранилища BCD, неправильный выбор операционной системы для загрузки, ошибочный начальный загрузчик
4	Ядро, уровень HAL, службы Windows Executive	Конфигурация драйверов или служб, зависимости служб
5	Диспетчер сеансов	Графический режим дисплея, системная среда, конфигурация компонентов

Диагностирование первого этапа запуска

Первое, что выполняется при включении питания компьютера — это процедура начального самотестирования POST. На этом этапе микропрограмма материнской платы проверяет исправность аппаратного обеспечения, удостоверяется в наличии необходимых драйверов и считывает параметры конфигурации системы с энергонезависимой памяти на материнской плате. Хотя энергонезависимая память может быть реализована как микросхема ЭСППЗУ[1], флеш-память или RAM с питанием от батарейки, обычно используется флеш-память, содержимое которой сохраняется даже после полного обесточивания.

После выполнения процедуры POST микропрограммой материнской платы подобные самотестирования и загрузку конфигурационных параметров выполняют подключаемые устройства, которые оснащены собственной микропрограммой, такие как видеоадаптеры и платы контроллеров периферийных устройств. Если на этом этапе происходит сбой запуска, то его

[1] Электрически стираемое программируемое постоянное запоминающее устройство (Electronically Erasable Programmable Read-Only Memory — EEPROM).

наиболее вероятной причиной будет неисправность оборудования или отсутствие необходимого устройства, такого как клавиатура, мышь или жесткий диск. В большинстве случаев наличие проблемы и ее причина указываются сообщением об ошибке, выводимым микропрограммным интерфейсом. В случае проблемы с видеовыводом, сообщение может принимать форму звукового сигнала, воспроизводимого на системном динамике.

Проблему с клавиатурой, мышью или дисплеем можно решить, проверив подключение этих устройств к компьютеру. Если же проблему вызывает какое-либо другое устройство, ее можно попытаться разрешить изменением конфигурации этого устройства в микропрограммном интерфейсе или же заменой проблемного устройства.

Диагностирование второго этапа запуска

По завершению самотестирования и конфигурирования материнской платы и подключенных устройств компьютер переходит на этап настройки, или начальной загрузки. Устройство, содержавшее операционную систему для загрузки, определяется настройками микропрограммного интерфейса. Порядок загрузочных устройств, а также включенное или отключенное состояние этих устройств, также оказывает влияния на загрузку. Как упоминалось ранее, компьютер пытается загрузить операционную систему с первого указанного в списке устройства. Если первое устройство не содержит приемлемой операционной системы, компьютер переходит ко второму устройству списка, и т. д. Если ни одно из указанных в списке устройств не содержит приемлемой операционной системы, выводится сообщение об ошибке наподобие следующего:

```
Non-system disk or disk error
  (Несистемный диск или ошибка чтения диска)
Replace and press any key when ready to continue
  (Замените диск и нажмите любую клавишу, когда можно продолжить)
```

В этом случае следует проверить правильность указанного списка загрузочных устройств и сами устройства. При попытке загрузки с привода оптических дисков проверьте наличие диска в приводе, а также, что привод указан в списке загрузочных устройств. При попытке загрузки с жесткого диска проверьте, что жесткий диск указан в списке загрузки и именно перед устройствами загрузки со съемными носителями, такими как устройства флеш-памяти или приводы оптических дисков. Если попытка загрузки предпринимается с новоустановленного жесткого диска, выключите и полностью обесточьте (т. е. извлеките шнур питания системного блока и шнур питания монитора из розетки) компьютер и проверьте правильность и надежность подключения кабелей данных и питания, а также правильность установки конфигурирующих перемычек.

Так как настройка параметров загрузки в микропрограммном интерфейсе может быть не обязательно интуитивной, рассмотрим несколько примеров такой настройки для представительного набора компьютеров от разных производителей. На ноутбуке автора компании Hewlett-Packard (HP) загрузочные параметры находятся на вложенных страницах **Boot Options** и **Boot Order** страницы **System Configuration**. Страница **Boot Options** содержит следующие опции:

- **F10 And F12 Delay (sec)** — задает время ожидания, в течение которого пользователь может нажать клавишу <F10> или <F12>. На данном ноутбуке нажатие клавиш <F10> и <F12> предоставляет доступ к параметрам загрузки и дополнительным параметрам загрузки соответственно;
- **DVD Boot** — разрешает или запрещает использовать для загрузки привод оптических дисков;

- **Floppy Boot** — разрешает или запрещает использовать для загрузки привод гибких дисков;
- **Internal Network Adapter Boot** — разрешает или запрещает использовать для загрузки встроенный сетевой адаптер.

Перемещение между параметрами осуществляется с помощью клавиш <↓> и <↑>, а выбор требуемого параметра — нажатием клавиши <Enter>.

На странице **Boot Order** предоставляется порядок загрузочных устройств, который по умолчанию выглядит таким образом:

1. **USB Floppy**.
2. **ATARI CD/DVD ROM Drive**.
3. **Notebook Hard Drive**.
4. **USB Diskette On Key**.
5. **USB Hard Drive**.
6. **Network Adapter** (только если разрешена опция **Internal Network Adapter**).

Перемещение по устройствам списка выполняется нажатием клавиш <↓> и <↑>, а перемещение выбранного устройства выше или ниже в списке выполняется нажатием клавиши <F5> или <F6> соответственно. Важно отметить, что данный компьютер (подобно многим новым компьютерам) различает USB-брелки (**USB Diskette key**), т. е. флешки, и USB-диски (**USB Hard Drive**), т. е. жесткие диски, подключаемые к USB-порту.

На другом ноутбуке, Dell Inspiron, все загрузочные параметры собраны на одной странице меню микропрограммного интерфейса **Boot**. Порядок загрузочных устройств по умолчанию следующий:

1. **Hard disk** (жесткий диск).
2. **USB hard disk** (жесткий диск USB).
3. **CD/DVD** (привод оптических дисков).
4. **USB CD/DVD** (привод оптических дисков USB).
5. **USB Floppy** (привод гибких дисков USB).
6. **Network** (Сеть).

Перемещение между загрузочными устройствами осуществляется с помощью клавиш <↓> и <↑>. Нажатие клавиши <Enter> открывает данный уровень для выбора для него загрузочного устройства. Уровень загрузки можно временно отключить, задав для него значение **Disabled**.

Все больше настольных компьютеров оснащаются аппаратными контроллерами RAID[1]. На компьютере автора производства фирмы Dell для включения и отключения аппаратного контроллера RAID используется опция **SATA Operation** подменю **Drives**. Обычно аппаратные контроллеры RAID для настольных компьютеров поддерживают типы RAID 0 или RAID 1. Тип RAID 0 не предоставляет возможностей защиты данных, а просто размещает один логический том на нескольких физических дисках. Тип RAID 1 предоставляет возможность защиты данных посредством зеркалирования дисков. При зеркалировании один диск используется в качестве запасного и содержит точно такие же данные, как и основной диск. При этом в системе отображается только один, активный, диск.

[1] Redundant array of independent disks — избыточный массив независимых дисков.

ПРАКТИЧЕСКИЙ СОВЕТ

Компьютер с аппаратным контроллером RAID может отказаться загружаться, если удалить один из приводов, требуемых для работы RAID, не отключив предварительно аппаратный контроллер RAID. Если оставшийся диск является загрузочным, отключите в BIOS возможность RAID, а затем перезагрузите компьютер, чтобы разрешить загрузку операционной системы.

Диагностирование третьего этапа запуска

Выполнив настройку, микропрограммный интерфейс передает управление компьютером диспетчеру загрузок, который запускает загрузчик Windows (boot loader).

На компьютерах с BIOS система считывает данные с главной загрузочной записи (MBR), которая обычно расположена в первом секторе жесткого диска. Запись содержит загрузочные инструкции и таблицу разделов, определяющую дисковые разделы. Активный раздел, который называется *загрузочным разделом* (boot partition), также содержит в своем первом секторе загрузочные данные. Эти данные предоставляют сведения о файловой системе раздела и позволяют микропрограмме найти и запустить программу Bootmgr в корневом каталоге загрузочного раздела. Программа Bootmgr переключает исполнение из реального режима в 32- или 64-разрядный защищенный режим и загружает 32- или 64-разрядный диспетчер загрузки Windows (который содержится в файле самой программы), соответственно. Диспетчер загрузки Windows находит и запускает загрузчик Windows (файл Winload.exe).

На этом этапе проблемы могут быть вызваны отсутствием загрузочного раздела или отсутствующими или искаженными данными загрузочного раздела. Выводимые сообщения об ошибках могут содержать следующие:

```
Error loading operating system
 (Ошибка при загрузке операционной системы)
```

и

```
Invalid partition table
 (Недействительная таблица разделов)
```

Во многих случаях проблемы данного этапа разрешить с помощью инструмента **Восстановление запуска** (Startup Repair).

В отличие от компьютеров с BIOS, компьютеры, использующие EFI, оснащены встроенным диспетчером загрузки. При установке Windows в диспетчер загрузки EFI вставляется элемент, называющийся *диспетчером загрузки Windows* (Windows Boot Manager), который указывает местонахождение исполняемого файла диспетчера загрузки на системном разделе EFI (\Efi\Microsoft\Boot\Bootmgfw.efi). Диспетчер загрузки затем передает управление загрузчику Windows.

В данном случае проблемы могут возникнуть вследствие установки другой операционной системы или изменения настроек диспетчера загрузки EFI. Во многих случаях эти проблемы можно решить с помощью инструмента **Восстановление запуска** и/или редактированием настроек диспетчера загрузки EFI.

Диагностирование четвертого этапа запуска

С помощью служб микропрограммного интерфейса начальный загрузчик завершает загрузку операционной системы. Начальный загрузчик загружает ядро операционной системы (файл Ntoskrnl.exe), а затем загружает уровень HAL (файл Hal.dll). Далее начальный загрузчик загружает в память куст реестра `HKEY_LOCAL_MACHINE\SYSTEM` (файл *%System-Root%*\System32\Config\System), после чего сканирует ключ `HKEY_LOCAL_MACHINE\ SYSTEM\Services`

в поисках драйверов устройств, сконфигурированных для данного класса загрузки, и загружает их в память.

После передачи управления загрузчиком Windows ядру операционной системы, ядро и уровень HAL инициализируют службы Windows Executive, которые в свою очередь обрабатывают конфигурационную информацию, хранящуюся в кусте реестра `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet`, после чего запускает драйверы устройств и системные службы. Драйверы и службы запускаются в соответствии с их значением типа запуска. Это значение задается в подразделе `Start` реестра для каждого раздела `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\`*Имя*, где *Имя* обозначает имя устройства или службы. Допускаются следующие значения этого подраздела:

- `0` — определяет драйвер загрузки;
- `1` — определяет системный драйвер;
- `2` — определяет автозагружаемый драйвер или службу;
- `3` — определяет загружаемый по требованию драйвер или службу;
- `4` — определяет отключенный или незапущенный драйвер или службу;
- `5` — определяет службу с отложенным запуском.

Драйверы запускаются в перечисленном выше порядке.

Большинство проблем на данном этапе связано с неправильными конфигурациями драйверов или служб. Некоторые драйверы и службы зависят от других компонентов и служб. Если компоненты или службы, от которых зависит данный драйвер или служба, не настроены должным образом, то это будет причиной проблемы с работой такого драйвера или службы.

В процессе запуска для конфигурации устройств и служб используются подразделы раздела реестра `HKEY_LOCAL_MACHINE\SYSTEM`. Подраздел `Select` содержит несколько значений, используемых для этой цели:

- значение `Current` является указателем на подраздел раздела `ControlSet`, содержащий текущие определения конфигураций для всех устройств и служб;
- значение `Default` является указателем на подраздел `ControlSet`, содержащий определение конфигурации, используемой компьютером при следующем запуске, при условии отсутствия ошибок и неиспользовании альтернативной конфигурации;
- значение `Failed` является указателем на подраздел `ControlSet`, содержащий определение конфигурации, вызвавшей отказ загрузки Windows;
- значение `LastKnownGood` является указателем на подраздел `ControlSet`, содержащий определение конфигурации, позволившей последний успешный вход в систему.

При обычном запуске компьютера используется набор управления `Default`. Как правило, при отсутствии ошибок при запуске или если не выбрана последняя удачная конфигурация, значения подразделов `Default`, `Current` и `LastKnownGood` указывают на один и тот же подраздел `ControlSet`, например `ControlSet001`. В случае неудачного запуска и последующего выбора последней удачной конфигурации в дополнительных параметрах загрузки микропрограммного интерфейса, значение элемента `Failed` заменяется указателем на определение конфигурации, вызвавшей отказ загрузки. В случае успешного запуска без выбора последней успешной конфигурации, значение `LastKnownGood` заменяется указателем на определение текущей конфигурации.

Диагностирование пятого этапа запуска

На последнем этапе запуска компьютера ядро операционной системы запускает диспетчер сеансов (файл Smss.exe). Тот инициализирует системную среду, создавая системные переменные среды и запуская подсистему Win32 (файл Csrss.exe). В этой точке процесса запуска также происходит переключение из текстового режима видеовывода в графический. Обычно в случае неисправности видеоадаптера или его плохого контакта в разъеме видеовывод будет отсутствовать в любом из этих режимов, но неправильная конфигурация видеоадаптера часто обнаруживается при переключении в графический режим. При неправильной конфигурации видеоадаптера возникают проблемы с полосами на экране *(см. разд. "Поиск и устранение неисправностей дисплея" главы 3)*.

Дисплей является только одним из нескольких компонентов, проблемы с которыми начинают впервые проявляться на этом последнем этапе запуска компьютера. При сбое запуска на этом этапе проблемные компоненты можно определить с помощью журнала загрузки. А если на этом этапе загрузки происходит ошибка останова, определить проблемный компонент может помочь информация в сообщении об этой ошибке.

Диспетчер сеансов запускает диспетчер входа в систему (Windows Logon Manager, файл Winlogon.exe), который в свою очередь запускает диспетчер управления службами (Services Control Manager, файл Services.exe) и локальную систему безопасности (Local Security Authority, файл Lsass.exe) и переходит в режим ожидания входа пользователя в систему. Когда пользователь выполняет вход в систему, диспетчер входа в систему запускает на исполнение файл Userinit.exe и оболочку Проводника (File Explorer). Файл Userinit.exe инициализирует пользовательскую среду, создавая пользовательские переменные среды, запуская программы автозагрузки и выполняя прочие необходимые задания. Оболочка Проводника Windows предоставляет рабочий стол, панель задач и систему меню.

Причиной проблем, возникающих в процессе или после входа в систему, является, скорее всего, неправильная конфигурация какой-либо службы или приложения автозагрузки. Одним из подходов к диагностированию проблем этого типа будет временное отключение служб и приложений автозагрузки, как рассматривается в следующем разделе.

Управление конфигурацией запуска и загрузки

Обычно, в начале запуска компьютера можно нажать клавишу <F8> или <F12>, чтобы получить доступ к меню дополнительных параметров загрузки и выбрать в нем один из нескольких дополнительных режимов загрузки. Но выбор дополнительного режима загрузки не вносит постоянных изменений в конфигурацию загрузки или хранилище BCD. Для редактирования конфигурации загрузки и управления хранилищем BCD используются, среди прочих, такие средства, как диалоговое окно **Загрузка и восстановление**, утилита **Конфигурация системы** и редактор хранилища BCD. Применение этих инструментов рассматривается в следующих разделах.

Настройка параметров загрузки и восстановления

Диалоговое окно **Загрузка и восстановление** позволяет управлять основными параметрами операционной системы в процессе запуска компьютера. Посредством этих параметров можно задать операционную систему, загружаемую по умолчанию, длительность периода отображения списка выбора операционных систем, а также длительность периода отображения опций восстановления, при возникновении необходимости в них. Независимо от вы-

бранной для загрузки операционной системы, эти параметры следует оптимизировать, чтобы сократить время ожидания при загрузке, ускоряя, таким образом, запуск компьютера.

Диалоговое окно **Загрузка и восстановление** можно открыть следующим образом:

1. В Панели управления щелкните на ссылке категории **Система и безопасность** и в открывшемся списке элементов этой категории выберите ссылку **Система**.
2. В левой панели окна щелкните на ссылке **Дополнительные параметры системы**, вследствие чего откроется диалоговое окно **Свойства системы**.
3. В разделе **Загрузка и восстановление** вкладки **Дополнительно** нажмите кнопку **Параметры**. Откроется диалоговое окно **Загрузка и восстановление** (рис. 4.1).

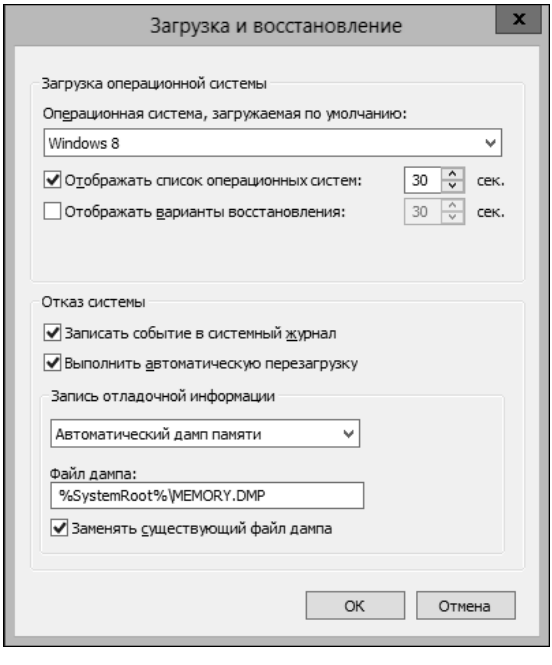


Рис. 4.1. Диалоговое окно для настройки параметров запуска операционной системы

4. Если на компьютере установлено несколько операционных систем, указать операционную систему для загрузки по умолчанию можно в соответствующем списке вверху окна.
5. Для отображения списка операционных систем установите соответствующий флажок и задайте длительность периода отображения списка с помощью счетчика справа от флажка. Чтобы ускорить процесс запуска, длительность периода следует установить равной 5 с.
6. Для отображения вариантов восстановления установите соответствующий флажок и задайте длительность периода отображения вариантов посредством счетчика справа от этого флажка. Как и в случае со списком операционных систем, чтобы ускорить процесс запуска, длительность этого периода рекомендуется установить равной 5 с.
7. Если требуется вести запись событий, связанных с отказами системы, установите флажок **Записать событие в системный журнал** в разделе **Отказ системы**. Если требуется автоматическая перезагрузка компьютера после отказа, установите флажок **Выполнять автоматическую перезагрузку**.
8. Нажмите кнопку **OK**, чтобы сохранить и применить выполненные настройки.

Управление конфигурацией загрузки системы

Утилита **Конфигурация системы** (файл Msconfig.exe) позволяет выполнять тонкую настройку процесса запуска компьютера. Обычно эта утилита применяется для диагностирования и поиска и устранения неполадок. Например, как часть процесса поиска причин неполадок, компьютер можно настроить на выполнение диагностического запуска, когда загружаются только базовые устройства и службы.

Окно утилиты можно открыть, выполнив из Панели управления последовательный переход по ссылкам **Система и безопасность | Администрирование | Конфигурация системы**. Другой способ открыть это окно — выполнить команду `msconfig.exe` в консоли командной строки или в поле поиска панели **Приложения**. Как можно видеть на рис. 4.2, окно утилиты содержит несколько вкладок с различными параметрами.

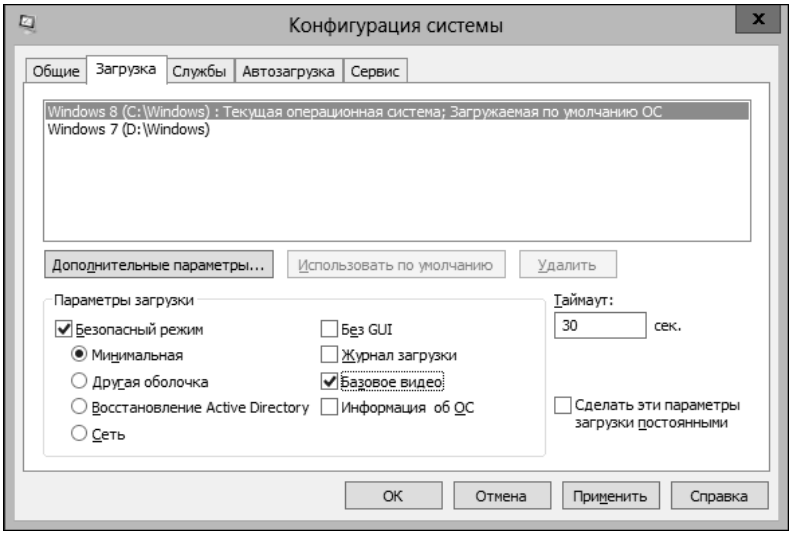


Рис. 4.2. Утилиту **Конфигурация системы** можно использовать для диагностирования

Параметры на вкладке **Общие** позволяют настраивать способ запуска компьютера и являются исходной точкой процесса диагностирования и поиска причин неполадок. Посредством этих параметров компьютер можно настроить для запуска в нормальном, диагностическом или выборочном режиме. В случае запуска в одном из двух последних режимов после устранения неполадок и перезапуска компьютера следует снова открыть окно утилиты **Конфигурация системы** и на вкладке **Общие** задать обычный запуск, установив соответствующий переключатель.

Параметры на вкладке **Загрузка** позволяют управлять отдельными процессами, связанными с загрузкой. В частности, компьютер можно настроить для запуска в одной из разновидностей загрузки в режиме безопасности и установить дополнительные параметры, такие как загрузка без графического интерфейса пользователя (флажок **Без GUI**). Если по завершению процесса диагностирования и поиска причин неполадок необходимо сохранить конкретный набор параметров, это можно сделать, установив флажок **Сделать эти параметры загрузки постоянными**, в результате чего эти параметры будут добавлены в виде дополнительного варианта загрузки.

Нажатие кнопки **Дополнительные параметры** на вкладке **Загрузка** открывает диалоговое окно **Дополнительные параметры загрузки** (рис. 4.3).

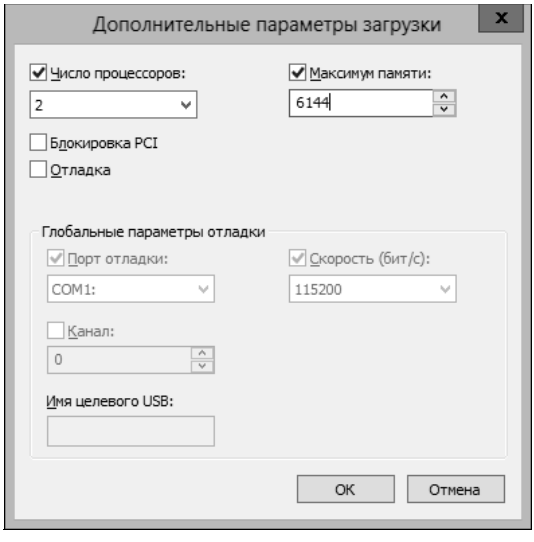


Рис. 4.3. Диалоговое окно для установки дополнительных параметров загрузки

Кроме блокировки PCI и разрешения отладки, в этом окне можно выполнять следующие настройки.

- Задавать количество процессоров для использования операционной системой, будь то дискретные процессоры в отдельных гнездах или же ядра одного центрального процессора. Эта опция может быть полезной при подозрении, что проблема связана с работой нескольких процессоров или параллелизмом. Рассмотрим следующий сценарий: имеется компьютер, оснащенный четырехъядерным процессором. Специализированное приложение для управления складскими запасами работает на этом компьютере очень плохо, тогда как на компьютерах с одноядерным процессором проблем не возникает. Настройка данного компьютера на использование только одного ядра улучшает работу приложения до уровня других, одноядерных, компьютеров. Отсюда можно сделать вывод, что приложение не оптимизировано должным образом для работы в режиме параллельных вычислений, о чем извещает команда его разработчиков.
- Задавать максимальный объем памяти для использования операционной системой. Эта опция используется при наличии подозрений, что причиной проблемы может быть установка дополнительной памяти. Рассмотрим следующий сценарий: в компьютер, оснащенный 8 Гбайт оперативной памяти, было дополнительно установлено 8 Гбайт. Немного позже после этой установки возникают проблемы с запуском Windows 8. Вместо того чтобы вскрывать компьютер и физически извлекать дополнительную память, чтобы проверить, не является ли она причиной проблемы, можно просто ограничить объем памяти, установив для параметра **Максимум памяти** значение 8192 Мбайт.

При наличии подозрений, что причиной проблем запуска компьютера могут быть установленные на нем службы, эти подозрения можно быстро подтвердить или опровергнуть, выбрав на вкладке **Общие** диалогового окна **Конфигурация системы** диагностический или выборочный запуск, а на вкладке **Службы** временно отключив службу, которая подозревается, как причина этой проблемы, после чего перезапустить компьютер. Если проблема больше не проявляется, скорее всего, ее причиной была отключенная служба. В качестве решения проблемы данную службу можно отключить постоянно или же связаться с ее поставщиком и узнать, нет ли более новой версии исполняемого файла этой службы. Для отключения службы нужно просто сбросить ее флажок.

Аналогично, при подозрении, что причиной проблемы запуска компьютера может быть какая-либо программа автозагрузки, проверить эти подозрения можно, исключив это приложение из автозагрузки. Для этого нужно выбрать вкладку **Автозагрузка**, а на ней щелкнуть по ссылке **Открыть диспетчер задач** (Open Task Manager). Откроется окно **Диспетчер задач**, в котором нужно выбрать вкладку **Автозагрузка**. Теперь следует выбрать подозреваемое приложение и отключить его, нажав кнопку **Отключить** в правом нижнем углу окна. Если проблема больше не проявляется, скорее всего, ее причиной было отключенное приложение автозагрузки. В качестве решения проблемы данное приложение можно отключить постоянно или же связаться с его поставщиком и узнать, нет ли более новой версии исполняемого файла этого приложения.

Следует иметь в виду, что при использовании утилиты **Конфигурация системы** для диагностирования и поиска причин неполадок после устранения неполадок и перезапуска компьютера следует снова открыть окно утилиты и на вкладке **Общие** задать обычный запуск, установив соответствующий переключатель.

Использование редактора хранилища BCD

Хранилище BCD содержит несколько записей параметров конфигурации загрузки. Для компьютеров с BIOS это хранилище содержит следующие записи.

- Одну запись для диспетчера загрузки Windows. Так как имеется только один диспетчер загрузки, то для него требуется лишь одна запись.
- Одна или больше записей для приложения загрузчика Windows (Windows Boot Loader) — по одной записи для каждого экземпляра операционной системы Windows 8, Windows 7 или Windows Vista, установленной на компьютере. Для серверных версий Windows, начиная с Server 2008, также будет по одной записи для каждой установки.

Кроме этого, для других установленных операционных систем имеется одна запись для унаследованной операционной системы. Эта запись не предназначена для приложения загрузки, а используется для инициализации загрузчика Ntldr и Boot.ini для загрузки Windows XP или более ранних версий Windows. Если на компьютере установлено несколько унаследованных операционных систем, требуемую систему для загрузки можно указать после выбора записи для унаследованных операционных систем.

Диспетчер загрузки Windows является приложением загрузки. Кроме этого приложения, используются другие загрузчики, в том числе:

- загрузчик унаследованной операционной системы, обозначаемый как Ntldr;
- загрузчик Windows Vista или более поздних версий Windows, обозначаемый как Osloader;
- приложение Windows Boot Sector, обозначаемое как Bootsector;
- диспетчер загрузки микропрограмм (Firmware Boot Manager), обозначаемый как Fwbootmgr;
- загрузчик возобновления Windows (Windows Resume Loader), обозначаемый как Resume.

Записи хранилища BCD можно просматривать и редактировать с помощью редактора BCD (исполняемый файл Bcdedit.exe). Редактор BCD является утилитой командной строки. Запустить редактор BCD можно следующим образом:

1. Откройте консоль командной строки с правами администратора.
2. Для этого щелкните по значку консоли командной строки правой кнопкой мыши и в открывшейся панели внизу экрана щелкните на опции **Запуск от имени администратора**.
3. В консоли выполните команду `bcdedit`.

В табл. 4.3 приводится список и краткое описание команд редактора хранилища BCD. Эти команды позволяют:

- создавать, импортировать, экспортировать и идентифицировать все хранилище BCD;
- создавать, удалять и копировать отдельные записи хранилища BCD;
- задавать и/или удалять значения параметров записей хранилища;
- управлять порядком загружаемых операционных систем и диспетчером загрузки;
- конфигурировать службы EMS[1] и управлять ими;
- конфигурировать и управлять отладкой загрузки, а также отладкой гипервизора.

Таблица 4.3. *Команды редактора хранилища BCD*

Команда	Описание
`/bootdebug`	Включает или отключает возможность отладки загрузки для приложения загрузки
`/bootems`	Включает или отключает службы EMS для приложения загрузки
`/bootsequence`	Задает одноразовый порядок загрузки для диспетчера загрузки
`/copy`	Создает копии записей хранилища
`/create`	Создает новые записи в хранилище
`/createstore`	Создает новое (пустое) хранилище данных конфигурации загрузки
`/dbgsettings`	Задает глобальные параметры отладчика
`/debug`	Включает или отключает возможность отладки ядра для записи операционной системы
`/default`	Задает запись по умолчанию для использования диспетчером загрузки
`/delete`	Удаляет записи из хранилища
`/deletevalue`	Удаляет из хранилища параметры записи
`/displayorder`	Задает порядок отображения операционных систем в меню многовариантной загрузки
`/ems`	Включает или отключает службы EMS для записи операционной системы
`/emssettings`	Задает глобальные параметры служб EMS
`/enum`	Выводит список записей в хранилище
`/export`	Экспортирует содержимое системного хранилища в файл, который впоследствии можно использовать для восстановления состояния хранилища
`/hypervisorsettings`	Задает параметры гипервизора
`/import`	Восстанавливает состояния системного хранилища из архивного файла, созданного командой `/export`
`/mirror`	Создает дубликат записей в хранилище
`/set`	Задает значения параметров записи хранилища
`/store`	Задает хранилище BCD для применения. Если не указано конкретное хранилище, используется системное хранилище

[1] Emergency Management Services — службы аварийного управления.

Таблица 4.3 *(окончание)*

Команда	Описание
/sysstore	Задает устройство системного хранилища. Применимо только к системам EFI
/timeout	Задает значение тайм-аута для диспетчера загрузок
/toolsdisplayorder	Задает порядок отображения элементов в меню инструментов
/v	Отображает все идентификаторы записей в полном виде вместо использования кратких обозначений для известных идентификаторов

Управление хранилищем BCD

Редактор хранилища BCD представляет собой инструмент с расширенными возможностями для просмотра и редактирования конфигурации предоперационной загрузочной среды. Хотя в последующих разделах рассматривается редактирование хранилища BCD, делать это следует только в том случае, если вы являетесь профессионалом в области компьютерных технологий. В любом случае, прежде чем вносить какие-либо изменения в хранилище BCD, следует создать полную резервную копию компьютерной системы. Причина этому должна быть очевидной — в случае неудачных модификаций хранилища компьютер может отказаться загружаться, и резервную копию можно использовать для восстановления его прежнего состояния.

Просмотр записей хранилища BCD

Хранилища BCD могут быть системными и несистемными. *Системное хранилище* BCD содержит загрузочные записи операционных систем и связанные загрузочные параметры. При использовании редактора хранилища BCD обработке подвергается системное хранилище BCD.

Для компьютера только с одной операционной системой записи хранилища BCD будут выглядеть подобно показанным в листинге 4.1.

Листинг 4.1. Записи хранилища BCD для компьютера с одной операционной системой

```
Диспетчер загрузки Windows
--------------------------
идентификатор           {bootmgr}
device                  partition=C:
description             Windows Boot Manager
locale                  ru-RU
inherit                 {globalsettings}
integrityservices       Enable
default                 {current}
resumeobject            {ef70312f-2452-11e2-b6ce-d4d83fa24edd}
displayorder            {current}
toolsdisplayorder       {memdiag}
timeout                 30

Загрузка Windows
----------------
идентификатор           {current}
```

```
device                  partition=C:
path                    \Windows\system32\winload.exe
description             Windows 8
locale                  ru-RU
inherit                 {bootloadersettings}
recoverysequence        {ef703131-2452-11e2-b6ce-d4d83fa24edd}
integrityservices       Enable
recoveryenabled         Yes
allowedinmemorysettings 0x15000075
osdevice                partition=C:
systemroot              \Windows
resumeobject            {ef70312f-2452-11e2-b6ce-d4d83fa24edd}
nx                      OptIn
bootmenupolicy          Standard
```

Как можно видеть из листинга 4.1, хранилище BCD для данного компьютера имеет две записи: одну для диспетчера загрузки Windows и одну для загрузчика Windows. В данном случае диспетчер загрузки Windows вызывает загрузчик Windows, который в свою очередь запускает Windload.exe для загрузки Windows 8.

Записи хранилища BCD для диспетчера загрузки Windows и для загрузчика имеют похожие свойства. Краткое описание основных из этих свойств приведено в табл. 4.4.

Таблица 4.4. *Свойства записей хранилища BCD*

Свойство	Описание
`Description`	Отображает описательную информацию, помогающую определить тип записи
`Device`	Отображает путь физического устройства. Для раздела жесткого диска значение этого свойства будет, например, `partition=C:`
`FileDevice`	Отображает путь к файловому устройству, например, `partiton=C:`
`FilePath`	Отображает путь к требуемому файлу, например, `\Hiberfil.sys`
`Identifier`	Отображает дескриптор записи. Это может быть тип приложения начального загрузчика, например, Bootmgr или Ntldr, ссылка на запись текущей операционной системы, или идентификатор GUID конкретного объекта. Список стандартных идентификаторов приводится в табл. 4.5
`Inherit`	Отображает список записей, подлежащих наследованию
`Locale`	Отображает региональные стандарты компьютера, например, en-US или ru-RU. Значение этого свойства определяет язык, используемый в пользовательском интерфейсе. Папка \Boot содержит подпапку для каждого поддерживаемого регионального стандарта, каждый из которых содержит подробности пользовательского интерфейса, ориентированные на данный язык, для диспетчера загрузки Windows и средства проверки памяти Windows (файл Memdiag.exe)
`Osdevice`	Отображает путь к устройству операционной системы, например `partiton=C:`
`Path`	Отображает действительный путь к приложению начального загрузчика, например, \Windows\System32\Winload.exe

При работе с BCD-хранилищем в редакторе BCD можно видеть ссылки на идентификаторы GUID и стандартные идентификаторы. Краткое описание последних приведено в табл. 4.5. Идентификаторы GUID имеют следующий формат:

```
{NNNNNNNN-NNNN-NNNN-NNNN-NNNNNNNNNNNN}
```

где каждая буква N представляет шестнадцатеричную цифру. Например:

```
{16b857ad-9e02-11e0-9c17-b7d085eb0682}
```

Разделяющие группы цифр тире должны вводиться в позициях, показанных в примере. Как идентификаторы GUID, так и стандартные идентификаторы заключаются в фигурные скобки.

Таблица 4.5. *Стандартные идентификаторы*

Идентификатор	Описание
{badmemory}	Содержит глобальный список дефектов оперативной памяти, который может быть унаследован любой записью загрузочного приложения
{bootloadersettings}	Содержит коллекцию глобальных параметров, которые должны наследоваться всеми записями приложения начального загрузчика Windows
{bootmgr}	Обозначает запись диспетчера загрузки Windows
{current}	Представляет виртуальный идентификатор, соответствующий загрузочной записи текущей операционной системы
{dbgsettings}	Содержит глобальные параметры отладчика, которые могут быть унаследованы любой записью загрузочного приложения
{default}	Представляет виртуальный идентификатор, соответствующий записи приложения по умолчанию начального загрузчика
{emssettings}	Содержит глобальные службы EMS, которые могут быть унаследованы любой записью загрузочного приложения
{fwbootmgr}	Обозначает запись диспетчера загрузки микропрограмм. Эта запись используется системами EFI
{globalsettings}	Содержит коллекцию глобальных параметров, которые должны наследоваться всеми записями приложения загрузки
{hypervisorsettings}	Содержит параметры гипервизора, которые могут наследоваться любой записью загрузчика оперативной системы
{memdiag}	Обозначает запись приложения для диагностирования памяти
{ntldr}	Обозначает загрузчик наследуемых операционных систем Windows (Ntldr), посредством которого можно загружать версии Windows более ранние, чем Windows Vista. Используется, когда на компьютере установлена наследуемая операционная система
{ramdiskoptions}	Содержит дополнительные параметры, требуемые диспетчером загрузки для устройств RAM-дисков
{resumeloadersettings}	Содержит коллекцию глобальных параметров, которые должны наследоваться всеми записями приложения Windows выхода из режима гибернации

Когда на компьютере установлены дополнительные экземпляры версий Windows Vista или более поздних версий, для каждой дополнительной операционной системы в хранилище BCD создается отдельная запись. Например, хранилище BCD может иметь одну запись для диспетчера загрузки Windows и по одной записи загрузчика Windows для каждой установленной операционной системы.

Когда же на компьютере дополнительно установлена наследуемая операционная система, например Windows XP, хранилище BCD будет иметь три записи: одну для диспетчера загрузки Windows, одну для загрузчика наследуемой операционной системы Windows и одну

для загрузчика Windows. Стандартная запись для загрузчика наследуемой операционной системы Windows выглядит так, как показано в листинге 4.2.

Листинг 4.2. Пример записи загрузчика наследуемой операционной системы Windows

```
Windows Legacy OS Loader
------------------------
identifier:       {ntldr}
device:           partition=C:
path:             \ntldr
description:      Earlier version of Windows
```

Записи для диспетчера загрузки Windows, загрузчика наследуемой операционной системы Windows и загрузчика Windows являются основными типами записей управления загрузкой. Кроме них хранилище BCD также содержит информацию о параметрах загрузки и загрузочных утилитах. Запись загрузчика Windows может содержать параметры для отслеживания загрузочных настроек, например, состояние политики **No Execute (NX)** — `Opt In` или `Opt Out`. Запись загрузчика Windows может также содержать информацию о доступных загрузочных утилитах, например об утилите проверки памяти Windows.

Получить значение идентификатора GUID, требуемое для манипулирования хранилищем BCD, можно, выполнив команду `bcdedit /v` с правами администратора.

Создание и идентификация хранилища BCD

Создать несистемное хранилище BCD с помощью редактора BCD можно, выполнив следующую команду (в консоли, открытой с правами администратора):

```
bcdedit /createstore StorePath
```

где параметр *`StorePath`* обозначает путь файла несистемного хранилища BCD. Например:

```
bcdedit /createstore c:\non-sys\bcd
```

На EFI-системах можно временно задать устройство системного хранилища BCD с помощью команды `/sysstore`. В данном случае используется следующий синтаксис:

```
bcdedit /sysstore StoreDevice
```

где параметр *`StoreDevice`* обозначает идентификатор фактического устройства хранилища BCD. Например:

```
bcdedit /sysstore c:
```

Устройство должно быть системным разделом. Обратите внимание, что такая настройка не сохраняется после перезагрузки и применяется только в тех случаях, когда устройство системного хранилища не определено.

Импортирование и экспортирование хранилища BCD

Редактор хранилища BCD предоставляет отдельные команды для импорта и экспорта хранилища BCD. С помощью команды `/export` содержимое хранилища BCD можно скопировать в определенную папку. Эта команда имеет следующий синтаксис:

```
bcdedit /export StorePath
```

где параметр *StorePath* задает путь файла, в который выполняется экспортирование системного хранилища BCD. Например:

```
bcdedit /export c:\backup\bcd
```

Для восстановления хранилища BCD из экспортированного файла применяется команда `/import`. Она имеет следующий синтаксис:

```
bcdedit /import ImportPath
```

где параметр *ImportPath* задает путь файла, из которого выполняется импортирование системного хранилища BCD. Например:

```
bcdedit /import c:\backup\bcd
```

На EFI-системах к команде импорта можно добавить параметр `/clean`, чтобы задать удаление всех существующих записей загрузчика микрограммы. Например:

```
bcdedit /import c:\backup\bcd /clean
```

Создание, копирование и удаление записей хранилища BCD

Редактор BCD позволяет создавать, копировать и удалять записи в хранилище BCD. Для создания записей идентификаторов, приложений и наследований применяется команда `/create`.

Как показано ранее в табл. 4.5, редактор BCD распознает многие стандартные идентификаторы, включая идентификатор `{dbgsettings}` для создания записи параметров отладчика, идентификатор `{ntldr}` для создания записи загрузчика наследуемой оперативной системы Windows и идентификатор `{ramdiskoptions}` для создания записи дополнительных параметров RAM-диска. Для создания идентификаторов используется следующий синтаксис команды `/create`:

```
bcdedit /create Identifier /d "Description"
```

где параметр *Identifier* обозначает стандартный идентификатор для создаваемой записи. Например:

```
bcdedit /create {ntldr} /d "Earlier Windows OS Loader"
```

Также можно создавать записи для конкретных загрузочных приложений, включая следующие:

- `bootsector` — задает приложение реального режима загрузочного сектора; используется для настройки загрузочного сектора под приложение реального режима;
- `osloader` — задает приложение загрузчика операционной системы; применяется для загрузки версий Windows Vista или более поздних версий Windows;
- `resume` — задает приложение загрузчика возобновления Windows; применяется для вывода операционной системы из режима гибернации;
- `startup` — задает приложение реального режима; используется для определения приложения реального режима.

Для создания записей приложений применяется следующий синтаксис команды `/create`:

```
bcdedit /create /application AppType /d "Description"
```

где параметр *AppType* обозначает одно из перечисленных выше приложений. Например:

```
bcdedit /create /application osloader /d "Windows 8"
```

Для удаления записей из системного хранилища BCD применяется команда `/delete`, которая имеет следующий синтаксис:

```
bcdedit /delete Identifier
```

При удалении стандартного идентификатора с командой `/delete` необходимо использовать параметр `/f`, чтобы принудить удаление. Например:

```
bcdedit /delete {ntldr} /f
```

По умолчанию при использовании команды `/delete` подразумевается параметр `/cleanup`, означающий, что редактор BCD удаляет все ссылки на удаляемую запись. Таким образом обеспечивается отсутствие в хранилище данных недействительных ссылок на удаленные идентификаторы. Так как записи также удаляются из отображаемого списка порядка загрузки, в результате удаления записи может быть задана другая операционная система в качестве системы, загружаемой по умолчанию. Чтобы при удалении записи удалить все ссылки на нее, за исключением ссылки из отображаемого списка загрузки, с командой `/delete` следует использовать параметр `/nocleanup`.

Установка значений записей BCD

После создания записи хранилища BCD нужно задать значения для параметров дополнительных записей, для которых это требуется. Для установки значений параметров опций применяется следующий базовый синтаксис:

```
bcdedit /set Identifier Option Value
```

где *Identifier* обозначает модифицируемую запись, *Option* — параметр, которому нужно присвоить значение, а *Value* — присваиваемое значение. Например:

```
bcdedit /set {current} device partitioned:
```

Для удаления параметров и их значений используется команда `/deletevalue`, которая имеет следующий синтаксис:

```
bcdedit /deletevalue Identifier Option
```

где *Identifier* обозначает модифицируемую запись, а *Option* — параметр, который нужно удалить. Например:

```
bcdedit /deletevalue {current} badmemorylist
```

Присваивать булевы значения параметрам можно разными способами. Для значения **Истина** можно использовать `1`, `On`, `Yes` или `True`, а для значения **Ложь** — `0`, `Off`, `No`, или `False`.

Записи хранилища BCD для всех загрузочных приложений и значения параметров можно просмотреть, выполнив команду `bcdedit /enum all /v` в консоли, открытой с правами администратора. Эта команда выводит список всех записей BCD, независимо от их текущего состояния, предоставляя при этом подробное описание всех элементов. Каждая дополнительная запись имеет конкретное назначение и перечисляет значения, которые можно присваивать, включая следующие.

- **Выход из режима гибернации** (Resume From Hibernate). Эта запись содержит данные текущей конфигурации для выхода из режима гибернации. Выходом из режима гибернации управляет предоперационная утилита Winresume.exe, которая находится в папке C:\Windows\System32. Данные гибернации, как указывается в параметре `filepath`, хранятся в файле hiberfil.sys в корневой папке устройства `OSDevice` (в данном примере это устройство `C:`). Так как функциональность выхода из режима гибернации работает ина-

че, если на компьютере включены возможности расширения физических адресов[1] и отладчика, эти возможности отслеживаются посредством параметров `pae` и `debugoptionenabled`.

- **Проверка памяти Windows** (Windows Memory Tester). Эта запись содержит данные текущей конфигурации для проверки памяти Windows. Проверку памяти осуществляет предоперационная утилита memtest.exe. Так как эта утилита определяет проблемную память по умолчанию, параметру `badmemoryaccess` по умолчанию присвоено значение `Yes`. Эту возможность можно отключить, выполнив команду `bcdedit/set {memdiag} badmemoryaccess NO`. Для проверки памяти можно задать количество проходов с помощью параметра редактора BCD `passcount` и набор тестов как `basic` (базовый) или `extended` (расширенный) с помощью параметра `testmix`. Например, следующая команда задает два прохода проверки памяти и базовый тестовый набор `basic`:

  ```
  bcdedit/set {memdiag} passcount 2 textmix basic
  ```

- **Загрузка наследованной Windows** (Windows Legacy OS Loader). Эта запись содержит данные текущей конфигурации для загрузки версий Windows, более ранних, чем Windows Vista. В параметре *`device`* задается раздел, который следует использовать по умолчанию (например, `C:`), а в параметре *`path`* — путь по умолчанию к приложению загрузчика (например, `Ntldr`).

- **Параметры EMS** (EMS Settings). Эта запись содержит данные конфигурации, которая применяется при загрузке с использованием служб EMS. Включение служб EMS определяется индивидуально для каждой отдельной записи загрузчика Windows. Если службы EMS предоставляются посредством BIOS и нужно использовать параметры BIOS, это можно сделать, выполнив команду `bcdedit /emssettings bios`. Для служб EMS также можно задать EMS-порт и скорость передачи в бодах. Например, следующая команда задает EMS-порт `2` и скорость передачи `115200`:

  ```
  bcdedit /emssettings EMSPORT:2 EMSBAUDRATE:115200
  ```

  С целью включения и отключения служб EMS для приложения загрузки используется команда редактора BCD `/bootems` с указанием загрузочного приложения с требуемым состоянием (`On` или `Off`). Например, следующая команда включает службы аварийного управления для диспетчера загрузки:

  ```
  bcdedit /bootems {bootmgr} ON
  ```

- **Параметры отладчика** (Debugger Settings). Эта запись содержит данные конфигурации, которая применяется при загрузке с включенным отладчиком. Включение отладчика определяется индивидуально для каждой отдельной записи загрузчика Windows. Просмотреть параметры отладчика гипервизора можно, выполнив команду `bcdedit /dbgsettings`. Для задания параметров отладки также применяется команда `/dbgsettings`. В частности, посредством параметра *`debugtype`* (тип отладки) этой команды можно установить тип отладчика как `serial`, `1394` или `USB`. Для отладки типа `serial` в параметре *`debugport`* задается последовательный порт для отладчика, а в параметре *`baudrate`* — скорость передачи для отладки в бодах. Для отладки типа `1394` в параметре *`channel`* задается канал отладки. Для отладки типа `USB` имя целевого устройства USB для отладки указывается в параметре *`targetname`*. Для отладки любого типа наличие флага `/noumex` означает, что исключения пользовательского режима следует игнорировать. Далее приводится несколько примеров задания типа отладки и соответствующих параметров:

[1] Physical Address Extension — PAE.

```
bcdedit /dbgsettings SERIAL DEBUGPORT:1 BAUDRATE:115200
bcdedit /dbgsettings 1394 CHANNEL:23
bcdedit/dbgsettings USB TARGETNAME:DEBUGGING
```

- **Параметры гипервизора** (Hypervisor Settings). Эта запись содержит данные конфигурации, которая применяется при работе с гипервизором с включенным отладчиком. Включение отладчика определяется индивидуально для каждой отдельной записи загрузчика Windows. Просмотреть и задать параметры отладчика гипервизора можно с помощью команды `bcdedit /hypervisorsettings`. В параметре *`debugtype`* этой команды задается тип отладчика, в параметре *`debugport`* — последовательный порт для отладчика, а в параметре *`baudrate`* — скорость передачи в бодах. Параметры для команды `hypervisorsettings` задаются так же, как и параметры для команды `/dbgsettings`. Например, следующая команда задает последовательный тип отладки, порт `2` и скорость передачи в бодах `115200`:

  ```
  bcdedit /hypervisorsettings SERIAL DEBUGPORT:1 BAUDRATE:115200
  ```

  А в следующем примере задается тип отладки `1394` на канале `23`:

  ```
  bcdedit /hypervisorsettings 1394 CHANNEL:23
  ```

В табл. 4.6 приводятся основные параметры записей приложений загрузки. Так как диспетчер загрузки Windows, средства проверки памяти Windows, загрузчик Windows и загрузчик возобновления Windows являются приложениями загрузки, эти параметры применимы ко всем этим приложениям.

Таблица 4.6. *Основные параметры записей загрузочных приложений*

Параметр	Описание
`BadMemoryAccess`	Включает и отключает возможность использования приложением памяти, внесенной в список неисправных страниц памяти
`BadMemoryList`	Целочисленный список номеров страниц неисправной системной памяти
`BaudRate`	Целочисленное значение, которое определяет скорость передачи в бодах для последовательного отладчика
`BootDebug`	Булево значение, которое включает или отключает отладчик загрузчика
`BootEMS`	Булево значение, которое включает или отключает службы EMS
`Channel`	Целочисленное значение, которое определяет канал для отладчика типа 1394
`ConfigAccessPolicy`	Задает политику доступа как `DEFAULT` или `DISALLOWMMCONFIG`
`DebugAddress`	Целочисленное значение, которое определяет адрес порта для последовательного отладчика
`DebugPort`	Целочисленное значение, которое определяет номер порта для последовательного отладчика
`DebugStart`	Задает тип запуска отладчика: `ACTIVE`, `AUTOENABLE` или `DISABLE`
`DebugType`	Задает тип отладчика: `SERIAL`, `1394` или `USB`
`EMSBaudRate`	Задает скорость передачи в бодах для служб EMS
`EMSPort`	Задает номер последовательного порта для служб EMS
`FirstMegaBytePolicy`	Задает тип политики первого мегабайта: `USENONE`, `USEALL` или `USEPRIVATE`
`GraphicsModeDisabled`	Булево значение, которое включает или отключает графический режим
`GraphicsResolution`	Задает разрешение графики, например 1024×768 или 800×600

Таблица 4.6 *(окончание)*

Параметр	Описание
`Locale`	Задает местонахождение загрузочного приложения
`Noumex`	Булево значение, задающее игнорирование (когда равно `TRUE`) или учет (когда равно `FALSE`) исключений пользовательского режима
`NoVESA`	Булево значение, которое включает или отключает видеорежим VESA[1]
`RecoveryEnabled`	Булево значение, которое включает или отключает использование последовательности восстановления
`RecoverySequence`	Задает последовательность восстановления
`TargetName`	Задает строковое значение целевого имени для USB-отладчика
`TestSigning`	Булево значение, включающее или отключающее использование сертификатов подписи предварительного тестового кода
`TruncateMemory`	Задает игнорирование памяти, расположенной по указанному физическому адресу и выше

В табл. 4.7 представлены основные параметры записей приложений загрузчика Windows (`Osloader`).

Таблица 4.7. *Основные параметры записей приложений загрузчика Windows*

Параметр	Описание
`AdvancedOptions`	Булево значение, которое включает или отключает дополнительные параметры
`BootLog`	Булево значение, которое включает или отключает журнал инициализации загрузки
`BootStatusPolicy`	Задает политику состояния загрузки как `DisplayAllFailures`, `IgnoreAllFailures`, `IgnoreShutdownFailures` или `IgnoreBootFailures`
`ClusterModeAddressing`	Задает максимальное количество процессоров в одном кластере APIC2
`ConfigFlags`	Задает флаги конфигурации, специфические для процессора
`DbgTransport`	Задает имя файла для транспорта частного отладчика
`Debug`	Булево значение, которое включает или отключает отладку ядра
`DriverLoadFailurePolicy`	Задает политику сбоя загрузки драйвера как `Fatal` или `UseErrorControl`
`Ems`	Булево значение, которое включает или отключает службы EMS ядра
`Hal`	Задает имя файла для частного уровня HAL
`HalBreakPoint`	Булево значение, включающее или отключающее специальную точку прерывания уровня HAL
`HypervisorLaunchType`	Задает тип запуск гипервизора как `Off` или `Auto`

[1] Video Electronics Standards Association — ассоциация по стандартам в области видеоэлектроники.

[2] Advanced Programmable Interrupt Controller — усовершенствованный программируемый контроллер прерываний.

Таблица 4.7 *(продолжение)*

Параметр	Описание
IncreaseUserVA	Целочисленное значение, увеличивающее размер виртуального адресного пространства (в мегабайтах), которое могут использовать процессы пользовательского режима
Kernel	Задает имя файла для частного ядра
LastKnownGood	Булево значение, включающее или отключающее загрузку последней удачной конфигурации
MaxProc	Булево значение, включающее или отключающее отображение максимального количества процессоров в системе
Msi	Задает прерывание MSI[1] для применения как Default или ForceDisable
NoCrashAutoReboot	Булево значение, включающее или отключающее **Выполнять автоматическую перезагрузку после сбоя**
NoLowMem	Булево значение, включающее или отключающее использование нижней памяти
NumProc	Задает количество процессоров для использования при запуске
nx	Задает режим защиты No Execute (NX) как OptIn, OptOut, AlwaysOn или AlwaysOff
OneCPU	Булево значение, задающее использование только процессора загрузки
OptionsEdit	Булево значение, включающее или отключающее редактор параметров
OSDevice	Задает устройства, содержащее корневой каталог системы
Pae	Задает возможность PAE[2] как Default, ForceEnable или ForceDisable
PerfMem	Задает размер в байтах буфера для протоколирования данных производительности
RemoveMemory	Задает объем в мегабайтах памяти, удаляемой из общего объема памяти, доступного операционной системе
RestrictAPICCluster	Задает наибольший номер кластера APIC для использования системой
ResumeObject	Задает идентификатор для объекта возобновления, который связан с данным объектом операционной системы
SafeBoot	Задает тип запуска в безопасном режиме как Minimal, Network или DsRepair
SafeBootAlternateShell	Булево значение, включающее или отключающее использование альтернативной оболочки при загрузке в безопасном режиме
Sos	Булево значение, включающее или отключающее вывод дополнительной информации о загрузке
SystemRoot	Задает путь к корневому каталогу системы
UseFirmwarePCISettings	Булево значение, включающее или отключающее периферийные устройства (PCI), настроенные в BIOS

[1] Message signaled interrupt — прерывание, инициируемое сообщением.

[2] Physical address extension — расширение физических адресов.

Таблица 4.7 *(окончание)*

Параметр	Описание
UsePhysicalDestination	Булево значение, задающее принудительное использование физического контроллера APIC
Vga	Булево значение, задающее принудительное использование видео дисплея VGA
WinPE	Булево значение, задающее загрузку в предустановочную среду Windows PE

Редактирование параметров предотвращения выполнения данных и расширения физических адресов

Возможность предотвращения выполнения данных DEP представляет собой функциональность защиты памяти. При задействовании этой функциональности процессор помечает все адреса памяти приложения, как неисполняемые, если только данный адрес явно не содержит исполняемый код. При попытке исполнения кода на странице памяти, помеченной как неисполняемая, процессор порождает исключение, не допуская исполнения этого кода. Таким образом предотвращается внедрение кода вредоносных приложений, таких как вирусы, в большинство областей памяти.

Для компьютеров, оснащенных процессорами, которые поддерживают возможность NX, операционную систему можно настроить на выборочное использование или неиспользование защиты, предоставляемой этой функциональностью, присвоив параметру `nx` значение `OptIn` или `OptOut` соответственно. Например, следующая команда задает выборочное неиспользование возможности NX:

```
bcdedit /set {current} nx optout
```

Когда параметру `nx` присвоено значение `OptIn`, возможность DEP включена только для основных программ и служб Windows. Это поведение по умолчанию. Когда же параметру `nx` присвоено значение `OptOut`, все программы и службы, а не только основные программы и службы Windows, используют возможность DEP. Программы, для которых не требуется использовать эту возможность, должны быть явно исключены (opted out) из области ее применения *(см. разд. "Настройка предотвращения выполнения данных" главы 2)*. Защиту NX также можно настроить на постоянное включение или отключение, используя аргументы `alwayson` и `alwaysoff` соответственно. Например:

```
bcdedit /set {current} nx alwayson
```

Процессоры, поддерживающие возможность NX, должны работать в режиме расширения физических адресов (PAE). Режим PAE можно настроить, присвоив параметру `PAE` значение `default`, `forceenable` или `forcedisable`. Когда параметр `PAE` имеет значение `default`, операционная система использует конфигурацию PAE по умолчанию. Когда этот параметр имеет значение `forceenable`, операционная система использует возможность PAE, а когда `forcedisable` — не использует. Например, следующая команда задает использование по умолчанию возможности PAE:

```
bcdedit /set {current} pae default
```

Редактирование порядка отображения операционных систем в списке загрузки

Порядок отображения операционных систем в меню загрузки на компьютере с несколькими операционными системами можно изменить с помощью команды редактора BCD `/displayorder`. Синтаксис этой команды следующий:

```
bcdedit /displayorder id1 id2 ... idn
```

где параметр *id1* обозначает идентификатор первой операционной системы в меню, *id2* — идентификатор второй, и т. д. Например, следующий порядок отображения операционных систем в меню выбора загрузки:

```
Windows Boot Loader
--------------------
identifier              {16b857b4-9e02-11eO-9c17-b7d085eb0682}

Windows Boot Loader
-------------------
identifier              {14504de-e96b-11cd-a51b-89ace9305d5e}

Windows Boot Loader
-------------------
identifier              {8b78e48f-02dO-11dd-af92-a72494804a8a}
```

можно изменить, выполнив команду `/displayorder`:

```
bcdedit /displayorder {8b78e48f-02d0-11dd-af92-a72494804a8a}
{16b857b4-9e02-11e0-9c17-b7d085eb0682}
{14504de-e96b-11cd-a51b-89ace9305d5e}
```

А установить определенную операционную систему первой в меню можно посредством использования с командой `/displayorder` параметра `/addfirst`, как показано в следующем примере:

```
bcdedit /displayorder {16b857b4-9e02-11e0-9c17-b7d085eb0682} /addfirst
```

Подобным образом установить определенную операционную систему последней в меню можно посредством использования с командой `/displayorder` параметра `/addlast`, как показано в следующем примере:

```
bcdedit /displayorder {8b78e48f-02d0-11dd-af92-a72494804a8a} /addlast
```

Изменение операционной системы, загружаемой по умолчанию

Изменить операционную систему, загружаемую по умолчанию, можно с помощью команды редактора BCD `/default`. Синтаксис этой команды следующий:

```
bcdedit /default id
```

где параметр *id* обозначает идентификатор операционной системы в записи загрузчика. Например, операционную систему следующей записи хранилища BCD:

```
Windows Boot Loader
-------------------
identifier      {16b857b4-9e02-11e0-9c17-b7d085eb0682}
```

можно установить загружаемой по умолчанию, выполнив такую команду `/displayorder`:

```
bcdedit /default {16b857b4-9e02-11e0-9c17-b7d085eb0682}
```

Чтобы установить операционную систему, предшествующую Windows 8, в качестве загружаемой по умолчанию, с командой `/default` нужно использовать идентификатор этой операционной системы. Например, чтобы установить операционную систему, загружаемую по умолчанию, из следующей записи хранилища BCD:

```
Windows Legacy OS Loader
------------------------
identifier              {466f5a88-0af2-4f76-9038-095b170dc21c}
device                  partition=C:
path                    \ntldr
description             Earlier Microsoft Windows Operating System
```

нужно выполнить команду:

```
bcdedit /default {466f5a88-0af2-4f76-9038-095b170dc21c}
```

Редактирования периода тайм-аута

Изменить период тайм-аута для загрузки операционной системы по умолчанию можно с помощью команды редактора BCD `/timeout` следующим образом:

```
bcdedit /timeout nn
```

где параметр *nn* обозначает период тайм-аута в секундах.

Чтобы немедленно загружать операционную систему по умолчанию (т. е. без предоставления выбора загрузки других установленных на компьютере операционных систем), период тайм-аута нужно установить равным 0 секунд.

Одноразовое изменение порядка загрузки

Иногда требуется однократно изменить порядок загрузки с последующим восстановлением порядка загрузки по умолчанию. Для этого применяется команда `/bootsequence`, принимающая в качестве параметра идентификатор операционной системы, которую следует загрузить после перезапуска компьютера. Например:

```
bcdedit /bootsequence {16b857b4-9e02-11e0-9c17-b7d085eb0682}
```

Указанная операционная система будет загружена по умолчанию только после первой перезагрузки компьютера, а дальше будет восстановлен исходный порядок загрузки операционных систем.

ГЛАВА 5

Настройка политик пользователей и компьютеров

Групповая политика — это набор правил, применение которых может облегчить управление пользователями и компьютерами. В Windows 8 групповая политика содержит как управляемые параметры, называющиеся *параметрами политики* (policy settings), так и неуправляемые политики, называющиеся *предпочтениями политики* (policy preferences). Параметры политики позволяют управлять конфигурацией операционной системы и ее компонентами, а предпочтения политики — настраивать, применять и управлять параметрами операционной системы и приложений. Ключевая разница между параметрами и предпочтениями состоит в принуждении. Параметры групповой политики являются предметом строгого принуждения, в то время как предпочтения таковым не являются.

В этой главе рассматривается применение параметров политик. Использование предпочтений политик обсуждается в следующей главе.

Основы групповых политик

Параметры групповой политики применяются для управления конфигурацией операционной системы, а также для отключения опций и элементов управления пользовательского интерфейса для параметров, управляемых групповой политикой. Большинство параметров групповой политики хранятся в разделах реестра, связанных с групповыми политиками. Операционная система и соответствующие приложения исследуют эти разделы.

Существуют два типа групповых политик: локальные групповые политики и групповые политики службы каталогов Active Directory. Локальная групповая политика используется для управления параметрами локальной машины, а групповая политика службы каталогов Active Directory — для управления параметрами компьютеров сайтов, доменов и организационных единиц (OE). Групповая политика упрощает администрирование, предоставляя администраторам централизованный контроль над привилегиями, правами и возможностями пользователей и компьютеров. Тщательное управление политиками имеет существенное значение для надлежащей работы. Параметры политик можно разбить на две общие категории: политики, применяемые к компьютерам, и политики, применяемые к пользователям. Политики компьютеров обычно применяются при загрузке операционной системы, а политики пользователей — при входе пользователей в систему.

В процессе загрузки и входа политики применяются в строго определенном порядке, о чем важно помнить при диагностировании проблем с системой. При наличии нескольких политик они применяются в следующем порядке:

1. Локальные политики.
2. Политики сайтов.
3. Политики доменов.
4. Политики организационных единиц.
5. Политики дочерних организационных единиц.

По умолчанию, в случае конфликта параметров политик, старшинство имеют параметры, применяемые позже, которые замещают предыдущие параметры. Например, политики организационных единиц превосходят политики доменов. Как и следовало ожидать, это правило старшинства политик имеет исключения, которые позволяют администраторами блокировать, контролировать и отключать политики.

Служба **Клиент групповой политики** изолирует извещения и обработку групповой политики от процесса входа в систему Windows. Это уменьшает объем ресурсов, используемых для обработки политики в фоновом режиме, повышает общую производительность, а также обеспечивает доставку и применение новых файлов групповой политики как часть процесса обновления, не требуя для этого перезапуска. Используя службу сведений о подключенных сетях (Network Location Awareness), клиент групповой политики может определить состояние компьютера и сети, а также доступную пропускную способность сети для обнаружения медленных линий связи. В результате клиент групповой политики лучше понимает, как работает операционная среда, и может лучше определять, какие политики применять и когда.

Сообщения событий групповой политики записываются в журнал **Система** компьютера. Кроме этого, имеется несколько опций для диагностирования неполадок. Можно использовать подробные сообщения событий в рабочем журнале. В средстве **Просмотр событий** можно выполнить просмотр операционного журнала, последовательно развернув узлы **Журналы приложений и служб\Microsoft\Windows\Group Policy\Operational**. А посредством утилиты командной строки Gpupdate.exe можно обновить параметры политик до самых последних значений. Хотя обычно эта утилита исполняется на диагностируемом компьютере, Windows Server 2012 позволяет запланировать ее исполнение для обновления групповых политик на удаленных компьютерах. Дополнительную информацию *см. в главе 4, "Automating Tasks, Policies, and Procedures"* книги "Windows Server2012 Pocket Consultant"[1].

Доступ к локальным групповым политикам и их использование

Локальные групповые политики применяются ко всем пользователям и администраторам, входящим в систему на компьютере, который является членом рабочей группы, а также ко всем пользователям и администраторам, выполняющим локальный вход в систему на компьютере, который является членом домена.

Как и в случае с Windows 7, компьютеры под управлением Windows 8 могут иметь один или больше объектов локальной политики, связанных с ними. Управление локальной групповой политикой осуществляется посредством объекта групповой политики (ОГП — GPO, Group Policy Object). Объект локальной групповой политики хранится на каждом компьютере в скрытой папке *%SystemRoot%*\System32\GroupPolicy. Дополнительные пользовательские и групповые объекты локальной групповой политики хранятся в папке *%SystemRoot%*\System32\GroupPolicyUsers.

[1] William R. Stanek. Windows Server 2012 Pocket Consultant. — Microsoft Press, 2012.

При использовании компьютеров в автономной, в отличие от доменной, конфигурации, наличие нескольких объектов локальной групповой политики может оказаться полезным. В частности, для администраторов можно создать один объект локальной групповой политики, а для не администраторов — другой, и больше не нужно будет явно включать и отключать параметры, создающие трудности в управлении компьютером, при выполнении заданий администрирования. Но в доменной конфигурации использование нескольких объектов локальной групповой политики может быть нежелательным. В доменах к большинству компьютеров и пользователей уже применяется несколько объектов групповой политики, и добавление нескольких объектов локальной групповой политики к этому разнообразию может внести путаницу в управление групповыми политиками.

Операционная система Windows 8 предоставляет три уровня объектов локальной групповой политики.

- **Локальная групповая политика** (Local Group Policy). Она является единственным объектом групповой политики, который позволяет применять конфигурационные параметры как компьютера, так и пользователя ко всем пользователям компьютера.
- **Административная и неадминистративная локальная групповая политика** (Administrators and Non-Administrators local Group Policy). Эта групповая политика содержит только конфигурационные параметры пользователя и применяется в зависимости от того, является ли используемая учетная запись пользователя членом локальной группы **Администраторы**.
- **Пользовательская локальная групповая политика** (User-specific local Group Policy). Эта групповая политика содержит только конфигурационные параметры пользователя и применяется к отдельным пользователям и группам.

Эту уровни объектов локальных групповых политик обрабатываются в перечисленном выше порядке.

Так как доступные параметры узла **Конфигурация пользователя** одинаковые для всех объектов локальной групповой политики, значение в одном объекте групповой политики может конфликтовать с соответствующим значением в другом объекте групповой политики. Операционная система Windows разрешает такие конфликты, заменяя любое предыдущее значение последним считанным и наиболее актуальным значением. Это последнее значение и используется Windows 8. В процессе разрешения конфликтов значение имеет только состояние включения параметров. Параметр в состоянии **Не задана** (Not Configured) не влияет на состояние параметра из предыдущего применения политики. Чтобы упростить администрирование домена, можно отключить обработку объектов локальных групповых политик на компьютерах под управлением Windows 8, включив параметр **Отключить обработку объектов локальной групповой политики** (Turn off local group policy objects processing) в объекте групповой политики домена. Доступ к этому параметру можно получить, развернув последовательно узлы объекта групповой политики **Конфигурация компьютера\Административные шаблоны\Система\Групповая политика** (Computer Configuration\Administrative Templates\System\Group Policy).

> ***Примечание***
>
> Включенные объекты локальных групповых политик всегда обрабатываются. Но они имеют низший приоритет. Это означает, что их параметры могут заменяться параметрами сайта, домена или организационной единицы.

По умолчанию на компьютере существует единственный объект локальной политики — объект локальной групповой политики. С помощью редактора объектов группой политики можно создавать и управлять другими объектами локальной политики. Так как локальная

групповая политика является подмножеством групповой политики, на локальном уровне недоступны многие возможности, которые доступны на уровне доменов. Прежде всего, нельзя управлять предпочтениями политики. Управлять можно только подмножеством параметров политики. Кроме этих основных различий, управление локальной групповой политикой и групповой политикой службы каталогов Active Directory осуществляется во многом однотипно.

Чтобы работать с объектами локальной групповой политики, необходимо войти в систему с учетной записью администратора. Быстрее всего открыть объект локальной групповой политики верхнего уровня на локальном компьютере можно путем выполнения в поле поиска панели **Приложения** или в командной строке следующей команды:

```
gpedit.msc /gpcomputer: "%Имя_Компьютера%"
```

Эта команда запускает консоль MMC[1], добавляет в нее оснастку редактора объектов групповой политики и открывает в ней локальный компьютер для редактирования в качестве объекта групповой политики.

Открыть локальный объект групповой политики для редактирования можно также следующим образом:

1. Запустите консоль MMC. Это можно сделать, выполнив команду `mmc.exe` в поле поиска панели **Приложения** или в командной строке.
2. В консоли управления выберите меню **Файл**, а в нем команду **Добавить или удалить оснастку** (Add/Remove Snap-in).
3. В открывшемся диалоговом окне **Добавление и удаление оснасток** (Add or Remove Snap-ins) выберите опцию **Редактор объектов групповой политики** (Group Policy Object Editor), а затем нажмите кнопку **Добавить** (Add), расположенную между панелями.
4. В следующем диалоговом окне, **Выбор объекта групповой политики** (Select Group Policy Object), поле **Объект групповой политики** уже содержит требуемый объект — локальный компьютер, поэтому просто нажмите кнопку **Готово** (Finish). Нажмите кнопку **OK**, чтобы сохранить настройки.

Из рис. 5.1 видно, что теперь можно управлять локальной групповой политикой посредством предоставляемых параметров[2]. Так как локальная групповая политика не имеет предпочтений политики, узлы **Конфигурация компьютера** и **Конфигурация пользователя** не содержат отдельных подузлов **Политики** и **Настройка**[3] (Preferences).

В консоли MMC можно создавать и управлять другими объектами локальной политики. Для создания или доступа к другим объектам локальной групповой политики применяется следующая процедура:

1. В консоли управления выберите меню **Файл**, а в нем команду **Добавить или удалить оснастку** (Add/Remove Snap-In).
2. В открывшемся диалоговом окне **Добавление и удаление оснасток** (Add or Remove Snap-ins) выберите опцию **Редактор объектов групповой политики** (group Policy

---

[1] Microsoft Management Console — консоль управления (MMC).

[2] В локализации элементов окна допущена ошибка. Первая колонка правой панели должна называться не **Состояние**, а **Параметр** (Setting).

[3] Локализация узла **Preferences** как **Настройка**, возможно, не совсем удачная. Этот узел доступен в редакторе управления групповыми политиками (Group Policy Management Editor), который применяется для управления политиками компьютеров, членов доменов.

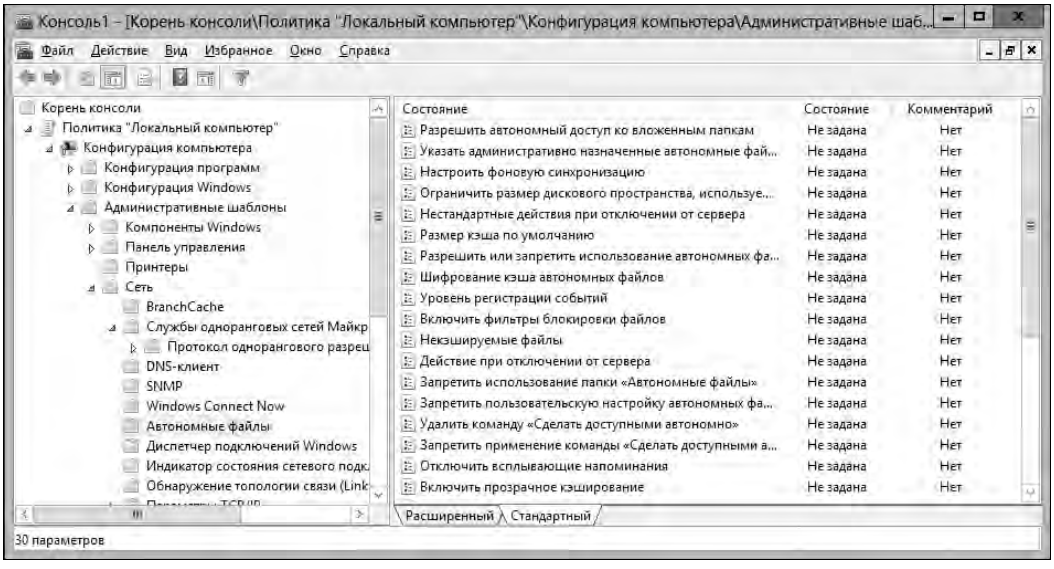


Рис. 5.1. Управление объектом локальной групповой политики в консоли MMC

Object Editor), а затем нажмите кнопку **Добавить** (Add), расположенную между панелями.

3. В диалоговом окне **Выбор объекта групповой политики** нажмите кнопку **Обзор**. В диалоговом окне **Поиск объекта групповой политики** (Browse for a Group Policy Object) перейдите на вкладку **Пользователи** (Users) (рис. 5.2).

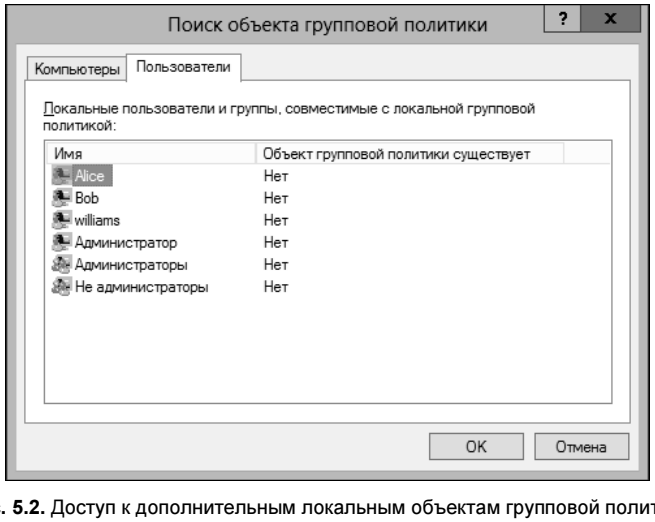


Рис. 5.2. Доступ к дополнительным локальным объектам групповой политики

4. В столбце **Объект групповой политики существует** (Group Policy Object Exists) укажите, существует ли определенный объект локальной групповой политики.

   Далее выполните одно из следующих действий.

   - Выберите имя **Администраторы**, чтобы создать объект локальной групповой политики **Администраторы** или получить доступ к нему. Нужно выбрать именно множе-

ственную форму **Администраторы** (Administrators), а не единственную **Администратор** (Administrator), чтобы обеспечить применение политики ко всем локальным администраторам.

- Выберите имя **Не администраторы** (Non-Administrators), чтобы создать объект локальной групповой политики **Не администраторы** или получить доступ к нему.
- Выберите локального пользователя, для которого нужно получить доступ к пользовательскому объекту локальной политики или создать такой объект.

5. Нажмите кнопку **OK**, чтобы сохранить настройки. Нажмите **Готово**, а затем снова **OK**. Если указанный объект еще не существует, он будет создан; в противном случае объект будет открыт для просмотра и редактирования.

Доступ к политикам сайтов, доменов и организационных единиц и их использование

В случае групповых политик службы каталогов Active Directory каждый сайт, домен или организационная единица может иметь одну или больше групповых политик.

Для работы с объектами групповой политики в службе каталогов Active Directory применяется консоль GPMC[1].

Чтобы работать с объектами групповой политики, необходимо обладать правами администратора.

На компьютерах под управлением серверной версии Windows консоль GPMC предоставляется, как часть штатной установки. А на компьютерах с установленной настольной версией Windows консоль GPMC входит в состав средств RSAT[2]. Установочный пакет RSAT для Windows 8 можно загрузить в центре загрузок корпорации Microsoft (**http://download.microsoft.com**).

Установив средства RSAT, консоль GPMC можно запускать с диспетчера серверов, выбрав меню **Средства** (Tools), а затем команду **Управление групповой политикой** (Group Policy Management).

Как показано на рис. 5.3, левая панель консоли GPMC по умолчанию содержит два узла высшего уровня — **Управление групповой политикой** (Group Policy Management) и **Лес** (Forest). (Узел **Лес** представляет собой лес, к которому в данный момент подключен компьютер и который называется согласно домену корня данного леса.)

Узел **Лес** содержит следующие вложенные узлы.

- **Домены** (Domains). Предоставляет доступ к параметрам политики для доменов данного леса. По умолчанию подключение выполняется к домену входа в систему, после чего можно добавить подключения к другим доменам. Домен содержит объект групповой политики **Default Domain Policy**, организационную единицу **Domain Controllers** (и связанный объект групповой политики **Default Domain Controllers Policy**) и объекты групповой политики, определенные в домене.
- **Сайты** (Sites) содержит параметры политики для сайтов связанного леса. Узел **Сайты** свернут по умолчанию.
- **Моделирование групповой политики** (Group Policy Modeling). Предоставляет доступ к мастеру моделирования групповой политики (Group Policy Modeling Wizard), с по-

[1] Group Policy Management Console — консоль управления групповой политикой.

[2] Remote Server Administration Tools — средства удаленного администрирования сервера.

мощью которого можно планировать развертывание политики и эмулировать параметры для тестирования. Также здесь доступны все сохраненные модели политик.

- **Результаты групповой политики** (Group Policy Results). Предоставляет доступ к мастеру результатов групповой политики (Group Policy Results Wizard), который позволяет работать с одного места со всеми связанными объектами групповой политики и организационными единицами каждого подключенного домена.

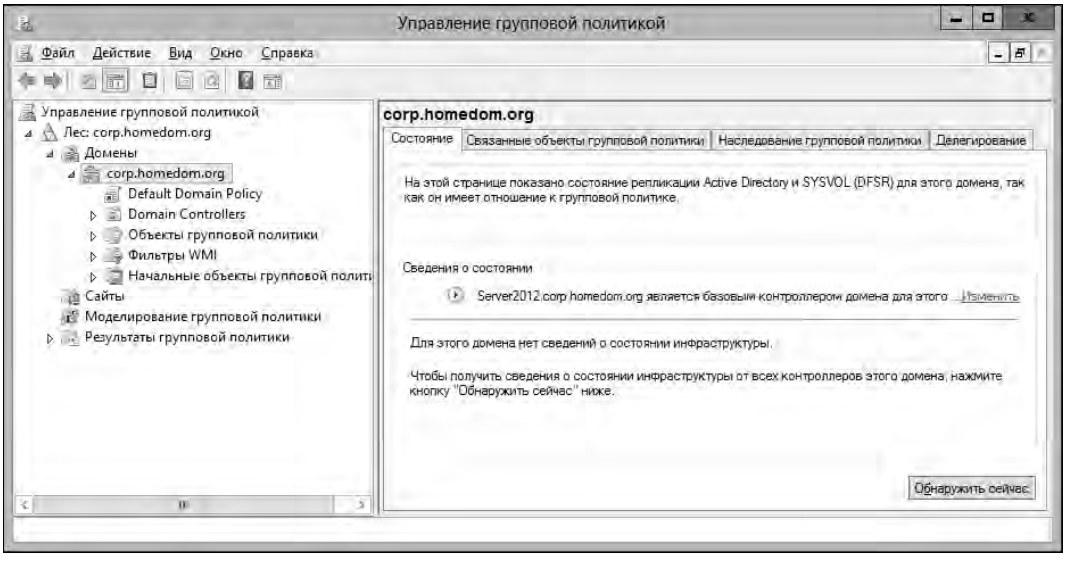


Рис. 5.3. Консоль GPMC для управления объектами групповой политики доменов, сайтов и организационных единиц

Объекты групповой политики, находящиеся в контейнерах доменов, сайтов и организационных единиц консоли GPMC, в действительности являются ссылками на объекты групповой политики, а не самими объектами. Настоящие объекты групповой политики находятся в контейнере **Объекты групповой политики** (Group Policy Objects) выбранного домена. Обратите внимание, что подобно значкам ярлыков, значки ссылок объектов групповой политики обозначены маленькой стрелкой в левом нижнем углу. Объект групповой политики можно открыть для редактирования, щелкнув его правой кнопкой мыши и выбрав в контекстном меню команду **Изменить** (Edit).

Откроется редактор управления групповыми политиками, в котором можно просматривать или редактировать данную групповую политику (рис. 5.4).

Групповая политика содержит два основных узла.

- **Конфигурация компьютера** (Computer Configuration). Этот узел позволяет задавать политики для применения к компьютерам, независимо от вошедших в систему пользователей.
- **Конфигурация пользователя** (User Configuration). Этот узел позволяет задавать политики для применения к пользователям, независимо от того, на какой компьютер они войдут.

Примечание

Имейте в виду, что параметры конфигурации пользователя, задаваемые посредством объектов локальных политик, применимы только к компьютерам, на которых была выполнена настройка

этих параметров. Чтобы применить параметры ко всем компьютерам, на которые может войти пользователь, нужно использовать групповые политики доменов, сайтов или организационных единиц.

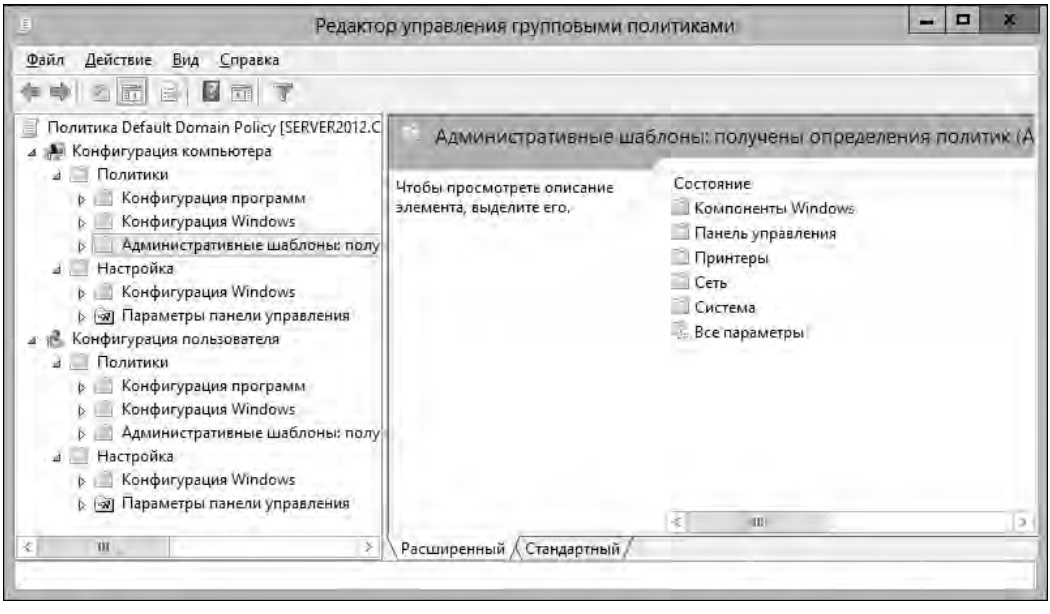


Рис. 5.4. Параметры групповой политики зависят от типа создаваемой политики и установленных подключаемых модулей

Узлы **Конфигурация компьютера** и **Конфигурация пользователя** содержат подузлы **Политики** и **Настройка** (Preferences). Для работы с параметрами политики используется узел **Политики**. Доступные в этом узле параметры групповой политики зависят от типа создаваемой политики и установленных подключаемых модулей. Обычно подузел **Политики** обоих узлов будет содержать следующие вложенные узлы.

- **Конфигурация программ** (Software Settings). Содержит политики для установки и конфигурирования программ. При установке программ в этот узел могут вставляться дополнительные подузлы.
- **Конфигурация Windows** (Windows Settings). Содержит политики для перенаправления папок, сценариев и безопасности.
- **Административные шаблоны** (Administrative Templates). Содержит политики для операционной системы, ее компонентов и программ. Эти политики, которые рассматриваются далее в этой главе, применяются специфически к пользователям и компьютерам.

Настройка политик

Для управления пользователями и компьютерами необходимо настроить политики административных шаблонов. Эти политики предоставляют удобный доступ к параметрам политики на основе реестра, которые управляют операционной системой, ее компонентами и программами. В то время как для хранения параметров настройки на основе реестра более ранние версии Windows, которые поддерживают групповые политики, используют файлы

административных шаблонов (AMD) с проприетарным языком разметки, Windows 8 использует для этой цели стандартный файловый формат XML, называющийся ADMX. В отличие от файлов ADM, которые хранятся в объекте групповой политики, к которому они относятся, файлы ADMX находятся в центральном хранилище. В доменах хранение файлов ADMX в центральном хранилище облегчает работу и управление ими.

Просмотр политик и шаблонов

Текущие настроенные шаблоны можно просматривать в узле **Административные шаблоны** редактора управления групповыми политиками. Этот узел содержит политики, которые можно настраивать для локальных систем, организационных единиц и сайтов (рис. 5.5).

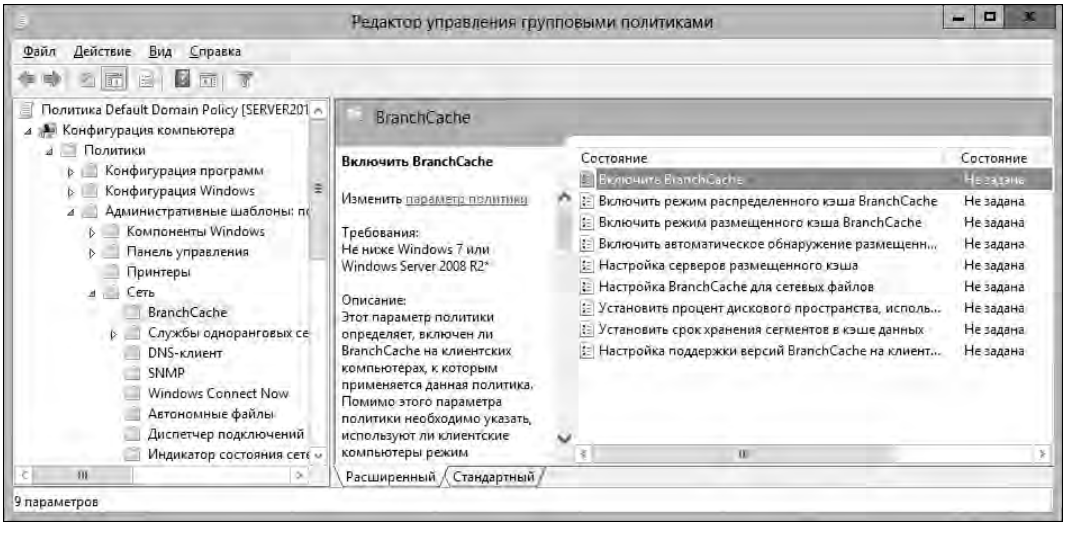


Рис. 5.5. Пример содержимого узла **Административные шаблоны** редактора управления групповыми политиками

Узлы **Конфигурация компьютера** и **Конфигурация пользователя** содержат разные наборы шаблонов. Шаблоны новых политик можно добавлять вручную посредством консоли GPMC или при установке новых компонентов Windows.

Любые изменения, вносимые в политики, доступные через административные шаблоны, сохраняются в реестре. Настройки компьютера сохраняются в разделе реестра `HKEY_LOCAL_MACHINE`, а настройки пользователя — в разделе `HKEY_USER`. Лучшим подходом к изучению доступных политик административных шаблонов будет их просмотр в узле **Административные шаблоны** редактора управления групповыми политиками. При просмотре этих шаблонов можно видеть, что параметры политики находятся в одном из следующих трех состояний:

- **Не задана** (Not Configured) — такой параметр политики не используется и не влияет на существующую конфигурацию компьютера;
- **Включена** (Enabled) — параметр политик сохранен в реестре;
- **Отключена** (Disabled) — параметр отключен на всех клиентских компьютерах, где применяется данная политика, т. к. он может, например, конфликтовать с другими включенными параметрами. Значение такого параметра сохраняется в реестре.

Включение, отключение и настройка параметров политик

В редакторе управления групповыми политиками политики административных шаблонов имеются как в узле **Конфигурация компьютера**, так и в узле **Конфигурация пользователя**. В большинстве случаев политики из этих узлов не пересекаются и не конфликтуют друг с другом. Но в случае конфликта политики компьютера имеют старшинство, что означает, что применяется политика компьютера. Наиболее часто применяемые политики и работа с ними подробно рассматриваются далее в этой главе.

Чтобы работать с политиками, нужно открыть требуемый сайт, домен или организационную единицу в редакторе управления групповыми политиками. Это можно сделать, выполнив следующую процедуру:

1. В консоли GPMC разверните требуемый узел леса, а в нем узел **Домены**.
2. Далее разверните узел требуемого домена, а затем узел **Объекты групповой политики** этого домена.
3. Щелкните правой кнопкой мыши на объекте групповой политики и в контекстном меню выберите команду **Изменить** (Edit). Откроется редактор управления групповыми политиками, содержащий выбранный объект групповой политики.

Теперь параметры этого объекта политики можно включать, отключать и настраивать следующим образом:

1. Разверните узел **Административные шаблоны** в узле **Конфигурация компьютера** или **Конфигурация пользователя** (в зависимости от того, какой тип политики требуется настроить).
2. В левой панели выберите вложенную папку политики, которую требуется настроить. Содержащиеся в этой папке параметры политики отобразятся в правой панели редактора.
3. Откройте окно свойств требуемого параметра политики, выполнив по нему двойной щелчок мышью. (Это также можно сделать, щелкнув на требуемом параметре правой кнопкой мыши и выбрав в контекстном меню команду **Свойства**.)
4. В панели **Справка** (Help) окна свойств параметра политики предоставляется описание данного параметра.
5. Чтобы задать состояние параметра, установите один из следующих переключателей:
   - **Не задано** (Not Configured) — параметр не применяется;
   - **Включить** (Enabled) — параметр применяется и включен;
   - **Отключить** (Disabled) — параметр применяется, но отключен.
6. Для включенного параметра установите дополнительные опции в левой панели окна, если таковы имеются.
7. Переход к следующему или предыдущему параметру политики можно выполнить, не закрывая окна свойств с помощью кнопок **Следующий параметр** и **Предыдущий параметр** (Next Setting и Previous Setting). Выполните настройку всех требуемых параметров, как описано в шагах 4—6.
8. Завершив настройку параметров политики, закройте окно редактора, нажав кнопку **OK**.

Добавление и удаление шаблонов

Кроме редактирования шаблонов политики, в редактор управления групповыми политиками можно добавлять новые шаблоны и удалять существующие. Процедура для этого следующая:

1. Откройте требуемый сайт, домен или организационную единицу в редакторе управления групповыми политиками.
2. Щелкните правой кнопкой мыши на папке **Административные шаблоны** (в узле **Конфигурация компьютера** или **Конфигурация пользователя**, в зависимости от требований) и в контекстном меню выберите команду **Добавление и удаление шаблонов** (Add/Remove Templates). Откроется одноименное диалоговое окно.
3. Чтобы добавить шаблон, нажмите в этом окне кнопку **Добавить**, а затем в диалоговом окне **Шаблоны политики** (Policy Templates) выберите требуемый шаблон и нажмите кнопку **Открыть** (Open).
4. Чтобы удалить шаблон, выберите требуемый, а затем нажмите кнопку **Удалить** (Remove).
5. Завершив добавление и удаление шаблонов, закройте окно, нажав кнопку **Закрыть**.

Работа с политиками управления файлами и данными

Каждый системный администратор должен быть знаком с политиками управления файлами и данными, влияющими на объем данных, который пользователь может хранить на компьютере, на способ использования автономных файлов и на состояние возможности восстановления системы.

Настройка политики дисковых квот

Политика управления дисковыми квотами применяется на уровне системы. Параметры политики находятся в папке **Конфигурация компьютера\Административные шаблоны\Система\Дисковые квоты** (Computer Configuration\Administrative Templates\System\Disk Quotas). В табл. 5.1 приводится список и краткое описание параметров политики дисковых квот.

Таблица 5.1. *Параметры политики дисковых квот*

Параметр политики	Описание
Применить политику к съемным носителям (Apply policy to removable media)	Распространяет действие политик дисковых квот, установленных для данной папки, на тома файловой системы NTFS съемных носителей. Если этот параметр не включен, дисковые квоты будут применяться только к томам NTFS на несъемных носителях
Включить дисковые квоты (Enable disk quotas)	Включает и отключает управление дисковыми квотами для всех томов NTFS компьютера и препятствует изменению параметра политики пользователями
Обеспечить соблюдение дисковой квоты (Enforce disk quota limit)	Задает принудительное соблюдение дисковых квот и препятствует изменению параметра политики пользователями. Когда пользователи достигают установленного для соблюдения предела дисковой квоты, система расценивает это как исчерпание физического пространства тома. Этот параметр политики отменяет параметры на вкладке **Квота** диалогового окна **Свойства** томов NTFS

Таблица 5.1 *(окончание)*

Параметр политики	Описание
Записать в журнал событие при превышении квоты (Log event when quota limit exceeded)	Задает записывание в локальном журнале приложений события, возникающего при достижении пользователями предела дисковой квоты для тома, а также не позволяет пользователям изменять параметр ведения журнала
Записать в журнал событие, возникающее при превышении порога предупреждений квоты (Log event when quota warning level exceeded)	Задает записывание в локальном журнале приложений события, возникающего при достижении пользователями порога предупреждений для дисковой квоты на томе
Определить квоту и порог предупреждений по умолчанию (Specify default quota limit and warning level)	Задает дисковую квоту и порог предупреждений по умолчанию для всех пользователей тома. Этот параметр заменяет все другие параметры и применяется только к новым пользователям тома

При работе с дисковыми квотами всегда рекомендуется использовать стандартный набор параметров политики для всех систем. Включать все параметры политики обычно не требуется. Вместо этого можно выборочно включить параметры, а затем управлять квотами на разных томах посредством стандартных возможностей NTFS. Процедура включения параметров политики дисковых квот следующая:

1. Выберите групповую политику для требуемого сайта, домена или организационной единицы в редакторе управления групповыми политиками. Затем выберите папку **Дисковые квоты**, последовательно развернув узлы **Конфигурация компьютера\Административные шаблоны\Система\Дисковые квоты** (Computer Configuration\Administrative Templates\System\Disk Quotas).
2. Дважды щелкните мышью на параметре **Включить дисковые квоты** (Enable disk quotas). В открывшемся одноименном диалоговом окне установите переключатель **Включить** и нажмите кнопку **OK**.
3. Далее дважды щелкните на параметре **Обеспечить соблюдение дисковой квоты**. Если требуется обеспечить соблюдение дисковых квот на всех томах NTFS компьютера, установите переключатель **Включить**. В противном случае установите переключатель **Отключить**, а затем задайте лимиты дискового пространства для каждого тома *(см. главу 14)*. Нажмите кнопку **OK**, чтобы сохранить настройки.
4. Дважды щелкните на параметре **Определить квоту и порог предупреждений по умолчанию** и в открывшемся одноименном окне (рис. 5.6) установите переключатель **Включено**.
5. В разделе **Квота по умолчанию** (Default quota limit) установите максимальный объем дискового пространства. Эта квота применяется только к новым пользователям, когда они впервые выполняют операцию записи на том с включенными квотами. К текущим пользователям эта квота не относится; также она не влияет и на текущие лимиты. Для сетевого диска, например, используемого всеми членами команды, разумным лимитом будет 1—5 Гбайт. Конечно же, это зависит от типа файлов, с которыми пользователи обычно работают. Для графических дизайнеров или разработчика приложений обработки данных может потребоваться намного больше дискового пространства.
6. Установите порог для предупреждений. Разумным значением будет около 90% общего лимита; т. е. если установлена квота в 10 Гбайт, то для порога предупреждений следует установить 9 Гбайт. Нажмите кнопку **OK**, чтобы сохранить настройки.

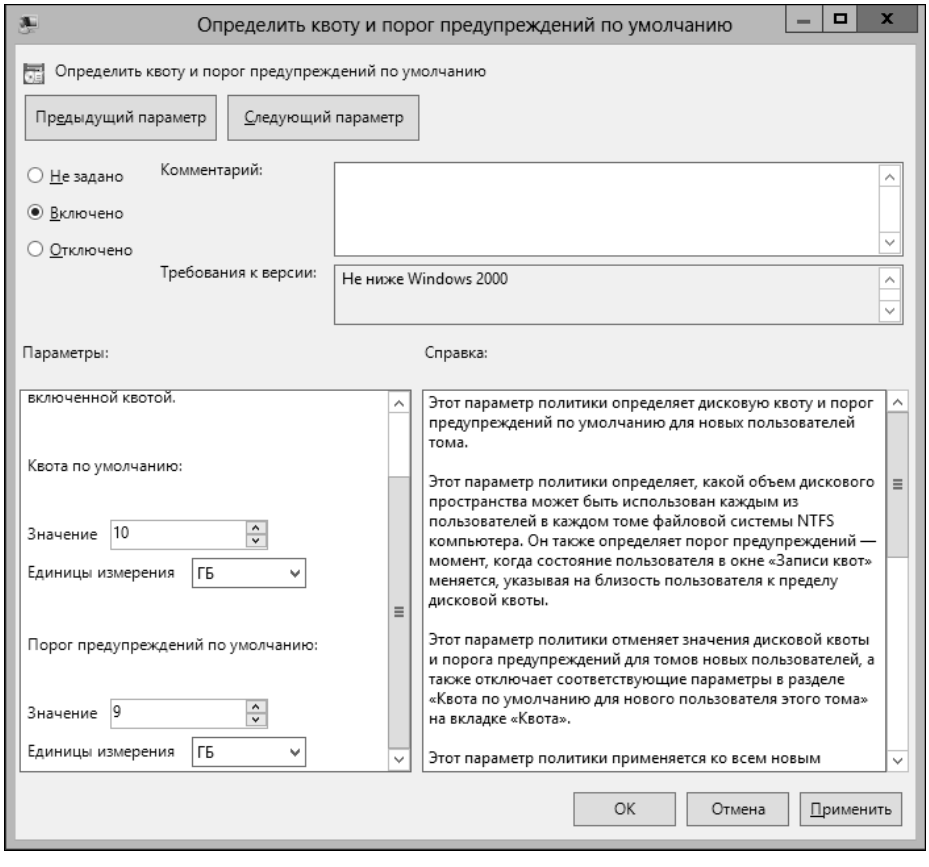


Рис. 5.6. Задание значений дисковых квот

7. Далее дважды щелкните на параметре **Записать в журнал событие при превышении квоты**. Установите переключатель **Включить**, чтобы записывать события превышения квоты в журнал приложений. Нажмите кнопку **OK**, чтобы сохранить эту настройку.
8. Дважды щелкните на параметре **Записать в журнал событие, возникающее при превышении порога предупреждений квоты**. Установите переключатель **Включить**, чтобы записывать события предупреждений в журнал приложений. Нажмите кнопку **OK**, чтобы сохранить эту настройку.
9. Наконец, дважды щелкните на параметре **Применить политику к съемным носителям**. Установите переключатель **Отключить**, чтобы применять дисковые квоты только к несъемным томам компьютера. Нажмите кнопку **OK**, чтобы сохранить настройку.

Настройка политики восстановления системы

Восстановление системы предназначено для сохранения состояния системных томов и позволяет пользователям восстановить систему к определенному предыдущему состоянию в случае проблем с текущим состоянием. Однако учтите, что эта полезная возможность способна поглощать огромный объем дискового пространства. Как рассматривалось в *главе 2*, функцию восстановления системы можно отключить для всех или отдельных дисков компьютера.

В редакторе управления групповыми политиками параметры политики **Восстановление системы** находятся в папке **Конфигурация компьютера\Административные шаблоны\Система\Восстановление системы** (Computer Configuration\Administrative Templates\System\System Restore). Посредством этих параметров можно переопределять и отключать управление возможностью восстановления системы. Политика восстановления системы имеет следующие параметры.

- **Отключить восстановление системы** (Turn off System Restore). Включение этого параметра не позволяет восстановить систему, вследствие чего этой возможностью нельзя управлять посредством диалогового окна **Свойства системы** или мастера восстановления системы. При отключенном или не заданном параметре пользователи могут настраивать восстановление системы и выполнять его с помощью вкладки **Защита системы** окна **Свойства системы**.
- **Отключить конфигурацию** (Turn off Configuration). Включение этого параметра запрещает конфигурирование защиты и восстановления системы. Пользователи не имеют доступа к диалоговому окну настройки параметров защиты. Если этот параметр не задан или отключен, пользователи могут изменять настройки восстановления системы на вкладке **Защита системы** окна **Свойства системы**.

Настройка параметров политики **Восстановление системы** осуществляется следующим способом:

1. Выберите групповую политику для требуемого сайта, домена или организационной единицы в редакторе управления групповыми политиками. Затем выберите папку **Восстановление системы**, последовательно развернув узлы **Конфигурация компьютера\Административные шаблоны\Система\Восстановление системы** (Computer Configuration\Administrative Templates\System\System Restore).
2. Чтобы включить или отключить возможность восстановления системы, дважды щелкните на параметре **Отключить восстановление системы** (Turn off System Restore). Установите переключатель **Включить** или **Отключить**, а затем нажмите кнопку **OK**.
3. Чтобы включить или отключить возможность настройки защиты системы, дважды щелкните на параметре **Отключить конфигурацию** (Turn off Configuration). Установите переключатель **Включить** или **Отключить**, а затем нажмите кнопку **OK**.

Настройка политики автономных файлов

Настройка политики автономных файлов выполняется как на уровне компьютера, так и на уровне пользователя, и оба эти уровня имеют некоторые параметры с одинаковыми именами. В отношении параметров с одинаковыми именами следует иметь в виду, что параметры компьютера имеют старшинство над параметрами пользователя; кроме этого, параметры различных уровней могут применяться в разное время.

В табл. 5.2 приводится список основных параметров политики автономных файлов и их краткое описание.

Таблица 5.2. *Основные параметры политики автономных файлов*

Тип параметра	Имя параметра	Описание
Компьютер	**Разрешить или запретить использование автономных файлов** (Allow or Disallow use of the Offline Files feature)	Включает или отключает возможность использования автономных файлов и предотвращает изменение настроек пользователями. Включает административное управление параметрами автономных файлов

Таблица 5.2 *(продолжение)*

Тип параметра	Имя параметра	Описание
Компьютер	**Настроить фоновую синхронизацию** (Configure Background Sync)	Управляет фоновой синхронизацией при медленных подключениях. Включен: периодически выполняется фоновая синхронизация файлов в общих папках между клиентом и сервером. Отключен: фоновая синхронизация выполняется в режиме по умолчанию
Компьютер	**Настроить режим медленного подключения** (Configure slow-link mode)	Управляет использованием медленных подключений. Включен: все общие папки, используемые с автономными файлами, настраиваются на работу с медленными подключениями. Отключен: автономные файлы не используют режим медленного подключения
Компьютер	**Включить фильтры блокировки файлов** (Enable file screens)	Задает типы файлов, которые можно сохранять в папке автономных файлов. Включен: пользователи не могут создавать файлы с отфильтрованными расширениями. Отключен: пользователи могут создавать любые типы файлов в папках автономных файлов
Компьютер	**Включить синхронизацию файлов в платных сетях** (Enable file synchronization on costed networks)	Управляет использованием фоновой синхронизации в низкоскоростных платных сетях, которая может вызвать дополнительные накладные расходы. Включен: синхронизация осуществляется в фоновом режиме, если пользователь находится в роуминге, приближается к пределу объема передачи данных тарифного плана или превысил его. Отключен: фоновая синхронизация сетевых папок не выполняется
Компьютер	**Включить прозрачное кэширование** (Enable Transparent Caching)	Управляет кэшированием сетевых файлов при работе с медленными подключениями. Включен: кэширование на клиенте оптимизируется с целью уменьшить число передач по медленным каналам. Отключен: прозрачное кэширование не применяется
Компьютер	**Шифрование кэша автономных файлов** (Encrypt the Offline Files cache)	Задает шифрование автономных файлов для повышения уровня безопасности
Компьютер	**Некэшируемые файлы** (Files not cached)	Позволяет указать типы (расширения) файлов, не подлежащих кэшированию
Компьютер	**Ограничить размер дискового пространства, используемого автономными файлами** (Limit disk space used by Offline Files)	Ограничивает объем дискового пространства, которое можно использовать для хранения автономных файлов
Компьютер	**Включить экономичное использование административно назначенных автономных файлов** (Turn on economical application of administratively assigned Offline Files)	Определяет способ синхронизации при входе в систему административно назначенных файлов. Включен: при входе в систему синхронизируются только новые файлы и папки. Отключен: при входе в систему синхронизируются только все файлы и папки

Таблица 5.2 *(окончание)*

Тип параметра	Имя параметра	Описание
Компьютер/ Пользователь	**Удалить команду "Сделать доступными автономно"** (Remove "Make Available Offline" command)	Запрещает пользователям сохранять сетевые файлы и папки для доступа вне сети
Компьютер/ Пользователь	**Удалить команду "Работать автономно"** (Remove "Work offline" Command)	Удаляет команду **Работать автономно** из Проводника, запрещая пользователям вручную выбирать оперативный или автономный режим использования автономных файлов
Компьютер/ Пользователь	**Указать административно назначенные автономные файлы** (Specify administratively assigned Offline Files)	Задает использование пути UNC[1] для указания файлов и папок, которые всегда доступны в автономном режиме

Из табл. 5.2 видно, что большинство параметров политики автономных файлов влияет на доступ, синхронизацию, кэширование и шифрование. Параметры политики автономных файлов компьютера находятся в папке редактора объектов групповой политики **Конфигурация компьютера\Административные шаблоны\Сеть\Автономные файлы**, а пользователя — в такой же папке, только в корневом узле **Конфигурация пользователя**.

Управлять автономным доступом к сетевым файлам можно административно. Обычно эта возможность применяется на файловых серверах или других сетевых системах с общими ресурсами. Административное управление автономными ресурсами можно осуществлять несколькими способами, настроив соответствующие параметры политики автономных файлов. Такая настройка осуществляется согласно следующей процедуре:

1. Выберите групповую политику для требуемого сайта, домена или организационной единицы в редакторе управления групповыми политиками. Многие политики автономных файлов можно настраивать как на уровне компьютера, так и на уровне пользователя (при этом настройки компьютера имеют приоритет над настройками пользователя). Параметры политики автономных файлов для компьютера находятся в папке редактора объектов групповой политики **Конфигурация компьютера\Административные шаблоны\Сеть\Автономные файлы**, а для пользователей — в такой же папке, но с корневой папкой **Конфигурация пользователя**.
2. Чтобы задать ресурсы, которые автоматически доступны в автономном режиме, дважды щелкните на параметре **Указать административно назначенные автономные файлы**. В открывшемся одноименном диалоговом окне установите переключатель **Включить** и нажмите кнопку **OK**. В открывшемся диалоговом окне **Вывод содержания** (Show Contents) задайте требуемые ресурсы, указав их путь UNC, например *\\CorpServer\23\Data* (рис. 5.7). Нажмите кнопку **OK** на этом и других открытых диалоговых окнах, чтобы закрыть их и сохранить выполненные настройки.

> ***Осторожно!***
>
> Решение о предоставлении автономного доступа к ресурсам следует внимательно обдумать, т. к. чем больше ресурсов выделяется таким способом, тем больший объем сетевого трафика генерируется для содержания кэшей автономных файлов.

[1] Universal Naming Convention — универсальные правила именования.

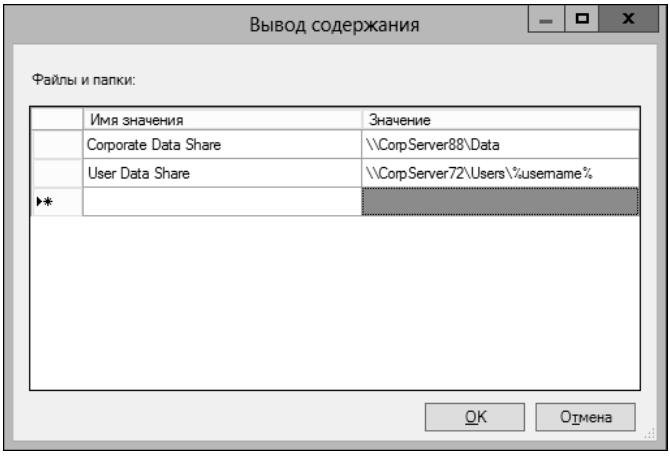


Рис. 5.7. Диалоговое окно **Вывод содержания** для указания автономных сетевых ресурсов

3. Чтобы запретить пользователям предоставлять файлы и папки в автономном режиме, дважды щелкните на параметре **Удалить команду "Сделать доступными автономно"**. В открывшемся одноименном диалоговом окне установите переключатель **Включить** и нажмите кнопку **OK**. Теперь пользователи не смогут сохранять сетевые файлы и папки для доступа вне сети.
4. Чтобы ограничить типы файлов, которые можно создавать в папках автономных файлов, дважды щелкните на параметре **Включить фильтры блокировки файлов**. В открывшемся одноименном окне установите переключатель **Включить**. Далее, в поле **Расширения** (Extensions) панели **Параметры** введите список запрещенных расширений файлов, разделяя их точкой с запятой, а затем нажмите кнопку **OK**. Запрещенные расширения вводятся в формате *звездочка-точка-расширение*, например, **.vbs* или **.js*. Теперь пользователи не смогут создавать в автономных папках файлы с этими расширениями.
5. Для Windows 8 и более поздних версий Windows может оказаться желательным включить параметр **Удалить команду "Работать автономно"**. Его задействование предотвращает изменение пользователями заданного автономного режима, не затрагивая при этом их возможности использования этого режима, как установлено.

В Windows Vista и более поздних версиях Windows синхронизация автономных файлов выполняется автоматически, с применением фоновой синхронизации при низкоскоростном канале. Для Windows 8 и более поздних версий Windows медленным каналом считается канал с сетевой задержкой свыше 35 миллисекунд. В противном случае медленным каналом считается канал с сетевой задержкой свыше 80 миллисекунд.

На компьютерах под управлением Windows Vista и более поздних версий Windows можно предотвратить переход в режим медленного подключения, отключив параметр **Настроить режим медленного подключения**. Для включенного параметра можно задать триггеры для перехода в режим медленного подключения, принимая во внимание пропускную способность и задержку сети.

Для настройки режима медленного подключения применяется следующая процедура:

1. Выберите групповую политику для требуемого сайта, домена или организационной единицы в редакторе управления групповыми политиками. Откройте папку **Конфигурация компьютера\Административные шаблоны\Сеть\Автономные файлы**.

2. Чтобы настроить условия для перехода в режим медленного подключения, дважды щелкните на параметре **Настроить режим медленного подключения**. В открывшемся одноименном диалоговом окне установите переключатель **Включить**, а затем нажмите кнопку **Показать** (Show). В открывшемся диалоговом окне **Вывод содержания** в полях **Имя значения** (Value Name) укажите требуемые ресурсы, а в поле **Значение** (Value) пороговую пропускную способность и/или задержку для данного ресурса. При этом нужно иметь в виду следующее:

   - в поле **Имя значения** ресурсы указываются с их UNC-путем. Например, для управления триггерами перехода в режим медленного подключения для всех общих ресурсов сервера CorpServer172 в это поле вводится значение `\\corpserver172\*`, а для файлов и папок сетевой папки Data сервера CorpServer85 — `\\corpserver85\data\*`;
   - чтобы указать применение данного параметра ко всем серверам, в поле **Имя значения** нужно ввести символ звездочки, т. е. `*`;
   - в поле **Значение** указывается триггер пропускной способности в битах в секунду, триггер задержки в миллисекундах или оба эти триггера. Например, чтобы выполнить переход в режим медленного подключения при пропускной способности сети меньше, чем 1024 бит/с, вводится значение `Пропускная способность=1024` (Throughput=1024), при задержке свыше 60 миллисекунд — значение `Задержка=60` (Latency=60), а чтобы указать оба триггера, вводятся значения, разделенные запятой, — `Пропускная способность=1024, Задержка=60`.

   Этот пример иллюстрируется на рис. 5.8.

   Указав все требуемые ресурсы и задав для них значения триггеров, нажмите кнопку **OK** в этом и других открытых диалоговых окнах, чтобы закрыть их и сохранить выполненные настройки.

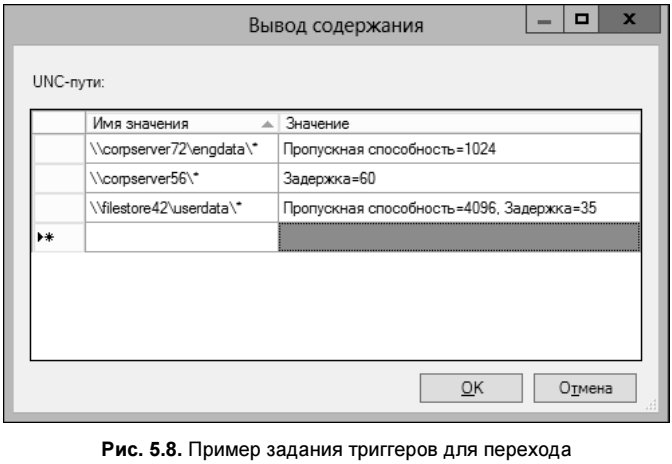


Рис. 5.8. Пример задания триггеров для перехода в режим медленного подключения для определенных ресурсов

Осторожно!

Решение о предоставлении автономного доступа к ресурсам следует внимательно обдумать, т. к. чем больше ресурсов выделяется таким способом, тем больший объем сетевого трафика генерируется для содержания кэшей автономных файлов.

3. По умолчанию при работе в режиме медленного подключения Windows выполняет фоновую синхронизацию автономных файлов приблизительно каждые шесть часов. Тон-

кую настройку фоновой синхронизации можно выполнить, включив параметр **Настроить фоновую синхронизацию** и задав значения параметров фоновой синхронизации. При настройке фоновой синхронизации нужно иметь в виду следующие моменты.

- Параметры **Интервал синхронизации** (Sync Interval) и **Дисперсия синхронизации** (Sync Variance) используются совместно для указания интервала обновления. По умолчанию параметру **Интервал синхронизации** присвоено значение `360` (минут), а параметру **Дисперсия синхронизации** — `60` (минут), чтобы предотвратить чрезмерную нагрузку на сеть и серверы вследствие множественных одновременных запросов от клиентов.
- Чтобы обеспечить периодическую синхронизацию всех сетевых папок, установите значение параметра **Максимальное разрешенное время без синхронизации** (Maximum Allowed Time Without A Sync). Например, чтобы обеспечить синхронизацию сетевых папок, по крайней мере, раз в день, этому параметру нужно присвоить значение `1440` (минут).
- Чтобы запретить синхронизацию на протяжении определенного периода времени, применяются параметры **Время начало блокировки** (Blockout Start Time) и **Длительность блокировки** (Blockout Duration). Значение первого из этих параметров задаются в часах и минутах в 24-часовом формате, а второго — в минутах. Например, чтобы запретить выполнение синхронизации сетевых папок от 14:00 до 18:00 ежедневно, первому параметру присваивается значение `1400`, а второму `240`.

4. Для Windows 8 и более поздних версий ОС можно контролировать разрешение фоновой синхронизации при работе в сотовых и других платных сетях, если пользователь находится в роуминге, приближается к пределу объема передачи данных тарифного плана или превысил его. Для этого применяется параметр политики автономных файлов **Включить синхронизацию файлов в платных сетях**. По умолчанию синхронизация в платных сетях отключена. Чтобы разрешить синхронизацию в платных сетях, этот параметр нужно включить.

Работа с политиками доступа и связности

Политики доступа и связности позволяют управлять сетевыми подключениями, коммутируемыми подключениями и настройками удаленного помощника. Эти политики определяют сетевую связность системы, а также удаленный доступ к ней.

Настройка сетевых политик

Существует большое число сетевых политик. Настройка политик для управления общим подключением к Интернету, брандмауэром подключения к Интернету, брандмауэром Windows и установкой сетевого моста осуществляется на уровне компьютера. На уровне же пользователя выполняется настройка параметров для управления локальными сетевыми подключениями, конфигурациями протоколов TCP/IP и удаленным доступом. В табл. 5.3 приводится список основных параметров сетевых политик и их краткое описание.

Параметры сетевых политик для компьютера находятся в папке редактора объектов групповой политики **Конфигурация компьютера\Административные шаблоны\Сеть\Сетевые подключения**, а для пользователей — в такой же папке, но с корневой папкой **Конфигурация пользователя**.

Таблица 5.3. *Параметры сетевых политик*

Тип параметра	Имя параметра	Описание
Компьютер	**Запрет установки и настройки сетевого моста в сети DNS-домена** (Prohibit installation and configuration of Network Bridge on your DNS domain network)	Управляет возможностью пользователей устанавливать и настраивать сетевые мосты. Этот параметр применяется только при подключении компьютера к тому же DNS-домену, к которому он был подключен при обновлении на нем данного параметра
Компьютер	**Требовать повышения прав пользователей домена при задании сетевого ресурса** (Require domain users to elevate when setting a network's location)	Определяет, требуется ли повышение прав пользователей домена при задании сетевого ресурса
Компьютер	**Маршрутизировать весь трафик через внутреннюю сеть** (Route all traffic through the internal network)	Применяется с функциональностью DirectAccess. Определяет, будут ли удаленные компьютеры иметь доступ к Интернету через корпоративную сеть или же напрямую, через свои интернет-подключения
Пользователь	**Возможность изменить свойства всех пользовательских подключений удаленного доступа** (Ability to change properties of an all user remote access connection)	Определяет, могут ли пользователи просматривать и редактировать свойства подключений удаленного доступа, которые доступны всем пользователям компьютера
Пользователь	**Запрет удаления подключений удаленного доступа** (Prohibit deletion of remote access connection)	Определяет, могут ли пользователи удалять подключения удаленного доступа

Из табл. 5.3 видно, что параметры сетевой политики для компьютеров предназначены для ограничения действий в сети организации. Применение этих ограничений запрещает пользователям использовать такие возможности, как общее подключение к Интернету в соответствующем домене. Целью этих ограничений является обеспечение безопасности корпоративных сетей, но они не мешают, например, пользователям с ноутбуками брать их домой и использовать эти возможности в своих сетях. Для управления этими ограничениями применяется следующая процедура:

1. Откройте в редакторе объектов групповых политик требуемую групповую политику, а затем выберите папку **Конфигурация компьютера\Административные шаблоны\Сеть\Сетевые подключения**.
2. Дважды щелкните мышью на требуемом параметре политики сетевого подключения. Установите переключатель **Включить** или **Отключить**, после чего нажмите кнопку **OK**.

Параметры пользователя политики сетевых подключений обычно предотвращают доступ к определенным конфигурационным возможностям, таким как дополнительные конфигурационные параметры протоколов TCP/IP. Настройка этих параметров политики сетевых подключений осуществляется следующим способом:

1. Откройте в редакторе объектов групповых политик требуемую групповую политику, а затем выберите папку **Конфигурация пользователя\Административные шаблоны\Сеть\Сетевые подключения**.

2. Дважды щелкните мышью на требуемом параметре политики сетевого подключения и установите переключатель **Включить** или **Отключить**, после чего нажмите кнопку **OK**.

Настройка политики удаленного доступа

Политику удаленного помощника можно использовать для управления возможностью предоставления удаленной помощи. Обычно параметры политики удаленного помощника включают таким образом, чтобы предотвратить предоставление незапрашиваемой помощи, разрешая при этом запрошенные предложения. Кроме этого, для запросов помощи можно установить конечную дату посредством политики вместо того, чтобы устанавливать ее с помощью окна свойств системы на каждом компьютере. Чтобы улучшить безопасность, приглашения удаленному помощнику, можно шифровать с использованием устойчивого шифрования. Но это сужает круг тех, кто может отвечать на такие приглашения удаленному помощнику только к тем лицам, которые работают на компьютерах под управлением Windows Vista или более поздних версий Windows.

Для настройки параметров политики удаленного помощника применяется следующая процедура:

1. Откройте в редакторе объектов групповых политик требуемую групповую политику, а затем разверните папку **Конфигурация компьютера\Административные шаблоны\Система\Удаленный помощник**.
2. Включите в ней параметр **Настроить запрашиваемую удаленную помощь** (Configure Solicited Remote Assistance). Теперь авторизованные пользователи могут запрашивать удаленную помощь.
3. Также можно задать уровень доступа для помощников. Для этого в раскрывающемся списке **Разрешить удаленное управление этим компьютером** (Permit remote control of this computer) предоставляются два значения:
   - **Разрешить помощникам управлять компьютером** (Allow helpers to remotely control the computer). Установка этого значения разрешает удаленным помощникам просматривать и управлять компьютером;
   - **Разрешить помощникам только просматривать компьютер** (Allow helpers to only view the computer). При выборе этого значения удаленные помощники могут только просматривать компьютер, но не выполнять на нем никаких действий.
4. Далее задайте в поле **Максимальное время билета (значение)** (Maximum ticket time (value)) максимальный срок действия приглашений удаленной помощи (рис. 5.9). Единица времени срока действия устанавливается в поле **Максимальное время билета (единицы)** (Maximum ticket time (units)). По умолчанию максимальный срок действия приглашения равен 1 часу. Нажмите кнопку **OK**, чтобы сохранить настройку.

> ***ПРАКТИЧЕСКИЙ СОВЕТ***
>
> Метод отправки приглашений по электронной почте можно задать как **Mailto** или **Simple MAPI**. Метод **Mailto** представляет собой способ отправки сообщений посредством браузера, когда получатель приглашения подключается через канал связи Интернета. При выборе метода MAPI приглашение отправляется в виде вложения в сообщения с помощью интерфейса MAPI[1]. При условии, что компьютеры могут установить друг с другом соединение по порту 80 и использовании стандартной программы электронной почты, такой как Microsoft Outlook или Windows Mail, рекомендуется использовать способ **Mailto**.

[1] Messaging Application Programming Interface — программный интерфейс коммуникационных приложений.

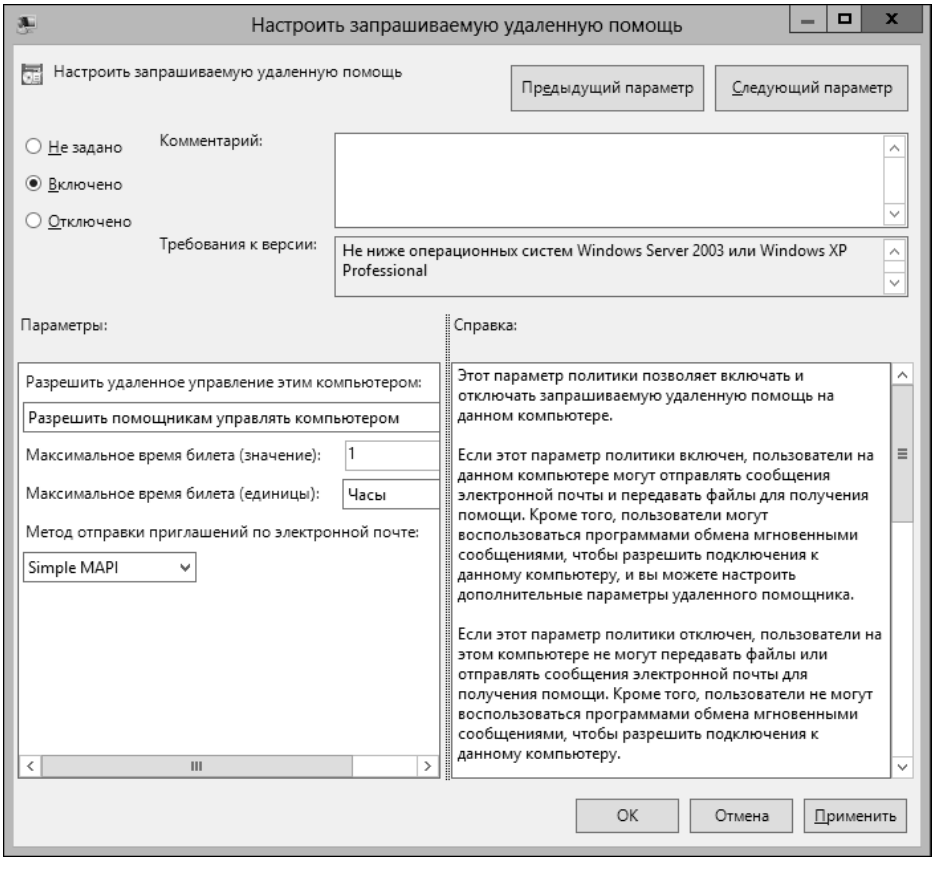


Рис. 5.9. Включение удаленной помощи и задание времени действия ее приглашений

5. Дважды щелкните на параметре **Настроить предлагаемую удаленную помощь** (Configure Offer Remote Assistance) и в открывшемся одноименном окне отключите его, установив переключатель **Отключить**. Теперь пользователи не могут получать незапрошенную удаленную помощь. Нажмите кнопку **OK**, чтобы сохранить настройку.
6. Чтобы применить устойчивое шифрование приглашений и ограничить подключение только компьютеров под управлением Windows Vista или более поздних версий Windows, включите параметр **Разрешить подключения только с компьютеров под управлением Windows Vista или более поздней версии** (Allow only Windows Vista or later connections).

Запретить удаленную помощь и удаленное управление можно следующим образом:

1. Откройте в редакторе объектов групповых политик требуемую групповую политику, а затем выберите папку **Конфигурация компьютера\Административные шаблоны\Система\Удаленный помощник**.
2. Дважды щелкните на параметре **Настроить запрашиваемую удаленную помощь** и отключите его. Затем перейдите к параметру **Настроить предлагаемую удаленную помощь**, нажав для этого кнопку **Предыдущий параметр** (Previous Setting) или **Следующий параметр** (Next Setting), как требуется, и также отключите его.
3. В завершение нажмите кнопку **OK**, чтобы сохранить выполненные настройки.

Работа с политиками сценариев компьютеров и пользователей

Политики сценариев управляют поведением и назначением сценариев компьютеров и пользователей. Можно конфигурировать четыре типа сценариев:

- **Сценарии запуска компьютера** — исполняются при запуске компьютера;
- **Сценарии завершения работы** — исполняются перед выключением компьютера;
- **Сценарии входа** — исполняются при входе пользователя в систему;
- **Сценарии выхода** — исполняются при выходе пользователя из системы.

Эти сценарии можно создавать в виде командных файлов, сценариев Windows или сценариев Windows PowerShell. В сценариях командных файлов применяется язык консоли командной строки. Сценарии Windows используют сервер сценариев Windows[1] и создаются на каком-либо языке сценариев, например VBScript или Microsoft JScript. Сценарии Windows PowerShell создаются на языке этой оболочки. Обратите внимание, что во многих случаях применение предпочтений политик может сделать использование сценариев пользователей и компьютера ненадобным.

Управление сценариями с помощью политики

Параметры политики для управления сценариями компьютера находятся в папке **Конфигурация компьютера\Административные шаблоны\Система\Сценарии**, а для управления сценариями пользователя — в такой же папке, но только корневой папкой будет **Конфигурация пользователя**. С помощью параметров политики сценариев можно управлять поведением сценариев запуска компьютера, выключения компьютера, входа и выхода. В табл. 5.4 приводится список основных параметров политики управления сценариями и их краткое описание. Как мы вскоре увидим, существует много разных вариантов настройки поведения сценариев.

Таблица 5.4. *Параметры политик сценариев компьютеров и пользователей*

Тип параметра	Имя параметра	Описание
Компьютер	**Отображать команды сценариев завершения работы во время их выполнения** (Display instructions in shutdown scripts as they run)	Отображает сценарии завершения работы компьютера и их инструкции в процессе исполнения
Компьютер	**Отображать команды сценариев запуска во время их выполнения** (Display instructions in startup scripts as they run)	Отображает сценарии запуска компьютера и их инструкции в процессе исполнения
Компьютер	**Выполнять сценарии загрузки асинхронно** (Run startup scripts asynchronously)	Позволяет системе выполнять сценарии загрузки одновременно, а не по одному за раз
Компьютер	**Выполнять сценарии Windows PowerShell первыми при запуске и завершении работы компьютера** (Run Windows PowerShell scripts first at computer startup, shutdown)	Задает выполнение сценариев Windows PowerShell перед сценариями других типов во время запуска и завершения работы компьютера

[1] Windows Script Host.

Таблица 5.4 *(окончание)*

Тип параметра	Имя параметра	Описание
Компьютер	**Указать максимальное время выполнения сценариев групповой политики** (Specify maximum wait time for Group Policy scripts)	Задает максимальное время ожидания завершения сценариев. Значение по умолчанию равно 600 секунд (10 минут)
Компьютер/ пользователь	**Выполнять сценарии входа в систему синхронно** (Run logon scripts synchronously)	Указывает, что система должна дождаться завершения работы сценариев входа, прежде чем отображать интерфейс Windows
Компьютер/ пользователь	**Выполнять сценарии Windows PowerShell первыми при входе пользователя в систему и выходе из системы** (Run Windows PowerShell scripts first at user logon, logoff)	Задает выполнение сценариев Windows PowerShell перед сценариями других типов во время входа пользователя в систему и при выходе из системы
Пользователь	**Отображать команды сценариев выхода во время их выполнения** (Display instruction in logoff scripts as they run)	Отображает сценарии выхода и их инструкции в процессе исполнения
Пользователь	**Отображать команды сценариев входа во время их выполнения** (Display instruction in logon scripts as they run)	Отображает сценарии входа и их инструкции в процессе исполнения
Пользователь	**Выполнять сценарии входа прежних версий в фоновом режиме** (Run legacy logon scripts hidden)	Скрывает отображение команд в сценариях входа, написанных для Windows NT 4.0 и более ранних версий Windows

Хотя можно задавать разные поведения сценариев, обычно требуется следующее:

- сценарии Windows PowerShell должны исполняться первыми;
- сценарии запуска и входа в систему должны исполняться одновременно (в большинстве случаев);
- исполнение должно быть в фоновом режиме;
- система не должна ожидать завершения выполнения сценария больше, чем одну минуту (в большинстве случаев).

Такое поведение можно обеспечить следующим образом:

1. Откройте в редакторе объектов групповых политик требуемую групповую политику, а затем выберите папку **Конфигурация компьютера\Административные шаблоны\Система\Сценарии**.
2. Включите параметр **Выполнять сценарии Windows PowerShell первыми при запуске и завершении работы компьютера**.
3. Включите параметр **Выполнять сценарии Windows PowerShell первыми при входе пользователя в систему и выходе из системы**.
4. Отключите параметр **Выполнять сценарии входа в систему синхронно**.
5. Включите параметр **Выполнять сценарии загрузки асинхронно**.
6. Отключите параметр **Отображать команды сценариев запуска во время их выполнения**.

7. Отключите параметр **Отображать команды сценариев завершения работы во время их выполнения.**
8. Включите параметр **Указать максимальное время выполнения сценариев групповой политики** и задайте в поле **Секунды** значение 60.
9. Выберите папку **Конфигурация пользователя\Административные шаблоны\Система\Сценарии**.
10. Включите параметр **Выполнять сценарии входа прежних версий в фоновом режиме**.
11. Отключите параметр **Отображать команды сценариев входа во время их выполнения**.
12. Отключите параметр **Отображать команды сценариев выхода во время их выполнения**.
13. Включите параметр **Выполнять сценарии Windows PowerShell первыми при входе пользователя в систему и выходе из системы**.

Назначение сценариев запуска и завершения работы компьютера

Назначение сценариев запуска и завершения работы компьютера можно осуществлять как часть групповой политики. Таким образом, компьютер и все его пользователи (или все компьютеры, являющиеся членами сайта, домена или организационной единицы) будут исполнять сценарии автоматически при запуске и при завершении работы.

Назначить сценарии компьютера можно следующим образом:

1. Скопируйте требуемые сценарии в папку Scripts\Startup или Scripts\Shutdown для соответствующих параметров (запуска или завершения работы). На контроллерах доменов сценарии находятся в папке *%SystemRoot%\Sysvol\Sysvol\%UserDnsDomain%*\Policies\GUID\Machine, а на рабочих станциях под управлением Windows 8 — в папке *%WinDir%*\System32\GroupPolicy\Machine.
2. Откройте в редакторе объектов групповых политик требуемую групповую политику, а затем выберите узел **Конфигурация компьютера\Конфигурация Windows\Сценарии (запуск\завершение)**.
3. Для работы со сценариями запуска щелкните правой кнопкой мыши на параметре **Автозагрузка** (Startup) и в контекстном меню выберите команду **Свойства**, а для работы со сценариями завершения работы проделайте эту процедуру с параметром **Завершение работы** (Shutdown). Проверьте наличие сценариев, нажав кнопку **Показать файлы** (Show Files) в диалоговом окне свойств требуемого параметра. В Проводнике откроется соответствующая параметру папка, которая должна содержать скопированные в нее, как указывалось ранее, сценарии.
4. Чтобы назначить сценарий, нажмите кнопку **Добавить** в диалоговом окне свойств параметра. Откроется диалоговое окно **Добавление сценария** (Add a Script). В поле **Имя сценария** (Script Name) введите имя требуемого сценария из папки Scripts\Startup или Scripts\Shutdown (в зависимости от параметра, с которым работаете). В поле **Параметры сценария** (Script Parameters) введите аргументы командной строки для передачи сценарию командного файла или параметры для передачи серверу сценариев для WSH-сценария. Повторите этот шаг, чтобы добавить дополнительные сценарии.
5. При запуске или завершении работы компьютера сценарии исполняются в том порядке, в котором они указаны в списке диалогового окна **Свойства**. Чтобы переместить сцена-

рий вверх или вниз по списку, выберите требуемый сценарий, а затем нажмите клавишу <↑> или <↓>, пока сценарий не займет требуемое место.

6. Имя и параметры заданных сценариев можно редактировать, выбрав требуемый сценарий в списке и нажав кнопку **Изменить** (Edit).
7. Удалить выбранный сценарий можно, нажав кнопку **Удалить** (Remove).

Назначение сценариев пользователя входа в систему и выхода из системы

Назначение сценариев пользователя можно осуществлять как часть групповой политики. Таким образом, все пользователи, которые работают с компьютером или являются членами сайта, домена или организационной единицы будут исполнять сценарии автоматически при входе в систему и выходе из системы.

Назначить сценарии пользователя можно следующим образом:

1. Скопируйте требуемые сценарии в папку Scripts\Logon или Scripts\Logoff для соответствующих параметров (входа или выхода из системы). На контроллерах доменов сценарии находятся в папке *%SystemRoot%\Sysvol\Sysvol\%UserDnsDomain%*\Policies\GUID\User, а на рабочих станциях под управлением Windows 8 — в папке *%WinDir%*\System32\GroupPolicy\User.
2. Откройте в редакторе объектов групповых политик требуемую групповую политику, а затем выберите узел **Конфигурация пользователя\ Конфигурация Windows | Сценарии (вход\выход из системы)**.
3. Для работы со сценариями входа в систему щелкните правой кнопкой мыши на параметре **Вход в систему** (Logon) и в контекстном меню выберите команду **Свойства**, а для работы со сценариями выхода из системы проделайте эту процедуру с параметром **Выход из системы**. Проверьте наличие сценариев, нажав кнопку **Показать файлы** (Show Files) в диалоговом окне свойств требуемого параметра. В Проводнике откроется соответствующая параметру папка, которая должна содержать скопированные в нее, как указывалось ранее, сценарии.
4. Чтобы назначить сценарий, нажмите кнопку **Добавить** в диалоговом окне свойств параметра. Откроется диалоговое окно **Добавление сценария**. В поле **Имя сценария** введите имя требуемого сценария из папки Scripts\Logon или Scripts\Logoff (в зависимости от параметра, с которым работаете). В поле **Параметры сценария** введите аргументы командной строки для передачи сценарию командного файла или параметры для передачи серверу сценариев для WSH-сценария. Повторите этот шаг, чтобы добавить дополнительные сценарии.
5. При входе в систему или выходе из нее сценарии исполняются в том порядке, в котором они указаны в списке диалогового окна **Свойства**. Чтобы переместить сценарий вверх или вниз по списку, выберите требуемый сценарий, а затем нажмите клавишу <↑> или <↓>, пока сценарий не займет требуемое место.
6. Имя и параметры заданных сценариев можно редактировать, выбрав требуемый сценарий в списке и нажав кнопку **Изменить**.
7. Удалить выбранный сценарий можно, нажав кнопку **Удалить**.

Работа с политиками входа в систему и автозагрузки

Операционная система Windows 8 предоставляет набор политик для управления процессом входа в систему, некоторые из них позволяют настраивать способ выполнения программ при входе пользователя в систему. Эти политики похожи на сценарии входа в систему, в том отношении, что они позволяют выполнять определенные задания при входе пользователя в систему. Другие политики позволяют изменить внешний вид экранов приветствия и входа в систему. Политики компьютера входа в систему и автозагрузки находятся в узле редактора групповых политик **Конфигурация компьютера\Административные шаблоны\Система\Вход в систему**, а политики пользователя — в такой же папке, но корневой папкой является **Конфигурация пользователя** (табл. 5.5).

Таблица 5.5. *Параметры политики входа в систему*

Тип параметра	Имя параметра	Описание
Компьютер	**Всегда использовать классический вход в систему** (Always Use Classic Logon)	Для Windows 7 и более ранних версий Windows этот параметр отключает простой экран входа в систему, используемый по умолчанию, и включает экран входа, используемый в предыдущих версиях Windows
Компьютер	**Всегда использовать настраиваемый фон входа в систему** (Always Use Custom Logon Background)	Позволяет использовать настраиваемый фон экрана входа в систему
Компьютер	**Всегда ждать сеть при запуске и входе в систему** (Always Wait For The Network At Computer Startup And Logon)	Заставляет компьютер ожидать полной инициализации сети. При запуске компьютера этот параметр политики применяется полностью, а не только посредством фонового обновления. При входе в систему это означает, что для аутентификации пользователя нельзя применять кэшированные параметры доступа пользователя, а нужно выполнять аутентификацию на контроллере доменов
Компьютер	**Не перечислять подключенных пользователей на компьютерах, подключенных к домену** (Do Not Enumerate Connected Users On Domain-Joined Computers)	При входе в систему на компьютерах, подключенных к домену, этот параметр предотвращает выполнение перечисления подключенных пользователей интерфейсом входа пользователя в систему
Компьютер	Перечислять локальных пользователей на компьютерах, подключенных к домену (Enumerate Local Users On Domain-Joined Computers)	Позволяет интерфейсу входа пользователя в систему выполнять перечисление локальных пользователей при входе в систему
Компьютер	**Отключить уведомления приложений на экране блокировки** (Turn Off App Notification On the Lock Screen)	Предотвращает вывод уведомлений приложений рабочего стола на экран блокировки
Компьютер	**Включить вход с помощью ПИН-кода** (Turn On PIN Sign-In)	Позволяет доменным пользователям выполнять вход в систему с использованием ПИН-кода

Таблица 5.5 *(окончание)*

Тип параметра	Имя параметра	Описание
Компьютер	**Выключить вход с графическим паролем** (Turn Off Picture Password Sign-in)	Запрещает доменным пользователям создавать и использовать графический пароль для входа в систему
Компьютер/ пользователь	**Не обрабатывать список запуска старых программ** (Do Not Process The Legacy Run List)	При включенном параметре система игнорирует список запуска наследуемых программ, за исключением программ, заданных посредством редактора системных политик в Windows NT 4
Компьютер/ пользователь	**Не обрабатывать список однократного запуска программ** (Do Not Process The Run Once List)	Принуждает систему игнорировать настраиваемые списки однократно запускаемых программ
Компьютер/ пользователь	**Выполнять эти программы при входе в систему** (Run These Programs At User Logon)	Позволяет задать список программ, исполняемых при входе в систему всеми пользователями. Программы указываются с использованием полного пути исполняемого файла (за исключением программ, расположенных в папке *%SystemRoot%*)

Настройка программ автозапуска на основе политики

Хотя пользователи могут настраивать свои программы автозапуска отдельно, обычно имеет больше смысла делать это посредством групповой политики, особенно в организации, в которой группа пользователей запускает одно и то же приложение. Задать программу для исполнения при входе пользователя в систему можно следующим образом:

1. Откройте в редакторе объектов групповых политик групповую политику для требуемого компьютера, а затем выберите папку **Конфигурация компьютера\Административные шаблоны\Система\Вход в систему**.
2. Дважды щелкните по параметру **Выполнять эти программы при входе в систему** и установите переключатель **Включить**.
3. Далее нажмите кнопку **Показать** (Show) и в открывшемся диалоговом окне **Вывод содержания** задайте требуемые приложения автозапуска, указав их полный путь файла или UNC-путь. Например, C:\Program Files (x86)\InternetExplorer\Iexplore.exe или \\DCServ01\Apps\Stats.exe.
4. Закройте все открытые диалоговые окна.

Отключение списков исполнения посредством политики

С помощью групповой политики можно отключить списки запускаемых наследуемых программ, а также списки однократно запускаемых программ. Списки запускаемых наследуемых программ находятся в разделах реестра `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run` и `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run`.

Списки однократно запускаемых программ хранятся в разделах реестра `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce` и `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce`.

Для списков запускаемых программ применяется следующая процедура:

1. Откройте в редакторе объектов групповых политик групповую политику для требуемого компьютера. Затем разверните узел с политикой компьютера входа в систему **Конфигурация компьютера\Административные шаблоны\Система\Вход в систему** или политику пользователя, которая находится в такой же папке, но корневой папкой будет **Конфигурация пользователя**.
2. Включите параметр **Не обрабатывать список однократного запуска программ**.
3. Включите параметр **Не обрабатывать список запуска старых программ**.

ГЛАВА 6

Автоматизация конфигурирования Windows 8

Предпочтения групповых политик позволяют автоматически выполнять настройку, развертывание и управление параметрами операционной системы и приложений, включая параметры для источников данных, подключенных дисков, переменных среды, сетевых дисков, опций папок и ярлыков. При развертывании или настройке компьютеров работать с предпочтениями групповых политик легче и проще, чем настраивать одни и те же параметры вручную на каждом компьютере, в образах Windows или посредством сценариев запуска, завершения работы, входа в систему и выхода из системы.

В этой главе рассматриваются основные понятия, необходимые для понимания и управления предпочтениями групповых политик. А в последующих главах обсуждаются способы применения предпочтений отдельных политик для автоматического конфигурирования компьютеров под управлением Windows, независимо от размера организации, в которой эти компьютеры используются.

Предпочтения групповой политики

Настройка предпочтений выполняется для групповых политик каталога папок Active Directory. Локальные групповые политики не имеют предпочтений. Групповая политика не осуществляет строгого принуждения применения предпочтений и не сохраняет их в отделах реестра, относящихся к политикам. Вместо этого предпочтения хранятся в той же области реестра, которая используется приложением или функциональностью операционной системы для хранения связанных параметров. Этот подход позволяет использовать предпочтения с приложениями и функциональностями операционной системы, не поддерживающими групповую политику.

Использование предпочтений не отключает возможности приложений или функциональностей операционной системы, и пользователи могут изменять параметры, заданные администратором посредством предпочтений. Но значения предпочтений заменяют значения существующих настроек, и восстановить их исходное состояние после удаления политики невозможно.

Как и в случае с параметрами политик, предпочтения обновляются через определенный интервал времени, по умолчанию составляющий 60—120 мин. Это означает, что заданные администратором значения предпочтений будут заменять настройки пользователя, выполненные после последнего обновления предпочтений. Вместо периодического обновления предпочтений можно задать их одноразовое применение.

Какой из этих двух подходов применения предпочтений выбрать, зависит от того, требуется ли принудительное применение предпочтения. Если не требуется, необходимо отключить автоматические обновления предпочтения, в противном случае автоматические обновления следует включить.

Так как предпочтения применяются как к конфигурации компьютеров, так и к конфигурации пользователей, каждый из соответствующих узлов редактора управления групповыми политиками содержит этот подузел[1]. Как в узле компьютера, так и узле пользователя подузел предпочтений содержит два вложенных узла:

- **Конфигурация Windows** (Windows Settings) — применяется для управления общими предпочтениями операционной системы и приложений;
- **Параметры панели управления** (Control Panel Settings) — применяется для управления параметрами Панели управления.

В табл. 6.1 представлен список предпочтений, их конфигурационные области и корневые узлы.

Таблица 6.1. *Параметры предпочтений групповой политики*

Тип предпочтения | Элемент предпочтения	Размещение	Область настройки
Приложения | Приложение (Applications | Application)	**Конфигурация Windows** (Windows Settings)	Пользователь
Источники данных | Системный источник данных (Data Sources | System Data Source)	**Параметры панели управления** (Control Panel Settings)	Компьютер и пользователь
Источники данных | Пользовательский источник данных (Data Sources | User Data Source)	**Параметры панели управления** (Control Panel Settings)	Пользователь
Устройства | Устройство (Devices | Device)	**Параметры панели управления** (Control Panel Settings)	Компьютер и пользователь
Сопоставления дисков | Сопоставленный диск (Drive Maps | Mapped Drive)	**Конфигурация Windows** (Windows Settings)	Пользователь
Среда | Переменная среды (Environment | Environment Variable)	**Конфигурация Windows** (Windows Settings)	Компьютер и пользователь
Файлы | Файл (Files | File)	**Конфигурация Windows** (Windows Settings)	Компьютер и пользователь
Параметры папок | Параметры папки (Windows XP) (Folder Options | Folder Options (Windows XP))	**Параметры панели управления** (Control Panel Settings)	Пользователь
Параметры папок | Параметры папки (Windows Vista и выше) (Folder Options | Folder Options (at least Windows Vista))	**Параметры панели управления** (Control Panel Settings)	Пользователь
Параметры папок | Тип файла (Folder Options | File Type)	**Параметры панели управления** (Control Panel Settings)	Компьютер

[1] Локализация этого узла — **Настройка** — не совсем соответствует английскому названию — **Preferences**. — *Прим. пер.*

Таблица 6.1 *(продолжение)*

Тип предпочтения | Элемент предпочтения	**Размещение**	**Область настройки**
Параметры папок | Открыть с помощью (Folder Options | Open With)	**Параметры панели управления** (Control Panel Settings)	Пользователь
Папки | Папка (Folders | Folder)	**Конфигурация Windows** (Windows Settings)	Компьютер и пользователь
INI-файлы | Файл .ini (Ini Files | Ini File)	**Конфигурация Windows** (Windows Settings)	Компьютер и пользователь
Параметры обозревателя | Internet Explorer версии 5 и 6 (Internet Settings | Microsoft Internet Explorer 5 and 6)	**Параметры панели управления** (Control Panel Settings)	Пользователь
Параметры обозревателя | Internet Explorer 7 (Internet Settings | Windows Internet Explorer 7)	**Параметры панели управления** (Control Panel Settings)	Пользователь
Параметры обозревателя | Internet Explorer 8 и 9 (Internet Settings | Windows Internet Explorer 8 and 9)	**Параметры панели управления** (Control Panel Settings)	Пользователь
Параметры обозревателя | Internet Explorer 10 (Internet Settings | Windows Internet Explorer 10)	**Параметры панели управления** (Control Panel Settings)	Пользователь
Локальные пользователя и группы | Локальный пользователь (Local Users And Groups | Local User)	**Параметры панели управления** (Control Panel Settings)	Компьютер и пользователь
Локальные пользователи и группы | Локальная группа (Local Users And Groups | Local Group)	**Параметры панели управления** (Control Panel Settings)	Компьютер и пользователь
Сетевые параметры | Коммутируемое подключение (Network Options | Dial-Up Connection)	**Параметры панели управления** (Control Panel Settings)	Компьютер и пользователь
Сетевые параметры | VPN-подключение (Network Options | VPN Connection)	**Параметры панели управления** (Control Panel Settings)	Компьютер и пользователь
Сопоставления дисков | Сопоставленный диск (Network Shares | Network Share)	**Конфигурация Windows** (Windows Settings)	Компьютер
Электропитание | Электропитание (Windows XP) (Power Options | Power Options (Windows XP))	**Параметры панели управления** (Control Panel Settings)	Компьютер и пользователь
Электропитание | Схема управления питанием (Windows XP) (Power Options | Power Scheme (Windows XP))	**Параметры панели управления** (Control Panel Settings)	Компьютер и пользователь
Электропитание | Схема управления питанием (Windows 7 и выше) (Power Options | Power Plan (at least Windows 7))	**Параметры панели управления** (Control Panel Settings)	Компьютер и пользователь
Принтеры | Локальный принтер (Printers | Local Printer)	**Параметры панели управления** (Control Panel Settings)	Компьютер и пользователь
Принтеры | Общий принтер (Printers | Shared Printer)	**Параметры панели управления** (Control Panel Settings)	Пользователь

Таблица 6.1 *(окончание)*

Тип предпочтения | Элемент предпочтения	Размещение	Область настройки
Принтеры | TCP/IP принтер (Printers | TCP/IP Printer)	**Параметры панели управления** (Control Panel Settings)	Компьютер и пользователь
Реестр | Элемент реестра (Registry | Registry Item)	**Конфигурация Windows** (Windows Settings)	Компьютер и пользователь
Реестр | Элемент семейства (Registry | Collection Item)	**Конфигурация Windows** (Windows Settings)	Компьютер и пользователь
Реестр | Мастер реестра (Registry | Registry Wizard)	**Конфигурация Windows** (Windows Settings)	Компьютер и пользователь
Региональные параметры Regional Options	**Параметры панели управления** (Control Panel Settings)	Пользователь
Назначенные задания | Назначенное задание Scheduled Tasks | Scheduled Task	**Параметры панели управления** (Control Panel Settings)	Компьютер и пользователь
Назначенные задания | Очередное задание (Windows XP) (Scheduled Tasks | Immediate Task (Windows XP))	**Параметры панели управления** (Control Panel Settings)	Компьютер и пользователь
Назначенные задания | Запланированная задача (Windows 7 и выше) (Scheduled Tasks | Scheduled Task (at least Windows 7))	**Параметры панели управления** (Control Panel Settings)	Компьютер и пользователь
Назначенные задания | Немедленная задача (Windows 7 и выше) (Scheduled Tasks | Immediate Task (at least Windows 7))	**Параметры панели управления** (Control Panel Settings)	Компьютер и пользователь
Службы | Служба (Services | Service)	**Параметры панели управления** (Control Panel Settings)	Компьютер
Ярлыки | Ярлык (Shortcuts | Shortcut)	**Конфигурация Windows** (Windows Settings)	Компьютер и пользователь
Главное меню | Меню "Пуск" (Windows XP) (Start Menu | Start Menu (Windows XP))	**Параметры панели управления** (Control Panel Settings)	Пользователь
Главное меню | Меню "Пуск" (Windows Vista и выше) (Start Menu | Start Menu (at least Windows Vista))	**Параметры панели управления** (Control Panel Settings)	Пользователь

Настройка предпочтений групповой политики

Конфигурирование и управления предпочтениями политики осуществляется иначе, чем параметрами политики. Для определения предпочтения задается действие управления, состояние редактирования или обе настройки.

Работа с действиями управления

При просмотре определенной области предпочтений можно также указать способ применения этих предпочтений, используя для этого действия управления. Большинство предпочтений поддерживают следующие действия управления.

- **Создать** (Create) — создает элемент предпочтения (только если он еще не существует).
- **Заменить** (Replace) — удаляет существующий элемент предпочтения, а затем снова создает его. Если элемент не существует, то создается новый элемент. Большинство предпочтений имеет дополнительные опции, управляющие работой операции **Заменить**. Пример диалогового окна для установки таких опций показан на рис. 6.1.

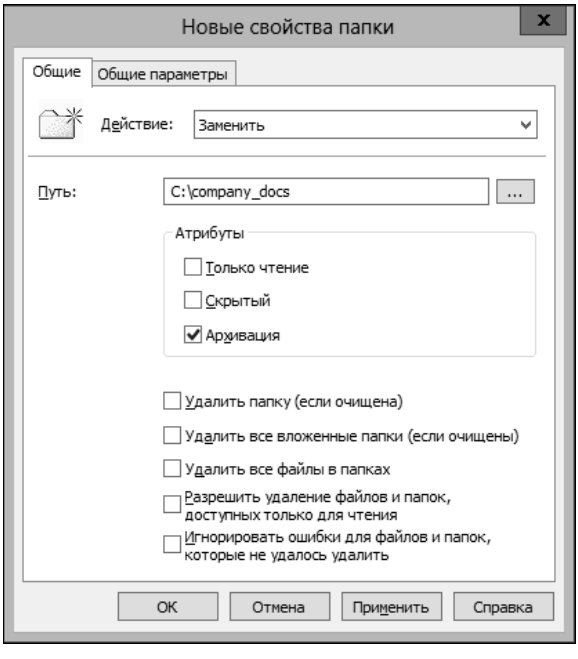


Рис. 6.1. Установка дополнительных параметров для действия управления

- **Обновить** (Update) — модифицирует указанные параметры элемента предпочтений. Это действие отличается от действия **Заменить** тем, что оно обновляет только параметры, определенные в элементе предпочтений. Все другие параметры остаются прежними. Если элемент предпочтения не существует, действие **Обновить** создает его.
- **Удалить** (Delete) — удаляет элемент предпочтения с компьютера пользователя. Большинство предпочтений имеет дополнительные опции, управляющие работой действия **Удалить**. Часто это такие же опции, как и для действия **Заменить**.

Действие управления регулирует применение элемента предпочтений или удаление элемента, если он больше не требуется. В число предпочтений, поддерживающих действия управления, входят предпочтения, которые используются для настройки следующих компонентов:

- приложений;
- источников данных;
- сопоставлений дисков;
- среды;

- файлов;
- папок;
- ini-файлов;
- локальных пользователей и групп;
- сетевых параметров;
- сетевых дисков;
- принтеров;
- элементов реестра;
- запланированных заданий;
- ярлыков.

Работа с состояниями редактирования

Небольшой набор предпочтений поддерживает состояния редактирования, которые позволяют настраивать отдельные элементы графических интерфейсов пользователя. С этим типом предпочтений элемент предпочтения применяется в соответствии с состоянием редактирования каждого параметра связанного интерфейса. Примененное состояние редактирования нельзя отменить; также нельзя удалить состояние редактирования, когда оно больше не применяется.

В число предпочтений, которые поддерживают состояния редактирования, входят предпочтения, которые используются для настройки следующих компонентов:

- параметры папок;
- настройки Интернета;
- параметры электропитания;
- региональные параметры;
- параметры главного меню.

Примечание

Состояния редактирования поддерживаются только стандартными параметрами папок.

Так как разные версии приложения и операционной системы Windows могут иметь различный интерфейс пользователя, конкретные опции закрепляются за определенной версией приложения. Например, элементы предпочтения параметров папок для Internet Explorer 8 и 9 задаются отдельно от таких же элементов для Internet Explorer 10.

По умолчанию при работе с предпочтениями этого типа каждый параметр интерфейса обрабатывается клиентом и применяется, даже если связанное значение не было явно установлено. Это фактически заменяет все существующие значения параметров, заданные посредством этого интерфейса. Состояние редактирования каждого связанного параметра отображается графически следующим образом:

- сплошная линия зеленого цвета означает, что параметр предоставляется и обрабатывается клиентом;
- пунктирная линия красного цвета означает, что параметр не предоставляется и не обрабатывается клиентом.

Пример этого типа указания состояния редактирования представлен на рис. 6.2.

Когда ограниченное пространство интерфейса не позволяет применять подчеркивание для указания состояния редактирования, в качестве эквивалента зеленой линии применяется зеленый кружок (означающий, что параметр предоставляется и обрабатывается клиентом), а в качестве эквивалента красной пунктирной линии применяется красный кружок (означающий, что параметр не предоставляется и не обрабатывается клиентом). Пример такого типа указания состояния редактирования представлен на рис. 6.3.

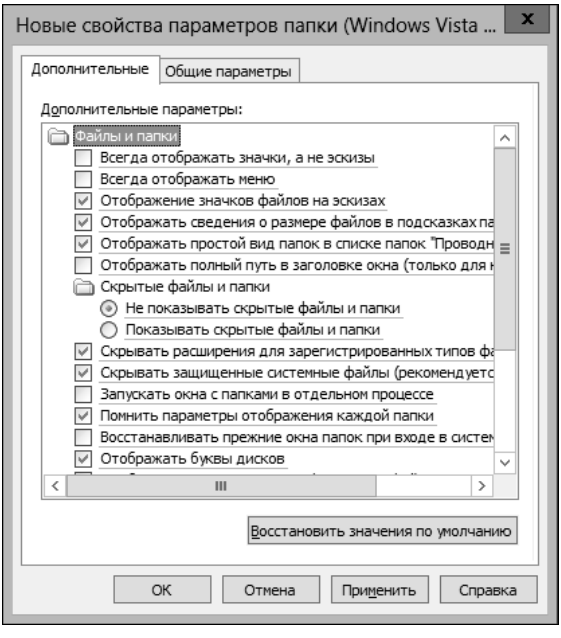


Рис. 6.2. Индикаторы состояния редактирования в виде линий

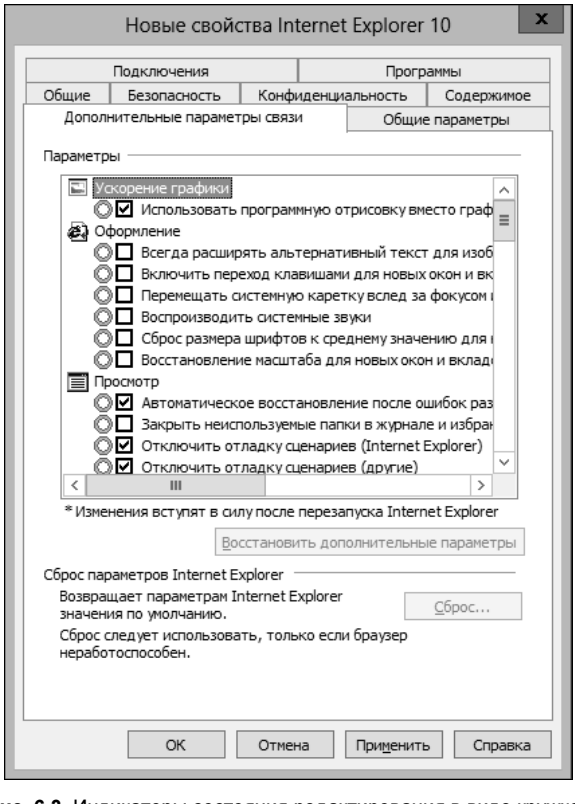


Рис. 6.3. Индикаторы состояния редактирования в виде кружков

Управлять состоянием редактирования параметров можно с помощью функциональных клавиш:

- <F5> — включает обработку всех параметров на выбранной вкладке. Эта возможность может быть полезной, когда при отключенной обработке некоторых параметров позже требуется обрабатывать все параметры вкладки;
- <F6> — включает обработку текущего выбранного параметра на выбранной вкладке. Эта возможность может быть полезной, когда требуется обрабатывать ранее отключенный параметр;
- <F7> — отключает обработку текущего выбранного параметра на выбранной вкладке. Эта возможность может быть полезной, когда требуется предотвратить обработку клиентом одного параметра;
- <F8> — отключает обработку всех параметров на выбранной вкладке. Эта возможность может быть полезной, когда требуется предотвратить обработку клиентом всех параметров на вкладке, а также когда требуется включить только несколько параметров.

Примечание

Следует иметь в виду, что значение, связанное с параметром, не имеет ничего общего с состоянием редактирования. Включение или отключение параметра не меняет состояние редактирования.

Использование альтернативных действий и состояний

Несколько предпочтений не поддерживают ни действий управления, ни состояний редактирования. К предпочтениям этого типа относятся предпочтения для конфигурирования устройств, очередных заданий и служб.

Для включения или отключения устройства определенного типа или класса используется список **Действие** (рис. 6.4).

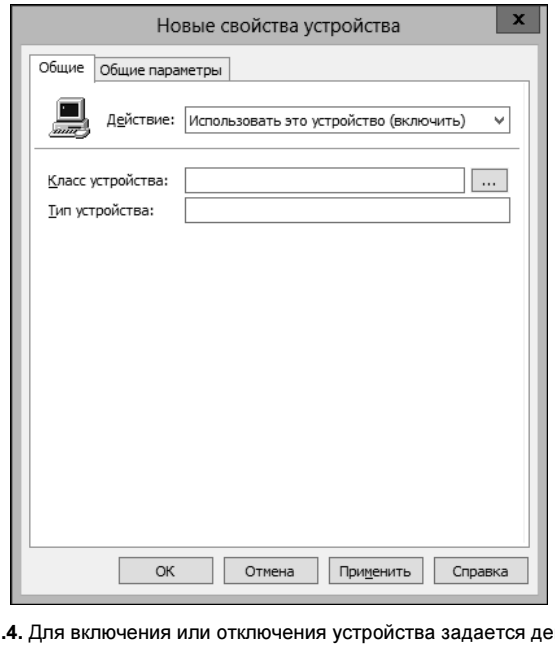


Рис. 6.4. Для включения или отключения устройства задается действие

Для очередных задач связанное предпочтение создает задание, которое исполняется, а затем автоматически удаляется. Для настройки существующей службы используется связанное предпочтение.

Управления элементами предпочтений групповой политики

Для просмотра и настройки предпочтений в редакторе управления групповыми политиками необходимо открыть соответствующий объект групповой политики *(см. главу 5)*. Теперь предпочтениями для компьютеров и/или пользователей можно управлять, используя следующие подходы:

- для настройки предпочтений для компьютеров, независимо от вошедших на них пользователей, разверните узел **Конфигурация компьютера**, в нем разверните узел предпочтений **Настройка**, а затем выберите требуемую область предпочтений;
- для настройки предпочтений для пользователей, независимо от того, на каком компьютере они выполнили вход, разверните узел **Конфигурация пользователя**, в нем разверните узел предпочтений **Настройка**, а затем выберите требуемую область предпочтений.

Создание и управление элементом предпочтения

Управление элементами предпочтений осуществляется отдельно для каждого элемента, который выбирается в требуемой области предпочтений. При просмотре определенной области предпочтений можно создать связанный элемент, щелкнув правой кнопкой в свободной области правой панели, выбрав в контекстном меню команду **Создать** (New), а затем выбрав во вложенном меню тип элемента, который требуется создать. Создать можно только тип элементов для выбранной области предпочтений. Например, в выбранной области **Принтеры** в узле конфигурации компьютера создать можно лишь предпочтение для TCP/IP-принтера или локального принтера.

Щелчок на элементе правой кнопкой мыши открывает контекстное меню, содержащее опции для управления этим элементом. Пример такого контекстного меню показан на рис. 6.5.

Подобные опции также отображаются в виде значков на панели инструментов при выборе элемента предпочтений. Кроме опций контекстного меню для управления элементом управления также применяется диалоговое окно его свойств. Открыть это окно можно, выбрав команду **Свойства** в контекстном меню элемента или же выполнив по нему двойной щелчок мышью. В диалоговом окне свойств элемента предпочтений можно просматривать и/или редактировать его параметры.

Клиенты групповой политики обрабатывают элементы предпочтений согласно их порядку старшинства. Элемент предпочтения с самым низким старшинством (последний в списке) обрабатывается первым, за ним обрабатывается элемент со следующим самым низким старшинством, и т. д., до тех пор, пока не будет обработан элемент с наивысшим старшинством (первый в списке).

Обработка в порядке старшинства выполняется с целью обеспечения приоритета старших элементов над младшими. В случае конфликта между параметрами элементов предпочтений приоритет имеют параметры, примененные последними. Чтобы изменить порядок старшинства элементов, выберите в правой панели требуемый элемент, а затем на панели инструментов нажмите кнопку **Переместить выделенный объект вниз** (Move the selected

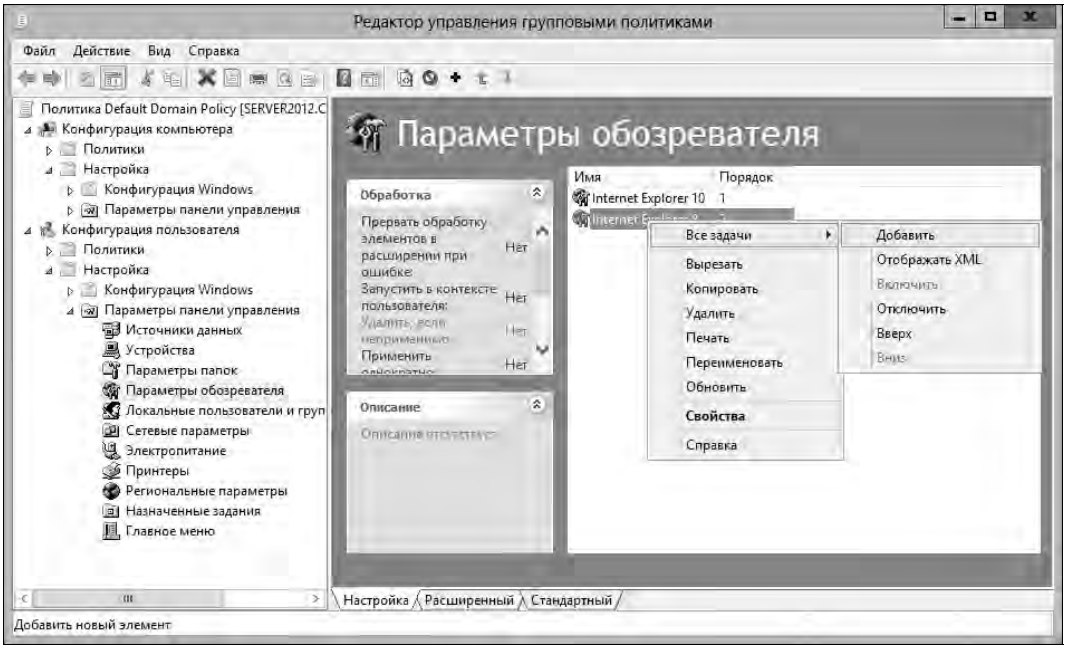


Рис. 6.5. Контекстное меню для управления элементом предпочтения

item down), чтобы понизить приоритет элемента, или кнопку **Переместить выделенный объект вверх** (Move the selected item up), чтобы повысить приоритет элемента.

Задание общих параметров элементов

Окно свойств всех элементов предпочтений имеет вкладку **Общие параметры** (Common), содержащую параметры, общие для всех элементов предпочтений. Хотя список параметров на этой вкладке зависит от конкретного элемента предпочтений, большинство из них имеет параметры, показанные на рис. 6.6.

Назначение общих параметров следующее.

- **Остановить обработку элементов в этом расширении при возникновении ошибки** (Stop processing items in this extension if an error occurs). По умолчанию, в случае сбоя обработки одного элемента предпочтения, обработка других элементов предпочтения продолжается. Это поведение можно изменить, установив данный флажок. В таком случае сбой обработки одного элемента вызывает прекращение обработки оставшихся элементов предпочтения в обрабатываемом расширении соответствующего объекта групповой политики. Установка этого параметра не затрагивает обработку элементов предпочтения в других объектах групповой политики.
- **Выполнять в контексте безопасности вошедшего пользователя** (Run in logged-in user's security context). По умолчанию клиент групповой политики обрабатывает предпочтения пользователя в контексте безопасности или учетной записи Winlogon (на компьютерах под управлением Windows XP или более ранних версий Windows), или системной учетной записи (на компьютерах под управлением Windows Vista или более поздних версий Windows). В этом контексте расширение предпочтения ограничено переменными среды и системными ресурсами компьютера. Альтернативно, клиент может обрабатывать предпочтения пользователя в контексте безопасности учетной записи во-

шедшего пользователя. Это позволяет расширению предпочтения обращаться к ресурсам, как будто это сделал пользователь, а не системная служба. Такой подход может потребоваться при использовании подключенных сетевых дисков или других предпочтений, для которых компьютер может не иметь прав доступа к ресурсам или может потребовать доступа к пользовательским переменным среды.

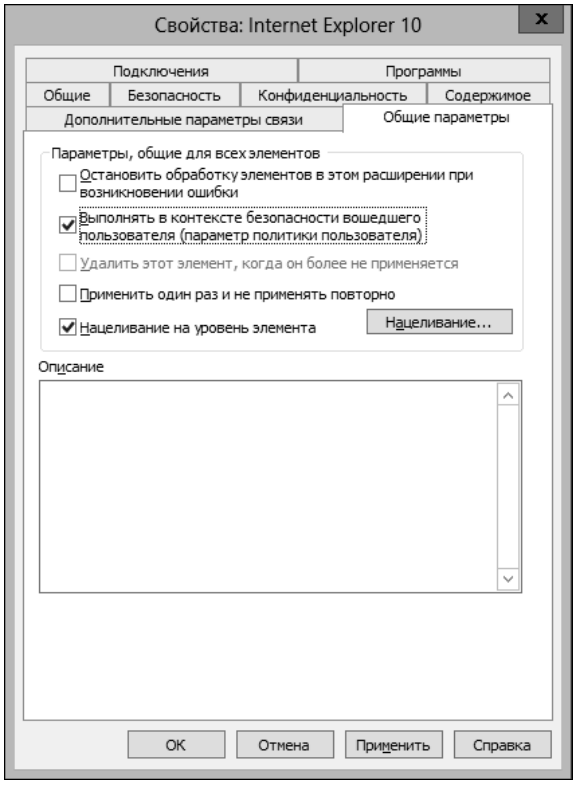


Рис. 6.6. Пример вкладки общих параметров элементов предпочтения

- **Удалить этот элемент, когда он более не применяется** (Remove this item when it is no longer applied). По умолчанию параметры политики объекта групповой политики, которые больше не применяются к пользователю или компьютеру, удаляются, т. к. они больше не установлены в области групповой политики реестра. В отличие от параметров политики, элементы предпочтения не удаляются автоматически по завершению применения к компьютеру объекта групповой политики. Это поведение можно изменить, установив данный флажок (если он доступен). Когда этот флажок установлен, расширение предпочтения определяет, продолжает ли данный элемент предпочтений находиться в области видимости. Если элемент предпочтения находится вне области видимости, расширение предпочтения удаляет параметр, связанный с данным элементом предпочтения.

Практический совет

Обычно предпочтения, которые поддерживают действия управления, можно удалить, когда они больше не применяются, но предпочтения, которые поддерживают состояния редактирования, удалить нельзя. При установке флажка **Удалить этот элемент, когда он более не применяется** задается действие управления **Заменить**. В результате при обработке групповой политикой расширение предпочтения выполняет операцию **Удалить**, а затем операцию **Создать**. После

этого, если элемент предпочтения покинул область видимости (т. е. он больше не применяется) для пользователя или компьютера, результаты элемента предпочтения удаляются (но не создаются снова). Нацеливание на уровень элемента также может вызвать выход элемента предпочтения из области видимости.

- **Применить один раз и не применять повторно** (Apply once and do not reapply). Групповая политика сохраняет предпочтения в той же области реестра, которая используется приложением или функциональностью операционной системы для хранения связанных параметров. В результате пользователи могут изменять параметры, заданные администратором посредством предпочтений. Но, по умолчанию, результаты элементов предпочтений перезаписываются при каждом обновлении групповой политики, чтобы обеспечить применение элементов предпочтений согласно назначению администратора. Установка данного флажка изменяет это поведение — теперь расширение предпочтений применяет результаты элемента предпочтений только один раз и больше не повторяет применение.
- **Нацеливание на уровень элемента** (Item-level targeting). Данный параметр позволяет использовать фильтр для элемента предпочтения, чтобы он применялся только к определенным пользователям или компьютерам. Когда клиент групповой политики выполняет оценку цели предпочтения, каждый целевой элемент оценивается как `True` (Истина) или `False` (Ложь).

  Если результат равен `True`, элемент предпочтения применяется и обрабатывается. В противном случае элемент предпочтения не применяется и не обрабатывается. При выборе этой опции нажмите кнопку **Нацеливание** (Targeting) и в открывшемся окне **Редактор нацеливания** (Targeting Editor) выполните настройку требуемого нацеливания.

Практический совет

Элементы нацеливания оцениваются в виде логического выражения. Такое логическое выражение может содержать переменные среды при условии, что они доступны в текущем контексте пользователя. После создания логического выражения необходимо проверить, что оно имеет смысл. Кроме этого, если вместо переменной среды жестко закодировать значение, нацеливание не будет работать так, как вы ожидаете.

ГЛАВА 7

Управление доступом пользователя и безопасностью

В сетевом отношении, компьютеры под Windows 8 можно настроить на членство в домашних группах, рабочих группах или доменах. Когда рабочая станция настроена на членство в домашней или рабочей сетевой группе, доступ пользователя и параметры безопасности также настраиваются локально на этой рабочей станции. А на рабочей станции, являющейся членом домена, доступ пользователя и параметры безопасности настраиваются на двух уровнях: на уровне локальной системы и на уровне домена. Доступ пользователя можно настроить на уровне локальной системы для конкретного компьютера, а на уровне домена — для нескольких систем или ресурсов по всему текущему лесу службы каталогов Active Directory.

В этой главе мы рассмотрим управление доступом к локальной системе и локальным учетным записям. Информацию по настройке доменного доступа и разрешений см. в книге "Windows Server 2012 Pocket Consultant". Следует иметь в виду, что для выполнения задач, рассматриваемых в этой книге, вход в систему можно выполнить локально или же посредством подключения к удаленному рабочему столу.

Пользовательские и групповые учетные записи

В операционной системе Windows 8 применяются как пользовательские, так и групповые учетные записи. Пользователи могут быть членами групповых учетных записей. Пользовательские учетные записи предназначены для предоставления доступа к системе отдельным лицам, а групповые учетные записи, которые обычно называются просто *группами*, служат для упрощения управления несколькими пользователями. Вход в систему можно выполнить с учетной записью пользователя, но не с учетной записью группы.

В Windows 8 определены два основных типа учетных записей пользователя.

- **Локальные учетные записи пользователя.** Это учетные записи пользователя, которые определены на локальном компьютере. Они предоставляют доступ только к локальному компьютеру. Управлять локальными учетными записями пользователя можно с помощью опций страницы **Учетные записи пользователей** (User Accounts), доступной из Панели управления, или посредством оснастки консоли MMC **Локальные пользователи и группы** (Local Users and Groups), доступной в узле **Служебные программы** (System Tools) утилиты **Управление компьютером** (Computer Management).
- **Доменные учетные записи пользователей.** Это учетные записи пользователей, определенные в службе каталогов Active Directory. Выполнив вход с помощью такой учетной

записи, можно обращаться к ресурсам по всему лесу. Компьютер, который является членом Active Directory, можно использовать для создания доменных учетных записей, используя оснастку консоли MMC **Active Directory — пользователи и компьютеры** (Active Directory Users and Computers). Чтобы эта оснастка была доступна, на компьютер необходимо установить средства RSAT. После этого консоль с данной оснасткой можно запустить, выбрав в меню **Средства** (Tools) утилиты **Диспетчер серверов** (Server Manager) команду **Пользователи и компьютеры Active Directory**.

И локальные, и доменные учетные записи пользователей можно определить как учетные записи обычного пользователя или как администратора. Обычная учетная запись на локальном компьютере имеет ограниченные права, а учетная запись администратора — расширенные права.

В Windows 8 добавлена специальная локальная учетная запись, называющаяся *учетной записью Microsoft* (Microsoft account), которой не было в предыдущих версиях Windows. Эту учетную запись можно рассматривать, как синхронизированные локальную и онлайновую учетные записи. Принцип работы этой записи такой:

- пользователь выполняет вход в систему, используя в качестве имени пользователя адрес электронной почты и пароль своей онлайновой учетной записи Microsoft;
- применение для входа в систему онлайновой учетной записи Microsoft предоставляет пользователю возможность использовать разные подключенные функциональности этой учетной записи.

Синхронизация учетной записи позволяет пользователю приобретать приложения и другое содержимое для своего компьютера в магазине Windows Store. Этот метод входа в систему обеспечивает доступ к синхронизированному содержимому (файлам, фотографиям и т. п.), а также определенным параметрам профиля, хранящимся на файловом хостинге SkyDrive, при входе с его использованием на любой компьютер под управлением Windows 8. Синхронизация содержимого компьютеров позволяет организовать непрерывность рабочей среды, независимо от того, на каком компьютере пользователи выполнят вход в систему. В остальном синхронизованные учетные записи работают точно таким же образом, как и обычные учетные записи.

В любое время обычную учетную запись можно преобразовать в учетную запись Microsoft, а учетную запись Microsoft — в обычную учетную запись.

Практический совет

Нежелательно разрешать пользователям создавать учетную запись Microsoft или входить в систему с ее использованием на корпоративных компьютерах. В таком случае учетные записи Microsoft можно заблокировать с помощью групповой политики **Учетные записи: блокировать учетные записи Майкрософт**, которая находится в узле **Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики\Параметры безопасности** (Computer Configuration\Windows Configuration\Security Settings\Local Policies\Security Options). Чтобы запретить пользователям создавать учетные записи Microsoft, установите в окне свойств этой политики флажок **Определить следующий параметр политики** и выберите в списке значение **Пользователи не могут добавлять учетные записи Майкрософт** (Users can't add Microsoft accounts), а чтобы запретить пользователям создавать учетные записи Microsoft и выполнять вход в систему под ними, выберите значение **Пользователи не могут добавлять учетные записи Майкрософт и использовать их для входа** (Users can't add or log on with Microsoft accounts).

Основы учетных записей пользователей

Все учетные записи пользователей отождествляются с *именем входа* (logon name). В Windows 8 имя входа состоит из двух частей:

- **имя пользователя** — отображаемое в учетной записи имя;
- **имя компьютера или домена пользователя** — имя компьютера или домена, в котором действует учетная запись пользователя.

Например, полное имя входа для пользователя `WilliamS`, учетная запись которого создана на компьютере `ENGPC85`, будет `ENGPC85\WilliamS`. Имея локальную учетную запись, пользователь `WilliamS` может входить на локальную рабочую станцию и обращаться к локальным ресурсам. Доступа к доменным ресурсам у него не будет.

При создании учетной записи Microsoft операционная система Windows 8 использует для имени входа предоставляемую пользователем информацию. Имя и фамилия пользователя используются, как часть отображаемой на экране информации, а в качестве имени входа берется полный адрес электронной почты, будучи информацией, которая хранится на локальном компьютере. Когда пользователь выполняет вход на компьютере, который подключен к Интернету, содержимое и настройки пользователя можно синхронизировать и обновить в соответствии с его предпочтениями. Если же компьютер не подключен к Интернету, содержимое и настройки пользователя берутся из его профиля, как и в случае входа с обычной учетной записью.

При работе в доменах полное имя входа можно представить двумя разными способами:

- имя учетной записи пользователя и полное имя домена, разделенные символом @. Например, полное имя входа для пользователя `Williams` в домене `technology.microsoft.com` будет `Williams@technology.microsoft.com`;
- имя учетной записи пользователя и имя домена, разделенные символом обратной косой черты — \. Например, полное имя входа для пользователя `Williams` в домене `technology` будет `technology\Williams`.

Хотя в Windows 8 при описании прав и привилегий учетной записи отображается имя пользователя, ключевыми идентификаторами учетных записей являются идентификаторы безопасности SID (Security Identifier). Однозначные идентификаторы SID генерируются при создании участников системы безопасности (security principal). Каждый идентификатор SID состоит из префикса, являющегося идентификатором безопасности компьютера или домена, и однозначного относительного идентификатора пользователя. Операционная система Windows 8 использует эти идентификаторы для отслеживания учетных записей и имен пользователей независимо друг от друга. Идентификаторы SID применяются для разных целей, но основными являются две из них. А именно предоставить легкий способ как для изменения имен пользователей, так и для удаления учетных записей, не беспокоясь при этом, что кто-то сможет получить доступ к ресурсам, просто снова создав удаленную учетную запись.

При изменении имени пользователя Windows 8 сопоставляет данный идентификатор SID с новым именем. При удалении учетной записи Windows 8 знает, что соответствующий идентификатор SID больше не является действительным. Поэтому, даже если снова создать учетную запись с таким же именем пользователя, как и удаленная, новая учетная запись не будет обладать такими же правами и разрешениями, как удаленная, потому что у нее будет другой идентификатор SID.

С учетными записями пользователей также связаны пароли и сертификаты. Пароль представляет собой строку аутентификации для учетной записи, а сертификаты используют секретный и открытый ключи для идентификации пользователя. Вход с паролем выполняется интерактивно, а при входе с помощью сертификата используется секретный ключ, который хранится на смарт-карте и считывается соответствующим устройством.

При установке Windows 8 операционная система устанавливает несколько встроенных учетных записей, назначение которых подобно учетным записям, создаваемым в доменах Windows. Основными встроенными учетными записями являются следующие.

- **Администратор.** Стандартная учетная запись, которая предоставляет полный доступ к файлам, папкам, службам и другим функциональностям. Эту учетную запись нельзя ни удалить, ни отключить. На компьютерах-членах Active Directory учетная запись **Администратор** обладает правами и разрешениями по всему домену. На локальной машине права и разрешения этой учетной записи распространяются только на локальную систему.
- **Гость.** Эта учетная запись предназначена для пользователей, которым требуется одноразовый или периодический доступ к компьютеру. Хотя эта учетная запись обладает ограниченными правами и разрешениями, нужно быть очень осторожным в ее использовании, т. к. это делает систему уязвимой к возможным проблемам безопасности. Более того, риск настолько велик, что эта учетная запись по умолчанию отключена.

По умолчанию эти две учетные записи являются членами разных групп. Прежде чем изменять любую из встроенных учетных записей, следует записать ее стандартные параметры свойств и членства в группах. Членство в группе предоставляет или ограничивает доступ учетной записи к определенным системным ресурсам. Например, **Администратор** является членом группы **Администраторы**, а **Гость** — членом группы **Гости**. Членство в группе позволяет учетной записи использовать права и разрешения данной группы.

Кроме встроенных учетных записей, Windows 8 имеет несколько псевдоучетных записей, которые применяются для выполнения специфических системных операций. Псевдоучетные записи имеются только на локальных системах. Настройки этих учетных записей нельзя редактировать с помощью инструментов управления пользователями; также эти учетные записи нельзя использовать для входа в систему. К псевдоучетным относятся следующие записи.

- **LocalSystem.** Применяется для исполнения системных процессов и обработки заданий системного уровня. Эта учетная запись предоставляет право входа в качестве службы (Log on as a service). С учетной записью **LocalSystem** исполняется большинство служб. В некоторых случаях эти службы имеют право взаимодействия с рабочим столом. Службы, для которых требуется меньше разрешений или прав входа, исполняются с учетной записью **LocalService** или **NetworkService**. С учетной записью **LocalSystem** исполняются, среди прочих, следующие службы:
  - **Фоновая интеллектуальная служба передачи** (Background Intelligent Transfer Service, BITS);
  - **Обозреватель компьютеров** (Computer Browser);
  - **Клиент групповой политики** (Group Policy Client);
  - **Сетевой вход в систему** (Netlogon);
  - **Сетевые подключения** (Network Connections);
  - **Диспетчер печати** (Print Spooler);
  - **Служба профилей пользователей** (User Profile Service).
- **LocalService.** Эта учетная запись применяется для исполнения служб, которым требуются меньшие разрешения и права входа на локальной системе. По умолчанию исполняющиеся с этой учетной записью службы имеют право входа в качестве службы (Log on as a service), а также обладают разрешениями **Настройка квот памяти для процесса** (Adjust memory quotas for a process), **Обход перекрестной проверки** (Bypass traverse checking), **Изменение системного времени** (Change the system time), **Изменение часо-**

вого пояса (Change the time zone), **Создание глобальных объектов** (Create global objects), **Создание аудитов безопасности** (Generate security audits), **Имитация клиента после проверки подлинности** (Impersonate a client after authentication) и **Замена маркера уровня процесса** (Replace a process level token). С учетной записью **LocalService** исполняются, среди прочих, следующие службы:

- **Служба шлюза уровня приложения** (Application Layer Gateway Service);
- **Удаленный реестр** (Remote Registry);
- **Смарт-карта** (Smart Card);
- **Обнаружение** SSDP (SSDP Discovery Service);
- **Модуль поддержки NetBIOS через TCP/IP** (TCP/IP NetBIOS Helper);
- **Веб-клиент** (WebClient).

♦ **NetworkService.** Эта учетная запись используется для исполнения служб, для которых требуется меньше привилегий и прав входа на локальной системе, но которым также необходимо иметь доступ к сетевым ресурсам. Подобно службам, исполняющимся с учетной записью **LocalService**, по умолчанию службы, исполняющиеся с учетной записью **NetworkService**, имеют право входа в качестве службы (Log on as a service), а также обладают разрешениями **Настройка квот памяти для процесса** (Adjust memory quotas for a process), **Обход перекрестной проверки** (Bypass traverse checking), **Создание глобальных объектов** (Create global objects), **Создание аудитов безопасности** (Generate security audits), **Имитация клиента после проверки подлинности** (Impersonate a client after authentication) и **Замена маркера уровня процесса** (Replace a process level token). С учетной записью **NetworkService** исполняются, среди прочих, следующие службы:

- **BranchCache**;
- **Координатор распределенных транзакций** (Distributed Transaction Coordinator);
- **DNS-клиент** (DNS Client);
- **Службы удаленных рабочих столов** (Remote Desktop Services);
- **Удаленный вызов процедур (RPC)** (Remote Procedure Call (RPC)).

Учетная запись **NetworkService** также может представляться удаленным системам, как учетная запись компьютера.

Основы учетных записей групп

Операционная система Windows 8 также содержит группы, которые используются для предоставления разрешений пользователям однородного типа и для упрощения администрирования учетных записей. Если пользователь является членом группы, которая имеет право доступа к определенному ресурсу, этот пользователь также имеет доступ к этому ресурсу. Пользователю можно дать права доступа к разным ресурсам, связанным с его работой, просто сделав его членом соответствующей группы. Следует иметь в виду, что в отличие от учетной записи пользователя, выполнить вход в систему с учетной записью группы нельзя. Так как группы разных доменов Active Directory или локальных компьютеров могут иметь одинаковые имена, названия им обычно даются в формате *Домен\ИмяГруппы* или *Компьютер\ИмяГруппы*. Например: *Technology\GMarketing* для группы *GMarketing* в домене или на компьютере *Technology*.

В Windows 8 используются следующие три типа групп.

♦ **Локальные группы.** Определяются на локальном компьютере и используются исключительно на нем. Локальные группы можно создавать в узле **Локальные пользователи и группы** утилиты **Управление компьютером**.

- **Группы безопасности** (Security Groups). Эти группы могут иметь связанные с ними дескрипторы безопасности. Группы безопасности определяются в доменах с помощью оснастки консоли MMC **Active Directory — пользователи и компьютеры**.
- **Группы распространения** (Distribution Groups). Используются в качестве списков рассылки сообщений электронной почты. Эти группы не могут иметь связанные с ними дескрипторы безопасности. Группы распространения определяются в доменах с помощью оснастки консоли MMC **Active Directory — пользователи и компьютеры**.

Подобно учетным записям пользователей, для отслеживания учетных записей групп используются однозначные идентификаторы SID. Это означает, что не следует ожидать от воссозданной удаленной учетной записи группы те же разрешения и привилегии, как и у прежней группы. Такая новая группа будет иметь новый идентификатор SID, и все разрешения и привилегии старой группы будут утеряны.

При назначении пользователю уровня доступа его можно сделать членом встроенной или предопределенной группы, включая следующие.

- **Операторы помощи по контролю учетных записей** (Access control assistance operators). Члены этой группы могут удаленно запрашивать атрибуты авторизации и разрешения для ресурсов на данном компьютере.

> ***Примечание***
>
> Операционная система Windows имеет несколько групп операторов. По умолчанию никакая учетная запись группы или пользователя не является членом групп операторов. Цель этого ограничения — обеспечить явное предоставление доступа группам операторов.

- **Администраторы** (Administrators). Членами этой группы являются администраторы локальной машины, которые имеют полный доступ ко всем ее ресурсам. Они могут создавать и удалять учетные записи, изменять членство в группах, устанавливать принтеры, управлять общими ресурсами и многое другое. Так как эта учетная запись предоставляет полный доступ к компьютеру, следует быть осторожным при предоставлении членства в ней.
- **Операторы архива** (Backup Operators). Члены этой группы могут выполнять резервное копирование и восстановление файлов и папок рабочей станции. Они могут выполнять вход в систему, осуществлять резервное копирование и восстановление, выключать компьютер. Особенности настройки этой учетной записи позволяют ее членам выполнять резервное копирование файлов независимо от того, имеют ли они доступ для чтения и записи этих файлов. Но они не могут изменять разрешения доступа файлов или выполнять другие административные задания.
- **Криптографические операторы** (Cryptographic Operators). Члены этой группы могут управлять настройкой шифрования, IP-безопасностью (IPSec), цифровыми удостоверениями и сертификатами.
- **Читатели журнала событий** (Event Log Readers). Члены могут просматривать журналы событий на локальном компьютере.
- **Гости** (Guests). Гости являются пользователями с очень ограниченными привилегиями. Члены этой группы могут осуществлять удаленный доступ к системе и ее ресурсам, но не могут выполнять большинства других заданий.
- **Администраторы Hyper-V** (Hyper-V Administrators). Члены этой группы могут управлять всеми возможностями Hyper-V[1]. Windows 8 имеет встроенные технологии виртуа-

[1] Система виртуализации для *x*64-систем на основе гипервизора.

лизации, поддерживаемые на 64-разрядном оборудовании с возможностью преобразования адресов второго уровня (SLAT[1]).

- **Операторы настройки сети** (Network Configuration Operators). Члены этой группы могут управлять параметрами сети на рабочей станции. Им также разрешено настраивать параметры протоколов TCP/IP и выполнять другие общие задачи по настройке сети.
- **Пользователи журналов производительности** (Performance Log Users). Члены могут просматривать и управлять счетчиками производительности, а также управлять протоколированием производительности.
- **Пользователи системного монитора** (Performance Monitor Users). Члены могут просматривать счетчики и журналы производительности.
- **Опытные пользователи** (Power Users). В предыдущих версиях Windows эта группа применялась для предоставления дополнительных привилегий, таких как возможность изменять настройки компьютера и устанавливать программы. В Windows 8 эта группа оставлена только для обратной совместимости с наследуемыми приложениями.
- **Пользователи удаленного рабочего стола** (Remote Desktop Users). Члены этой группы могут выполнять удаленный вход в систему посредством служб удаленного рабочего стола. После входа в систему их разрешения в ней определяются их членством в дополнительных группах. Пользователям, которые являются членами группы **Администраторы**, эта привилегия дается автоматически. (Но для удаленного входа в систему эта возможность должна быть включена на удаленном компьютере.)
- **Пользователи удаленного управления** (Remote Management Users). Члены имеют доступ к WMI-ресурсам по протоколам управления.
- **Репликатор** (Replicator). Члены этой группы могут управлять репликацией файлов для локального компьютера. Репликация файлов в основном применяется с доменами Active Directory и серверами Windows.
- **Пользователи** (Users). Пользователи выполняют большинство своей работы на одной рабочей станции под управлением Windows 8. Члены этой группы имеют больше ограничений, чем полномочий. Они могут выполнять локальный вход на рабочую станцию Windows 8, содержать локальный профиль, блокировать и выключать рабочую станцию.
- **WinRMRemoteWMIUsers.** Члены могут обращаться к WMI-ресурсам посредством удаленного управления Windows.

В большинстве случаев настройка доступа пользователей выполняется с помощью группы **Пользователи** или **Администраторы**. Предоставить уровень доступа пользователя и администратора можно, задав тип учетной записи, как **Стандартная** или **Администратор** соответственно. Хотя эти базовые задания можно выполнять, используя опции окна **Учетные записи пользователей**, доступного из Панели управления, пользователя можно сделать членом группы в узле **Локальные пользователи и группы** утилиты **Управление компьютером**.

Доменный и локальный вход в систему

На компьютерах, являющихся членами домена, для выполнения входа в систему и домен обычно применяются доменные учетные записи. Все администраторы в домене имеют доступ к ресурсам локальных рабочих станций, являющихся членами домена, пользователи же имеют доступ только к ресурсам локальных рабочих станций, на которые они могут вхо-

[1] Second Level Address Translation.

дить. В домене любой пользователь, имеющий действительную доменную учетную запись, может по умолчанию выполнять вход в систему на любом компьютере, являющемся членом домена. Выполнив вход в систему, пользователь имеет доступ ко всем ресурсам, правами на доступ к которым обладает его учетная запись или учетная запись группы, членом которой он является, непосредственно или косвенно, через доступ на основе утверждений (claims-based access). Это включает как ресурсы локальной машины, так и ресурсы домена.

Доступные для выполнения входа в систему рабочие станции домена можно ограничить на индивидуальной основе с помощью оснастки консоли MMC **Active Directory — пользователи и компьютеры**. Для этого в данной оснастке нужно щелкнуть правой кнопкой мыши на учетной записи требуемого пользователя и в контекстном меню выбрать команду **Свойства**. В открывшемся диалоговом окне свойств учетной записи следует перейти на вкладку **Учетная запись**, нажать на ней кнопку **Вход на** (Log on to), в открывшемся диалоговом окне **Рабочие станции для входа в систему** (Logon Workstations) установить переключатель **только на указанные компьютеры** (only on the specified computers), а затем добавить компьютеры, с которых данный пользователь может выполнять вход в систему.

Практический совет

Не путайте рабочие станции, разрешенные для входа в систему, с основными компьютерами (primary computers). Основные компьютеры относятся к политике **Перенаправлять папки только на основные компьютеры** (Redirect folders on primary computers only), которая находится в узле **Конфигурация компьютера\Административные шаблоны\Система\Перенаправление папок** (Computer configuration\Administrative templates\System\Folder Redirection). Эта политика позволяет администраторам указать, с каких компьютеров пользователи могут иметь доступ к перемещаемым профилям и перенаправляемым папкам. Целью этой политики является защита личных и корпоративных данных, когда пользователи входят в систему с иных компьютеров, чем те, которые они обычно используют для работы. Безопасность данных повышается вследствие того, что такие данные не загружаются и не кэшируются на компьютере, который не применяется пользователем на его обычном рабочем месте. В контексте этой политики, *основной компьютер* — это компьютер, который специально разрешено использовать с перенаправленными данными. Такое разрешение выполняется посредством редактирования дополнительных свойств пользователя или группы в каталоге Active Directory и присвоения свойству `msDS-PrimaryComputer` имен компьютеров, которым предоставляется разрешение.

Но при работе с Windows 8 вход в систему не всегда сопровождается входом в домен. На компьютерах, принадлежащих к рабочим группам, вход можно выполнять только в учетную запись пользователя. Кроме этого, для администрирования доменного компьютера может потребоваться выполнить в нем локальный вход в систему. Локальный вход в систему могут выполнять только пользователи, у которых есть локальная учетная запись. При локальном входе в систему пользователь получает доступ ко всем ресурсам компьютера, на которые предоставлены права его учетной записи или группы, к которой принадлежит его учетная запись.

Управление контролем учетных записей пользователей и запросами на повышение прав

Функциональность контроля учетных записей пользователей определяет права пользователей стандартных учетных записей и пользователей учетных записей администратора, обстоятельства установки и выполнения приложений и многие другие аспекты. В этом разделе данная функциональность обсуждается более подробно, чем в *главе 1*, а также всесторонне рассматривается влияние, оказываемое контролем учетных записей пользователей на учетные записи стандартных пользователей и администраторов. Эта информация представляет особую важность для управления системами с Windows 8.

Примечание

Изучение работы контроля учетных записей пользователей поможет вам стать лучшим администратором. Чтобы обеспечить работу этой функциональности, пришлось переделать многие аспекты операционной системы Windows. Некоторые из самых важных модификаций затронули особенности установки и выполнения приложений. Влияние архитектурных изменений на выполнение программ в Windows 8 всесторонне рассматривается в *главе 8*.

Переопределение учетных записей стандартных пользователей и администраторов

В Windows XP и более ранних версиях Windows вредоносные программы могли пользоваться тем обстоятельством, что большинство пользовательских учетных записей настраиваются, как члены группы администраторов локального компьютера. Эти повышенные привилегии позволяют вредоносным программам не только устанавливать себя на компьютере, но также выполнять на компьютере практически какие угодно действия, т. к. установленные администратором программы могут изменять защищенные области реестра и файловой системы.

Чтобы бороться с возрастающей угрозой вредоносных программ, организации закрыли компьютеры, образно говоря, на замок, требуя, чтобы пользователи входили в систему под стандартными учетными записями. А администраторам нужно было запускать утилиты для администрирования системы, используя опцию **Запуск от имени администратора** (Run as...). К сожалению, эти изменения процедуры могут оказать серьезный отрицательный эффект на производительность. Пользователь, вошедший в систему Windows XP по стандартной учетной записи, не может выполнять многих самых простых задач, таких как перевод системных часов и календаря, изменение часового пояса компьютера или изменение параметров управления электропитанием. Многие программы для Windows XP просто не будут работать должным образом без локальных прав администратора. Эти права им требуются, чтобы записывать данные в системные области при установке, а также в процессе штатной работы. Кроме этого, Windows XP не предупреждает наперед, когда для выполняемой задачи требуются права администратора.

Контроль учетных записей пользователей предназначен для улучшения удобства работы при одновременном повышении безопасности, применяя новый подход к использованию стандартных и администраторских учетных записей. Контроль учетных записей пользователей улучшен в плане обеспечения безопасности вычислений, предоставляя инфраструктуру, которая ограничивает область, требующую прав администратора, и требует, чтобы все приложения исполнялись в специфичном пользовательском режиме. Таким образом, контроль учетных записей пользователей предотвращает непреднамеренные изменения пользователями системных настроек и блокирует компьютер, чтобы запретить установку несанкционированных приложений или выполнение вредоносных действий.

Вследствие применения контроля учетных записей пользователей в Windows 8 определены два типа учетных записей пользователя: стандартные учетные записи и учетные записи администратора. Также в Windows 8 определены два режима (уровня) выполнения приложений: режим стандартного пользователя и режим администратора. Пользователи стандартных учетных записей могут использовать большинство программного обеспечения и изменять системные параметры, которые не затрагивают других пользователей или безопасность компьютера. А пользователи учетных записей администратора имеют полный доступ к компьютеру и могут выполнять любые требуемые изменения. Когда администратор запускает приложение, к этому приложению применяются его маркер доступа и связанные с ним права администратора, что дает этому пользователю все права и привилегии ад-

министратора локального компьютера для данного приложения. Когда же приложение запускает стандартный пользователь, во время выполнения этого приложения к нему применяется маркер доступа этого пользователя и связанные с ним права, что ограничивает его права для данного приложения правами и привилегиями стандартного пользователя. Кроме этого, все приложения настроены на исполнение в специфическом режиме при установке. Все выполняемые приложением стандартного режима задания, для которых требуются разрешения административного режима, определяются при установке и для их выполнения требуется разрешение пользователя.

Стандартные учетные записи пользователей Windows 8 обладают набором прав на выполнение следующих действий:

- установка шрифтов, просмотр системных часов и календаря и изменение часового пояса;
- изменение настроек экрана и настроек управления электропитанием;
- добавление принтеров и других устройств (если требуемые драйверы установлены на компьютере или предоставляются ИТ-администратором);
- загрузка и установка обновлений (если обновления используют установщики, совместимые с контролем учетных записей пользователей);
- создание и настройка подключений виртуальных частных сетей (virtual private network, VPN). Подключения VPN используются для создания защищенных подключений к частным сетям через Интернет;
- установка протокола WEP[1] для подключения к защищенным беспроводным сетям. Протокол WEP обеспечивает улучшенную безопасность для беспроводных сетей;
- возможность доступа и выключение компьютера по сети.

В Windows 8 также определены два режима (уровня) выполнения приложений: режим стандартного пользователя и режим администратора. Windows 8 определяет необходимость повышенных прав для исполнения пользователями программ, снабжая большинство приложений и процессов маркером безопасности. Если приложение имеет стандартный маркер безопасности или если приложение не определено, как приложение администратора, для его исполнения не требуются права администратора, и Windows 8 по умолчанию запускает его как стандартное приложение. Если же приложение имеет маркер администратора, для его выполнения требуются повышенные привилегии; поэтому прежде чем выполнять приложение, Windows 8 выводит сообщение, требующее, чтобы пользователь подтвердил его запуск.

Процесс получения разрешения, прежде чем исполнять приложение в режиме администратора или выполнять задания, которые изменяют конфигурацию системы, называется *повышением привилегий* (elevation). Повышение привилегий улучшает безопасность системы и уменьшает возможность отрицательных эффектов вредоносных программ посредством извещения пользователей о любых выполняемых ими действиях, которые могут повлиять на настройки системы, прежде чем выполнять эти действия, не допуская использования приложениями привилегий администратора без предварительного извещения об этом пользователей. Повышение привилегий также защищает администраторские приложения от атак стандартными приложениями. Дополнительную информацию по повышению привилегий и по особенностям работы контроля учетных записей пользователя *см. в главе 8.*

По умолчанию, прежде чем выводить запрос на повышение привилегий, Windows 8 переходит в режим безопасного рабочего стола. Безопасный рабочий стол изолирован от всех дру-

[1] Wired Equivalent Privacy — протокол шифрования в беспроводной связи.

гих программ и процессов, исполняющихся на компьютере, таким образом снижая шансы вредоносной программы или пользователя получить доступ к процессу, для которого повышаются права. Применение безопасного рабочего стола при выводе запроса на повышение прав можно отключить, используя вместо него стандартный рабочий стол, но это делает компьютер более уязвимым к успешным атакам вредоносного кода.

Оптимизация контроля учетных записей пользователей и режима одобрения администратором

Каждая операционная система Windows 8 имеет встроенную учетную запись администратора. Эта запись не защищается контролем учетных записей пользователей, и администрирование компьютера с этой учетной записи может быть небезопасным для компьютера. Чтобы защитить компьютеры в обстоятельствах, в которых локальная учетная запись администратора используется для администрирования компьютера, следует создать новую учетную запись администратора и использовать для администрирования компьютера именно ее.

Каждую учетную запись пользователя можно индивидуально настраивать или вообще отключить. При отключении средства контроля учетных записей пользователей теряется предоставляемая им дополнительная защита, и компьютер подвергается большему риску воздействия вредоносного кода. При отключении или включении контроля учетных записей пользователей компьютер необходимо перезапустить, чтобы выполненная настройка вступила в силу.

Ключевым компонентом контроля учетных записей пользователей является режим одобрения администратором (Admin Approval Mode), который определяет, выводить ли запрос на разрешение при запуске приложений администратора, и если выводить, то каким образом. По умолчанию режим одобрения администратором работает следующим образом:

- по умолчанию все учетные записи администраторов, включая встроенную учетную запись администратора, работают в режиме одобрения администратором и подлежат условиям этого режима;
- по этой причине, для всех администраторов при попытке запуска приложения администратора выводится запрос на повышение прав.

Пользователи, вошедшие в систему с учетной записью администратора, могут изменить особенности работы контроля учетных записей пользователей для всех пользователей, выполнив следующие шаги:

1. В Панели управления щелкните мышью по ссылке категории **Система и безопасность**. В разделе **Центр поддержки** щелкните по ссылке **Изменение параметров контроля учетных записей** (Change User Account Control settings).
2. В открывшемся окне **Параметры управления учетными записями пользователей** (User Account Control Settings) (рис. 7.1) с помощью ползунка укажите одну из четырех опций извещения. Краткое описание этих опций приводится в табл. 7.1.

Режимом одобрения администратором и запросами на повышение прав можно управлять посредством установки соответствующих параметров групповой политики **Параметры безопасности**, расположенной в узле **Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики**. Далее приводится описание основных параметров контроля учетных записей пользователей этой политики.

- **Контроль учетных записей: режим одобрения администратором для встроенной учетной записи администратора** (User Account Control: Use Admin Approval Mode for the built-in Administrator account). Определяет характеристики использования режима

Таблица 7.1. *Уведомления об изменении параметров компьютера*

Опция	Описание	Когда использовать	Используется безопасный рабочий стол?
Всегда уведомлять	Всегда уведомлять текущего пользователя, когда программы пытаются установить программное обеспечение или внести изменения в компьютер либо когда пользователь изменяет параметры Windows	Эту опцию следует устанавливать в тех случаях, когда для компьютера требуется наивысший возможный уровень безопасности и пользователи часто устанавливают программное обеспечение и посещают незнакомые сайты	Да
По умолчанию	Уведомлять текущего пользователя, когда программы пытаются внести изменения в компьютер, но не когда пользователь изменяет параметры Windows	Эту опцию следует устанавливать в тех случаях, когда для компьютера требуется высокий уровень безопасности, а также когда необходимо уменьшить количество уведомлений, выводимых пользователям	Да
Уведомлять только когда... (Не затемнять рабочий стол)	То же самое, что и опция **По умолчанию**, но не разрешает контролю учетных записей пользователей переключаться на безопасный рабочий стол	Эту опцию следует устанавливать в тех случаях, когда пользователи работают в доверяемой среде с известными приложениями и не посещают незнакомые веб-сайты	Нет
Никогда не уведомлять	Отключает все уведомления контроля учетных записей пользователей	Эту опцию следует устанавливать только в тех случаях, когда безопасность не является приоритетом, и пользователи работают в доверяемой среде с программами, которые не сертифицированы для Windows 8 по той причине, что они не поддерживают контроль учетных записей пользователей	Нет

одобрения администратором пользователями и процессами, исполняющимися по встроенной учетной записи администратора. По умолчанию этот параметр выключен, вследствие чего для встроенной локальной учетной записи администратора не применяется режим одобрения администратором и, как результат этого, не применяется процесс повышения полномочий, предусмотренный для администраторов в режиме одобрения администратором. Когда этот параметр отключен, пользователи и процессы, обладающие полномочиями встроенной учетной записи локального администратора, выполняют все приложения с полными привилегиями администратора.

- **Контроль учетных записей: разрешить UIAccess-приложениям запрашивать повышение прав, не используя безопасный рабочий стол** (User Account Control: Allow UIAccess applications to prompt for elevation without using the secure desktop). Определяет, могут ли UIAccess-приложения (UIA-программы) автоматически отключать безопасный рабочий стол для запросов на повышение прав, используемых обычным пользователем. Если этот параметр включен, UIA-программы, в том числе удаленный помощник Windows, могут автоматически отключать безопасный рабочий стол для запросов на повышение прав.

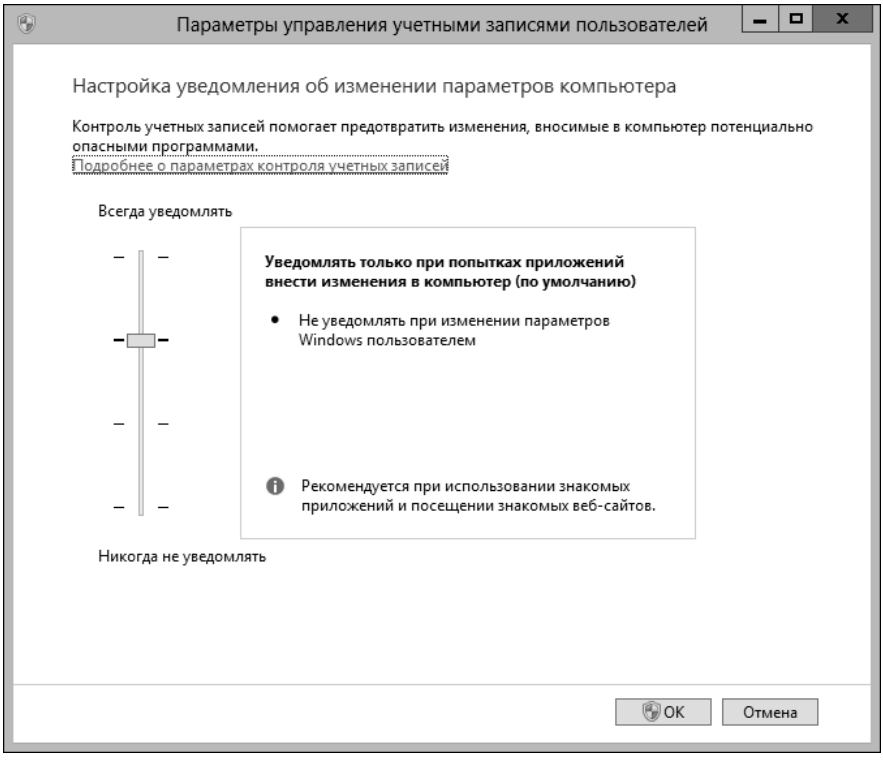


Рис. 7.1. Окно **Настройка уведомления об изменении параметров компьютера**

- **Контроль учетных записей: поведение запроса на повышение привилегий для администраторов в режиме одобрения администратором** (User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode). Определяет поведение запроса на повышение привилегий для администраторов, работающих в режиме одобрения администратором, а также особенности работы запроса на повышение привилегий. По умолчанию, при попытке исполнения администраторами приложений администрирования на безопасном рабочем столе, выводится запрос на разрешение выполнения приложения. Этот параметр можно настроить таким образом, чтобы выводился запрос: на разрешение выполнения приложения при работе в режиме безопасного стола; на предоставление учетных данных при работе в режиме безопасного стола или без этого режима (как в случае со стандартными пользователями); или на разрешение выполнения только для исполняемых файлов иных, нежели файлы Windows. Кроме того, данный параметр можно настроить, чтобы для администраторов не выводились никакие запросы; в таком случае повышение привилегий администратора выполняется автоматически. Независимо от значения этого параметра, администратор всегда может щелкнуть правой кнопкой мыши по значку приложения и в контекстном меню выбрать команду **Запуск от имени администратора** (Run as administrator).
- **Контроль учетных записей: поведение запроса на повышение привилегий для обычных пользователей** (User Account Control: Behavior of the elevation prompt for standard users). Определяет поведение запроса на повышение привилегий для обычных пользователей при попытке выполнения приложений администратора. По умолчанию, при попытке пользователей, вошедших в систему по учетной записи обычного пользователя, выполнить программу или какие-либо операции администрирования, на безопас-

ном рабочем столе выводится запрос на ввод учетных данных администратора. Этот параметр можно также настроить на вывод запроса параметров доступа на обычном, а не безопасном рабочем столе. Также можно задать автоматический отказ в повышении привилегий, когда пользователи не смогут повысить свои полномочия, предоставив параметры доступа администратора. Но установка последнего значения этого параметра не может помешать пользователю щелкнуть правой кнопкой мыши по значку приложения и в контекстном меню выбрать команду **Запуск от имени администратора** (Run as administrator).

- **Контроль учетных записей: повышение привилегий только для подписанных и проверенных исполняемых файлов** (User Account Control: Only elevate executable files that are signed and validated). Задает проверку подписей PKI[1] для любых интерактивных приложений, требующих повышения привилегий. Если этот параметр включен, повышение привилегий разрешается только для исполняемых файлов, которые успешно проходят проверку подписи и для которых имеются сертификаты в хранилище доверенных издателей локальных компьютеров. Этот параметр следует включать только в тех случаях, когда требуется наивысший уровень безопасности и все используемые приложения являются подписанными и проверенными.
- **Контроль учетных записей: повышать права только для UIAccess-приложений, установленных в безопасном местоположении** (User Account Control: Only elevate UIAccess applications that are installed in secure locations). Определяет, должны ли приложения, запрашивающие выполнение на уровне целостности UIAccess, находиться в безопасной папке файловой системы. Безопасными считаются только папки *%SystemRoot%*\Program Files, *%SystemRoot%*\Program Files (x86) и *%SystemRoot%*\Windows\System32.
- **Контроль учетных записей: все администраторы работают в режиме одобрения администратором** (User Account Control: Run all administrators in Admin Approval Mode). Определяет работу в режиме одобрения администратора всех пользователей, выполнивших вход в систему по учетной записи администратора. По умолчанию этот параметр включен, вследствие чего для учетных записей администраторов применяется режим одобрения администратором и, как результат этого, используется процесс запроса повышения полномочий, предусмотренный для администраторов в режиме одобрения администратором. Когда этот параметр отключен, к пользователям, выполнившим вход в систему по учетной записи администратора, не применяется режим одобрения администратором, и в результате этого к ним также не применяется процесс запроса повышения привилегий, предусмотренный для администраторов в режиме одобрения администратором.

> ***Практический совет***
>
> Связанные параметры контроля учетных записей для устройств рассматриваются в *главе 8*. Дополнительную информацию *см. в разд. "Оптимизация вывода запросов на повышение прав для виртуализации и установки" главы 8*.

В доменной среде требуемые параметры безопасности можно применять к определенному набору компьютеров с помощью групповой политики на основе службы каталогов Active Directory. Эти параметры также можно настраивать для отдельных компьютеров посредством локальной политики безопасности. Для этого нужно выполнить следующую процедуру:

1. Запустите редактор локальной групповой политики. Это можно сделать, выполнив команду `gpedit.msc` в поле поиска панели **Приложения** или в командной строке.

[1] Public Key Infrastructure — инфраструктура открытых ключей.

2. В дереве консоли последовательно разверните узлы **Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики** и выберите папку **Параметры безопасности** (рис. 7.2).

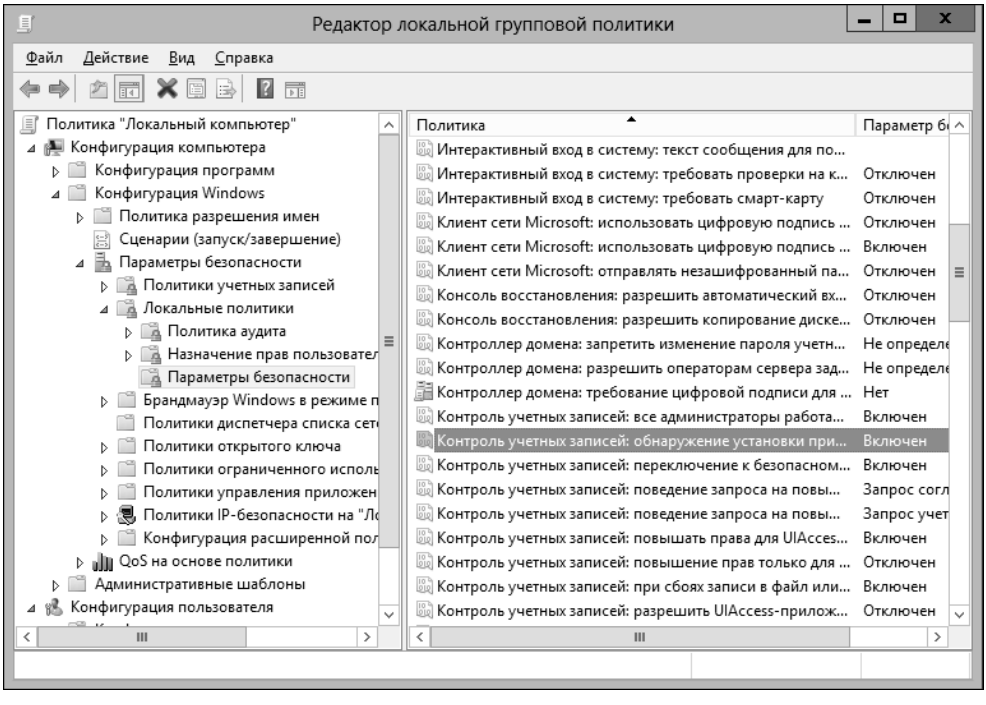


Рис. 7.2. Консоль локальной политики безопасности

3. Дважды щелкните мышью на необходимом параметре, настройте его требуемым образом и сохраните настройки, нажав кнопку **OK**. При необходимости повторите этот шаг для других параметров.

Управление локальным входом в систему

Все локальные учетные записи должны иметь пароль. Если учетная запись не снабжена паролем, она не имеет никакой защиты, и по такой учетной записи в систему может войти кто угодно. Но выполнить удаленный вход в систему по учетной записи без пароля нельзя.

Создание и работа с локальными учетными записями пользователей обсуждается в последующих разделах. Независимо от того, является ли компьютер членом домашней группы, рабочей группы или домена, он имеет локальные учетные записи.

Создание локальных учетных записей в домашней или рабочей группе

Операционная система Windows 8 поддерживает два основных типа локальных учетных записей пользователей: регулярные и синхронизированные. Для компьютера, который является членом домашней или рабочей группы, *регулярную учетную запись пользователя* можно создать следующим образом:

1. В разделе **Учетные записи пользователей и Семейная безопасность** (User Accounts and Family Safety) Панели управления щелкните по ссылке **Изменение типа учетной записи** (Change account type). Откроется окно **Управление учетными записями** (Manage Accounts) (рис. 7.3).

   В этом окне отображаются все настраиваемые учетные записи пользователей на локальном компьютере, упорядоченные по типу учетной записи и с указанием конфигурационной информации. Если учетная запись имеет пароль, она помечена как **Защищена паролем** (Password protected). Если учетная запись отключена, она обозначается соответствующим образом.

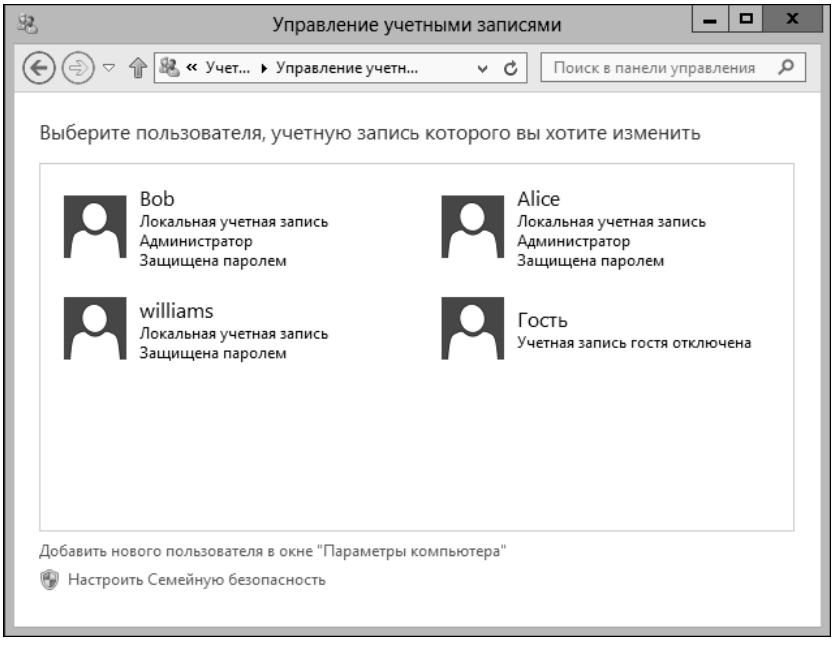


Рис. 7.3. Окно **Управление учетными записями** применяется для просмотра, редактирования и создания локальных учетных записей в рабочей или домашней группе

2. Щелкните по ссылке **Добавить нового пользователя в окне "Параметры компьютера"** (Add a new user In PC settings). В разделе **Другие пользователи** панели **Пользователи** открывшегося окна **Параметры** щелкните по ссылке **Добавить пользователя**. Откроется окно **Добавление пользователя**.
3. Если компьютер не подключен к Интернету, установки для создания обычной локальной учетной записи будут заданы по умолчанию. В противном случае нужно щелкнуть по ссылке **Вход без учетной записи Майкрософт** (Sign in without a Microsoft account).
4. На следующей странице нажмите кнопку **Локальная учетная запись** (Local account). (Этот шаг отсутствует на компьютерах, не подключенных к Интернету.)
5. На следующей странице введите в соответствующее поле имя локальной учетной записи и, дополнительно, пароль, подтверждение пароля и подсказку для пароля.
6. Нажмите кнопку **Далее**, а затем — кнопку **Готово**. По умолчанию создается стандартная учетная запись. Чтобы предоставить пользователю все полномочия на локальном компьютере, нужно изменить тип его учетной записи на администратора. Эта операция рассматривается в *разд. "Изменение типа локальной учетной записи" далее в этой главе.*

Синхронизированная учетная запись — это учетная запись Microsoft. Для компьютера, который является членом домашней или рабочей группы, учетную запись Microsoft можно создать следующим образом:

1. Откройте окно **Параметры компьютера**. Один из способов сделать это — нажать комбинацию клавиш <Windows>+<I> и внизу открывшейся панели **Параметры** щелкнуть по ссылке **Изменение параметров компьютера**.
2. В панели **Пользователи** щелкните по ссылке **Добавить пользователя** и создайте учетную запись Microsoft, следуя выводимым инструкциям.
3. Чтобы создать учетную запись Microsoft, компьютер должен быть подключен к Интернету. В процессе создания этой учетной записи Windows 8 подключается к магазину Microsoft Store, чтобы проверить наличие учетной записи для указанного адреса электронной почты. Если учетная запись еще не была создана, предлагается создать ее. Для этого на следующей странице для предоставленного адреса электронной почты нужно ввести пароль, фамилию и имя пользователя, страну или регион, а затем нажать кнопку **Далее**.
4. На следующей странице необходимо ввести информацию для контроля безопасности, включая дату рождения, номер телефона и/или запасной адрес электронной почты для отправки кода для сброса пароля, а также секретный вопрос и ответ на него для удостоверения личности владельца учетной записи в случае необходимости. Предоставив требуемую информацию, снова нажмите кнопку **Далее**.
5. На следующей, последней странице нужно ввести символы защиты от ботов (CAPTCHA-тест). После нажатия кнопки **Готово** на этой странице создается как онлайновая, так и локальная учетная запись Microsoft.

> ***Примечание***
>
> На компьютере, который не подключен к Интернету, при попытке создать учетную запись Microsoft можно будет создать только локальную учетную запись. Затем при подключении компьютера к Интернету нужно будет войти в систему по этой учетной записи, открыть панель **Пользователь** в окне **Настройки компьютера**, щелкнуть по ссылке **Переключиться на учетную запись Майкрософт** (Switch to a Microsoft account) и далее выполнить вышеописанную процедуру по созданию учетной записи Microsoft.

Синхронизированная учетная запись позволяет синхронизировать настройки приложений, параметры настройки профиля и некоторое содержимое профиля между разными устройствами, на которые выполняется вход посредством данной учетной записи. Управление синхронизируемыми и несинхронизируемыми параметрами осуществляется посредством настроек в панели **Синхронизация параметров** окна параметров компьютера.

Предоставление доступа к существующей доменной учетной записи с целью разрешить локальный вход в систему

Пользователю, который имеет доменную учетную запись, можно разрешить выполнять локальный вход в систему посредством следующей процедуры:

1. В разделе **Учетные записи пользователей** Панели управления щелкните по ссылке **Изменение типа учетной записи**. Откроется диалоговое окно **Учетные записи пользователей** (рис. 7.4) В этом диалоговом окне перечислены все настраиваемые учетные записи пользователей на локальном компьютере, упорядоченные по домену и с указанием группы, к которой они принадлежат.

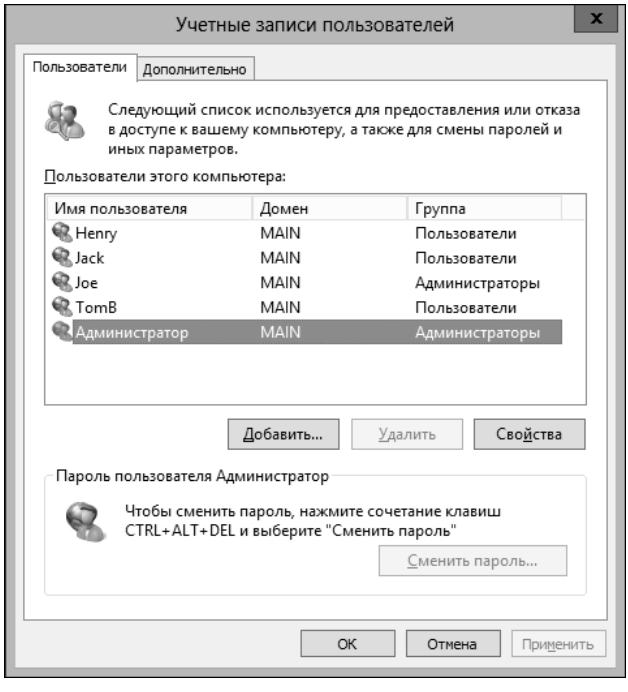


Рис. 7.4. Диалоговое окно **Учетные записи пользователей**

2. Чтобы добавить нового локального пользователя, нажмите кнопку **Добавить**. Будет запущен мастер добавления пользователя.
3. Мы создаем локальную учетную запись для пользователя, для которого уже есть доменная учетная запись. Введите в соответствующие поля имя доменной учетной записи пользователя и домен, членом которого он является; альтернативно, можно найти существующую доменную учетную запись, нажав кнопку **Обзор** и выбрав требуемого пользователя. Завершив выбор пользователя, нажмите кнопку **Далее**.
4. На следующей странице мастера укажите для добавляемого пользователя членство в локальной группе. Чтобы предоставить пользователю стандартные разрешения, установите переключатель **Стандартная**.
5. Учетная запись администратора создается с членством в локальной группе **Администраторы**. Чтобы предоставить пользователю полные права на локальном компьютере, установите переключатель **Администраторы**.
6. Учетная запись, для которой устанавливается переключатель **Другое**, обладает правами члена группы, выбранной из раскрывающегося списка.
7. Указав членство в локальной группе, нажмите в последующих окнах кнопки **Далее**, **Готово**, а затем **OK**. Повторите процедуру добавления для всех требуемых пользователей. По завершению добавления локальных пользователей закройте окно **Учетные записи пользователей**, нажав в нем кнопку **OK**. Чтобы изменить разрешения существующего локального пользователя или добавить пользователя в другие локальные группы, следуйте инструкциям, изложенным в *разд. "Управление локальными учетными записями и группами" далее в этой главе*.

Изменение типа локальной учетной записи

Тип локальной учетной записи пользователя можно изменить в окне **Учетные записи пользователей**. В частности, здесь можно задать учетную запись как стандартную или как администратора. Но для более расширенного управления локальными учетными записями, в частности присвоения группового членства, необходимо использовать оснастку консоли MMC **Локальные пользователи и группы** *(см. разд. "Добавление и удаление членов локальных групп" далее в этой главе)*.

Учетную запись пользователя домашней или рабочей группы можно изменить со стандартной на администратора и наоборот посредством следующей процедуры:

1. В разделе **Учетные записи пользователей** Панели управления щелкните по ссылке **Изменение типа учетной записи**. Откроется страница **Управление учетными записями** (Manage Accounts).
2. Щелкните по учетной записи, которую нужно изменить, а затем — по ссылке **Изменение типа учетной записи** (Change the account type).
3. На следующей странице, **Изменение типа учетной записи** (Change Account Type), установите переключатель **Стандартная** или **Администратор**, а затем нажмите кнопку **Изменение типа учетной записи**.

> ***Примечание***
>
> Если на компьютере имеется только одна учетная запись администратора, ее нельзя изменить на стандартную, т. к. компьютер должен иметь, по крайней мере, одного администратора.

В домене тип локальной учетной записи можно изменить посредством следующей процедуры:

1. В разделе **Учетные записи пользователей** Панели управления щелкните по ссылке **Изменение типа учетной записи**. Откроется диалоговое окно **Учетные записи пользователей**.
2. На вкладке **Пользователи** выберите требуемую учетную запись, а затем нажмите кнопку **Свойства**.
3. В открывшемся диалоговом окне **Свойства** перейдите на вкладку **Членство в группах** (Group Membership).
4. Задайте требуемый тип учетной записи, установив соответствующий переключатель — **Обычный доступ** (Standard User), **Администратор** (Administrator) или **Другой** (Other) (для переключателя **Другой** выберите в рскрывающемся списке соответствующую группу).
5. Последовательно нажмите кнопку **OK**, чтобы закрыть все окна.

Переключение между синхронизированными и обычными учетными записями

Переключаться между синхронизованными и обычными учетными записями можно с помощью утилиты настройки параметров компьютера. Учетную запись домашней или рабочей группы можно изменить со стандартной на учетную запись Microsoft и наоборот посредством следующей процедуры:

1. Войдите в систему по учетной записи пользователя, а затем откройте окно настроек параметров компьютера. Один из способов открыть это окно — нажать комбинацию клавиш <Windows>+<I>, а затем щелкнуть по ссылке **Изменение параметров компьютера** внизу панели **Параметры**.

2. В левой панели **Параметры** выберите раздел **Пользователи**, а в правой панели **Ваша учетная запись** (Your account) щелкните по ссылке **Переключиться на учетную запись Майкрософт** (Switch to a Microsoft account) или **Переключиться на локальную учетную запись** (Switch to a local account), а затем следуйте выводимым инструкциям.

Чтобы переключиться на учетную запись Microsoft, компьютер должен быть подключен к Интернету.

Создание паролей для локальных учетных записей

В домашней или рабочей группе локальные учетные записи по умолчанию создаются без пароля. Это означает, что в систему может войти кто угодно, просто щелкнув по имени пользователя на экране приветствия. Поэтому, чтобы повысить защищенность системы, всем учетным записям необходимо присвоить пароли.

Это можно сделать с помощью утилиты **Учетные записи пользователей**, выполнив вход в систему по учетной записи, для которой нужно создать пароль. Таким образом можно не беспокоиться об утере этим пользователем своих зашифрованных данных. Дело в том, что если пароль для учетной записи создается не ее владельцем (а, например, администратором), данный пользователь утратит доступ ко всем своим зашифрованным файлам, сообщениям электронной почты, личным сертификатам и сохраненным паролям. Это происходит по той причине, что главный ключ пользователя, который требуется для доступа к личному сертификату шифрования, чтобы разблокировать эти данные, зашифрован с помощью хэша, основанного на пустом пароле. А после создания пароля получается другой хэш, вследствие чего зашифрованные данные нельзя разблокировать. Единственным решением этой проблемы является удаление пароля для данной учетной записи, после чего пользователь снова сможет получить доступ к своим зашифрованным файлам. Но эта проблема присуща только для локальных, но не для доменных учетных записей.

Совет

С помощью утилиты **Учетные записи пользователей** можно установить подсказку для пароля, которая может быть полезной для восстановления забытого или утерянного пароля. Другим способом восстановления пароля будет использование файла сброса пароля, который можно записать на гибкий диск или флешку. Важно иметь в виду, что для восстановления паролей локальных учетных записей следует использовать лишь эти два способа, если только вы не хотите потерять данные пользователя. Почему могут теряться данные? Хотя администратор может создавать, сбрасывать или удалять пароль для локальной учетной записи пользователя, это действие удаляет все личные сертификаты и сохраненные пароли, связанные с этой учетной записью. В результате пользователь больше не сможет иметь доступ к своим зашифрованным файлам или личным сообщениям электронной почты, которые были зашифрованы с помощью его личного ключа. Кроме этого, пользователь также потеряет все сохраненные пароли для вебсайтов и сетевых ресурсов. Важно иметь в виду, что эта проблема затрагивает только локальные учетные записи. Администраторы могут изменять или сбрасывать пароли для доменных учетных записей без отрицательных последствий на возможности доступа этих пользователей к своим зашифрованным данным.

Создать пароль для локальной учетной записи пользователя можно посредством следующей процедуры:

1. Выполните вход в систему по учетной записи пользователя, для которой нужно создать пароль. (Это не обязательно, а только если нужно сохранить доступ пользователя к его зашифрованным данным. В противном случае пароль можно создать, работая под учетной записью администратора.) В разделе **Учетные записи пользователей** Панели управления щелкните по ссылке **Изменение типа учетной записи**. Откроется окно **Управление учетными записями**.

2. Щелкните по учетной записи, для которой требуется создать пароль. Чтобы не допустить возможной утери данных, вход в систему должен быть выполнен под этой учетной записью. Учетные записи с паролями помечены подписью **Защищена паролем** (Password protected). Учетные записи без этой подписи не имеют пароля.
3. Щелкните по ссылке **Создать пароль** (Create a password). В открывшемся одноименном окне (рис. 7.5) введите пароль, его подтверждение и подсказку для пароля. Подсказка для пароля представляет собой слово или фразу, по которой можно вспомнить забытый или потерянный пароль. Эту подсказку могут видеть все, кто пытается выполнить вход в систему по данной учетной записи.
4. Нажмите кнопку **Создать пароль**.

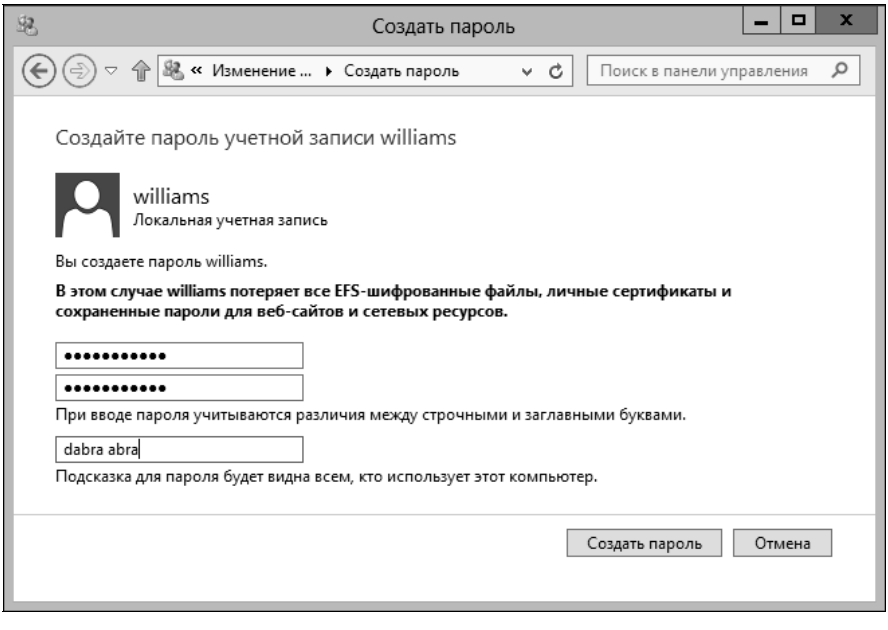


Рис. 7.5. Создание пароля для локальной учетной записи

Восстановление паролей локальных учетных записей

Как упоминалось в предыдущем разделе, для того чтобы сохранить доступ к зашифрованным данным и сохраненным паролям пользователя, вместо изменения или удаления пароля необходимо выполнить его восстановление.

В Windows 8 предоставляются два способа восстановления паролей локальных учетных записей.

- **Подсказка для пароля.** Подсказка для пароля отображается на экране приветствия, который выводится, когда в систему еще не вошел ни один пользователь. Если кто-то уже выполнил вход в систему, попросите его выйти. Щелкните на имени пользователя, чтобы отобразить запрос на ввод пароля, а затем нажмите кнопку входа, чтобы отобразить подсказку пароля. Надеюсь, подсказка поможет вам вспомнить пароль. Если же нет, то придется использовать диск сброса пароля.
- **Диск сброса пароля.** Диск сброса пароля можно создать для любой локальной учетной записи, защищенной паролем. С помощью такого диска можно изменить пароль учетной

записи, не зная старого пароля. Так как любой, кто имеет доступ к этим дискам, может изменить соответствующие пароли, диски необходимо хранить в безопасном месте. Если пользователям разрешается создавать свои диски сброса пароля, обязательно проинструктируйте их о важности этих дисков.

Примечание

Пароли доменных и локальных пользователей управляются по-разному. Администраторы могут управлять паролями доменных учетных записей и выполнять сброс забытого пароля с помощью оснастки консоли MMC, называющейся **Active Directory — пользователи и компьютеры** (Active Directory Users and Computers).

Пароли для локальных учетных записей можно хранить в защищенных шифрованием файлах на диске сброса пароля, для которого можно использовать гибкий диск или флешку. Инструкции по созданию диска сброса пароля *см. в разд. "Создание и использование диска сброса пароля" главы 1*. Инструкции по сбросу пароля локальной учетной записи *см. в разд. "Сброс пароля пользователя" главы 1*.

Управление входом в систему

По умолчанию, как для компьютеров членов домашних или рабочих групп, так и для компьютеров членов доменов, Windows 8 выводит экран блокировки и экран приветствия. Между этими двумя экранами имеется большая разница.

Экран блокировки выводится тогда, когда в систему не выполнил вход ни один пользователь. Установить параметры экрана блокировки можно в окне параметров компьютера, выбрав в его левой панели опцию **Персонализация**, а затем в правой панели опцию **Экран блокировки** (Lock screen). Можно установить такие параметры, как фоновый рисунок экрана блокировки, приложения рабочего стола для исполнения в фоновом режиме, указав для этих приложений, отображать ли сводную информацию о статусе и извещения и каким образом это делать. По умолчанию для приложений рабочего стола Сообщения, Календарь и Почта отображается сводная информация о статусе и уведомления. Администратор может переопределить эти параметры в групповой политике, включив параметр **Отключить уведомления приложений на экране блокировки** политики **Вход в систему**, находящейся в узле **Конфигурация компьютера\Система** консоли редактора локальных групповых политик.

Щелчок по экрану блокировки отображает экран приветствия. В доменных компьютерах на экране приветствия по умолчанию отображается имя последнего вошедшего в систему пользователя. Вход в систему можно выполнить по учетной записи этого пользователя или же выбрать для входа другую учетную запись, нажав кнопку со стрелкой влево слева от текущего аватара пользователя (которая называется **Сменить пользователя** (Switch user)), вследствие чего на экране приветствия будут отображены учетные записи других пользователей. Выберите одну из этих учетных записей и введите пароль для нее. Альтернативно, можно нажать кнопку **Другой пользователь** и ввести имя другого пользователя и пароль для него.

На *экране приветствия* компьютеров членов домашней или рабочей группы выводится список учетных записей данного компьютера. Чтобы войти в систему под одной из этих учетных записей, щелкните на ней мышью и введите ее пароль. Вопреки распространенному мнению, на экране приветствия не отображаются все учетные записи, созданные на данном компьютере. Некоторые учетные записи, такие как учетная запись **Администратор**, не отображаются автоматически.

Тогда как вывод учетных записей на экране приветствия делает удобным вход в систему действительным пользователям, это также облегчает задачу входа в систему несанкциони-

рованным пользователям и даже злоумышленникам. Как для компьютеров членов домашних или рабочих групп, так и для компьютеров членов доменов список учетных записей пользователей можно убрать с экрана приветствия, требуя, чтобы пользователи сами вводили свое имя пользователя. Убрав с экрана приветствия имя последнего выполнявшего вход в систему пользователя, можно повысить безопасность системы, т. к. в таком случае для входа в компьютер необходимо будет знать действительное имя пользователя. Скрыть это имя можно, включив политику **Интерактивный вход в систему: не отображать последнее имя пользователя** (Interactive logon: Do not display last user name), которая расположена в узле **Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики\Параметры безопасности** (Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options).

По умолчанию доменные пользователи не могут вводить ПИН-коды, но могут использовать графические пароли. Изменить эти настройки по умолчанию можно с помощью параметров локальной политики **Включить вход с помощью ПИН-кода** (Turn on PIN sign in) и **Выключить вход с графическим паролем** (Turn off picture password sign-in), которые находятся в узле **Конфигурация компьютера\Административные шаблоны\Система\Вход в систему** консоли редактора локальных групповых политик.

В доменной среде задать требуемую конфигурацию безопасности определенному набору компьютеров можно с помощью групповой политики службы каталогов Active Directory. А настройку безопасности отдельных компьютеров можно выполнить с помощью локальной политики безопасности. Настройка локальной политики для компьютера члена рабочей или домашней группы выполняется следующим образом:

1. Откройте консоль редактора локальной групповой политики. Один из быстрых способов сделать это — нажать клавишу <Windows>, а затем ввести с клавиатуры команду `gpedit.msc` (которая при первом нажатии клавиши будет вводиться в поле поиска открывшейся панели **Приложения**) и нажать клавишу <Enter>.
2. В редакторе групповых политик последовательно разверните узлы **Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики\Параметры безопасности** (рис. 7.6).

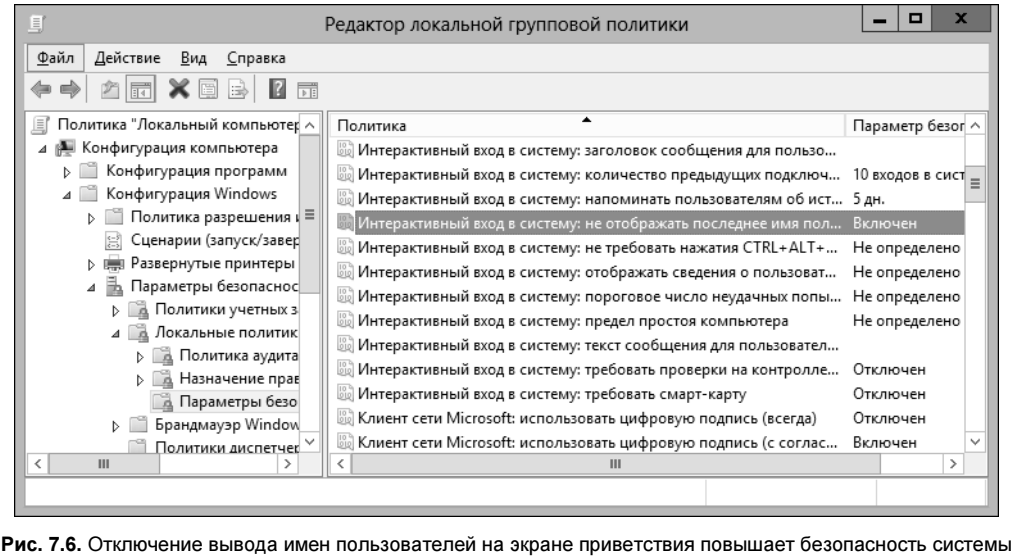


Рис. 7.6. Отключение вывода имен пользователей на экране приветствия повышает безопасность системы

3. Дважды щелкните на политике **Интерактивный вход в систему: не отображать последнее имя пользователя**.
4. В открывшемся одноименном диалоговом окне установите переключатель **Включить** и нажмите кнопку **OK**.
5. Далее разверните узел **Конфигурация компьютера\Административные шаблоны\Система\Вход в систему** и настройте связанные политики как требуется.

Удаление учетных записей и запрещение локального доступа к рабочим станциям

Администраторам доменов автоматически предоставляется доступ к локальным ресурсам рабочих станций. Другим пользователям доступ к локальным ресурсам рабочих станций запрещен, за исключением рабочих станций, на которых они могут выполнять вход в систему. Если за рабочей станцией в организации будет работать другой пользователь, предыдущий пользователь может продолжать иметь доступ к ее ресурсам. Аналогично пользователи, которым был предоставлен временный доступ к рабочей станции, могут в результате получить постоянный доступ к ней, если администратор забыл удалить их из списка доступа.

В доменной среде рабочие станции, с которых пользователи могут входить в систему, можно контролировать, редактируя свойства учетных записей в оснастке **Пользователи и компьютеры Active Directory**. Для этого дважды щелкните на требуемой учетной записи, в открывшемся диалоговом окне свойств учетной записи выберите вкладку **Учетная запись** и нажмите на ней кнопку **Вход на** (Log on to). В открывшемся диалоговом окне **Рабочие станции для входа в систему** установите переключатель **только на указанные компьютеры** и укажите компьютеры, с которых пользователь может выполнять вход в систему.

В среде домашней или рабочей группы можно удалить локальную учетную запись пользователя, запретив ему вход в систему. Удаление учетной записи выполняется следующим образом:

1. Войдите в систему по учетной записи с полномочиями локального администратора. В разделе **Учетные записи пользователей** Панели управления щелкните по ссылке **Изменение типа учетной записи**. Откроется окно **Управление учетными записями**.
2. Щелкните на учетной записи, которую требуется удалить, а затем щелкните по ссылке **Удаление учетной записи** (Delete the account).
3. Откроется диалоговое окно, в котором будет предоставлена возможность сохранить содержимое рабочего стола и личных папок удаляемого пользователя в папку на рабочем столе текущего пользователя. Чтобы сохранить эти данные, нажмите кнопку **Сохранение файлов** (Keep files), а в противном случае нажмите кнопку **Удалить файлы** (Delete files).
4. В следующем окне, **Подтверждение удаления** (Confirm Deletion), подтвердите удаление учетной записи, нажав кнопку **Удаление учетной записи** (Delete Account). При этом следует иметь в виду, что если только не наложить другие ограничения на вход в рабочую станцию, пользователь все равно сможет получить доступ к ней, выполнив вход по доменной учетной записи.

Управления сохраненными параметрами доступа

В Windows 8 можно использовать диспетчер учетных данных (Credential Manager) для сохранения в профиле пользователя учетных данных, с помощью которых он мог бы автоматически входить на серверы, веб-сайты и в программы. Учетные данные сохраняются в профиле пользователя. Такая возможность может быть полезной, когда у пользователя часто возникают проблемы со входом в защищенные ресурсы, например во внутрикорпоративную сеть или на внешние веб-сайты. В таком случае для каждого ресурса, с которым работает пользователь, можно сохранить учетные данные.

Диспетчер учетных данных позволяет сохранять четыре типа учетных данных.

- **Учетные данные Интернета.** Содержат информацию о размещении ресурса, имя пользователя учетной записи и ее пароль.
- **Учетные данные Windows.** Эти учетные данные проверяются посредством стандартной аутентификации Windows (NTLM или Kerberos) и содержат сведения о местонахождении ресурса, имя учетной записи и пароль пользователя.
- **Учетные данные на основе сертификата.** Содержат информацию о местонахождении ресурса и используют для аутентификации пользователя сертификат, который хранится в персональном хранилище диспетчера сертификатов.
- **Общие учетные данные.** Эти учетные данные проверяются посредством базового или специального способа аутентификации и содержат сведения о местонахождении ресурса, имя учетной записи и пароль пользователя.

Методы работы с сохраненными учетными данными рассматриваются в последующих разделах.

Практический совет

При создании на компьютере учетной записи Microsoft создаются и сохраняются общие учетные данные для Windows Live. Учетные данные Windows Live применяются для доступа к Microsoft Store, SkyDrive и другим службам Microsoft. Обычно эти учетные данные не следует редактировать или удалять. Но если по какой-либо причине произойдет рассогласование текущих и сохраненных учетных данных, тогда адрес электронной почты и пароль, применяемые для доступа к службам Microsoft, следует отредактировать должным образом.

Добавление учетных данных Windows и общих учетных данных

Каждая конкретная учетная запись пользователя имеет уникальные учетные данные. Отдельные элементы учетных данных хранятся в настройках профиля пользователя и содержат информацию, необходимую для получения доступа к защищенным ресурсам. Если учетные данные созданы при работе в доменной учетной записи с перемещаемым профилем (а не с локальным или обязательным профилем), сохраненная в них информация доступна при входе в систему с любого компьютера домена. В противном случае информация учетных данных доступна только на компьютере, на котором они были созданы.

Практический совет

Сохранение учетных данных для компьютеров, работающих в среде рабочей или домашней группы, а не являющихся членами домена, может сэкономить всем много времени. Например, если пользователь работает на компьютере, являющемся членом рабочей группы, но ему нужно

обращаться к нескольким разным серверам в разных местах или доменах, этот процесс можно облегчить, создав учетные данные Windows для каждого такого ресурса. Теперь, независимо от способа обращения пользователя к серверам, его аутентификация выполняется автоматически, без необходимости предоставления альтернативных учетных данных. Например, если пользователь подключает сетевой диск к серверу FileServer84, для которого были сохранены необходимые учетные данные, ему не нужно устанавливать флажок **Использовать другие учетные данные**, а затем предоставлять другие имя пользователя и пароль.

Добавить запись к учетным данным текущего пользователя можно следующим образом:

1. Выполните вход в систему по учетной записи пользователя, чьими учетными данными нужно управлять. В Панели управления щелкните по ссылке **Учетные записи пользователей**, в правой панели — по ссылке **Администрирование учетных записей** (Manage your credentials) и в открывшемся окне **Диспетчер учетных данных** (Credential Manager) выберите вкладку **Учетные данные Windows** (Windows Credentials).

   Эта вкладка содержит список записей учетных данных, упорядоченных по типу (если имеются какие-либо записи) (рис. 7.7).

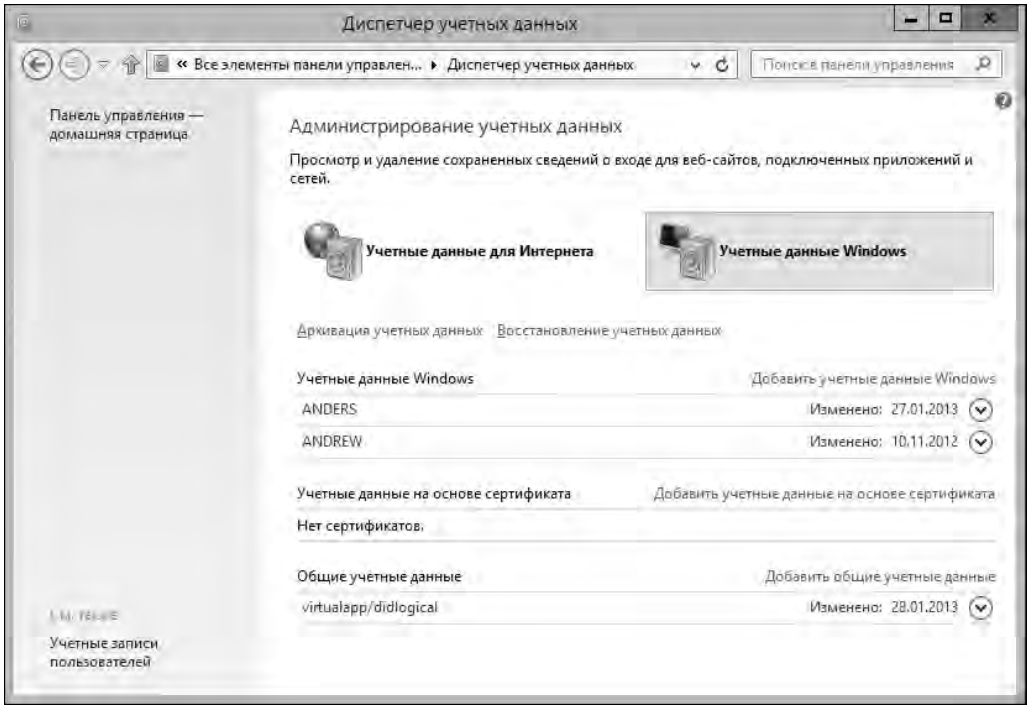


Рис. 7.7. Вкладка **Учетные данные Windows** окна **Диспетчер учетных данных**

Примечание

Обратите внимание, что Панель управления доменных компьютеров содержит ссылку **Учетные записи пользователей**, в то время как ссылка этого же назначения в Панели управления компьютеров членов рабочих или домашних групп называется **Учетные записи пользователей и Семейная безопасность** (User Account and Family Safety). Но для простоты и краткости в этой книге данная ссылка также упоминается просто как **Учетные записи пользователей**.

2. Щелкните по ссылке **Добавить учетные данные Windows** (Add a Windows credential) или **Добавить общие учетные данные** (Add a generic credential), в зависимости от типа

учетных данных, которые требуется добавить. В открывшемся окне добавления учетных данных (рис. 7.8) введите требуемые параметры учетных данных.

Доступны следующие опции.

- **Адрес в Интернете или сети** (Network or Internet address). Адрес сетевого или интернет-ресурса, для которого создается запись учетных данных. Это может быть имя сервера, например `Fileserver86`; полное доменное имя интернет-ресурса, например `www.microsoft.com`; или адрес, содержащий подстановочный знак, например `*.microsoft.com`. Если указывается имя сервера или полное доменное имя, данная запись применяется для доступа к определенному серверу или службе. А если приводится адрес с подстановочным знаком, запись используется для доступа к любому серверу в указанном домене. Например, адрес `*.microsoft.com` можно использовать для доступа к серверам **www.microsoft.com**, **ftp.microsoft.com**, **smtp.microsoft.com** и **extranet.microsoft.com**.

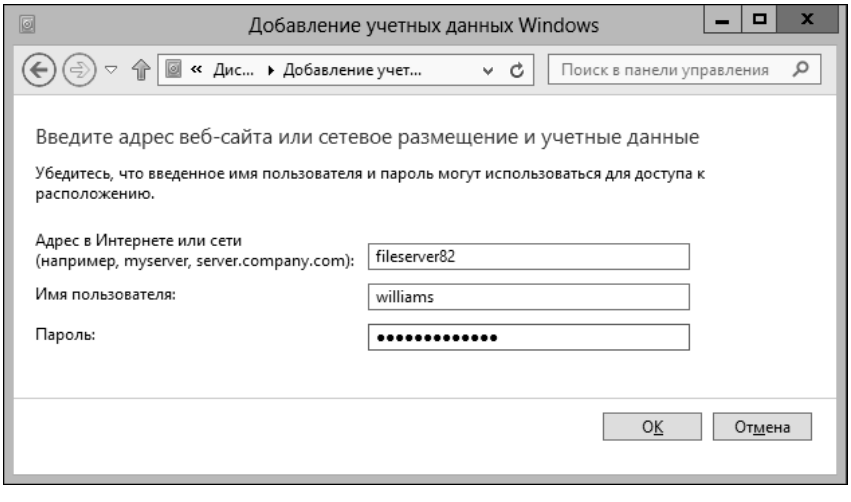


Рис. 7.8. Добавление учетных данных Windows

- **Имя пользователя.** Имя пользователя для входа на сервер со всеми необходимыми квалификаторами домена. Для ресурса в домене по умолчанию введите только имя пользователя, например `Williams`. Для других доменов введите полное имя домена и имя учетной записи, например `technology\Williams`. А для интернет-ресурса укажите полное имя учетной записи ресурса, например `Williams@msn.com`.
- **Пароль.** Пароль, требуемый для входа на сервер. Многие пользователи часто забывают, что при смене пароля для сервера или службы также необходимо сменить данный пароль в своих сохраненных учетных данных. Если пользователь забудет изменить пароль в сохраненных учетных данных, повторные попытки войти на сервер или подключиться к службе могут вызвать блокировку учетной записи.

3. Нажмите кнопку **OK**, чтобы сохранить запись учетных данных.

Добавление учетных данных на основе сертификата

Хранилище личных сертификатов в профиле пользователя содержит сертификаты, выданные пользователю для подтверждения его подлинности. Когда для пользователя был добав-

лен сертификат, можно создать учетные данные для доступа к ресурсам на основе этого сертификата.

Запись учетных данных на основе сертификата для текущего пользователя можно добавить следующим образом:

1. Выполните вход в систему по учетной записи пользователя, чьими учетными данными нужно управлять. В Панели управления щелкните по ссылке **Учетные записи пользователей**, а в правой панели — по ссылке **Администрирование учетных записей** и в открывшемся окне **Диспетчер учетных данных** выберите вкладку **Учетные данные Windows**.

   Эта вкладка содержит список записей учетных данных, упорядоченных по типу (если имеются какие-либо записи).
2. Щелкните по ссылке **Добавить учетные данные на основе сертификата** (Add a certificate-based credential). В поле **Адрес в Интернете или сети** введите имя сетевого или интернет-ресурса, для которого создается запись учетных данных. Это может быть имя сервера, полное доменное имя интернет-ресурса или адрес, содержащий подстановочный знак.
3. Нажмите кнопку **Выбор сертификата** (Select certificate). В открывшемся диалоговом окне **Безопасность Windows** (Windows Security) щелкните на персональном сертификате, который будет использоваться для данного ресурса, а затем нажмите кнопку **OK**.
4. Нажмите кнопку **OK** в следующем окне, чтобы сохранить запись учетных данных.

Редактирование учетных данных

Записи учетных данных можно редактировать в любое время, но следует иметь в виду, что локальные записи видимы только на компьютере, на котором они были созданы. Это означает, что для редактирования записи учетных данных необходимо войти в систему на той локальной станции, на которой эта запись была создана. Единственным исключением являются пользователи с перемещаемым профилем. Для них записи учетных данных можно редактировать на любом компьютере, с которого пользователь выполнил вход в систему.

Редактирование записи учетных данных пользователя выполняется следующим образом:

1. Выполните вход в систему по учетной записи пользователя, чьими учетными данными нужно управлять. В Панели управления щелкните по ссылке **Учетные записи пользователей**, а в правой панели — по ссылке **Администрирование учетных записей** и в открывшемся окне **Диспетчер учетных данных** выберите вкладку **Учетные данные Windows**.

   Эта вкладка содержит список текущих записей учетных данных, упорядоченных по типу.
2. Щелкните на записи учетных данных, которую нужно редактировать.
3. Щелкните по ссылке **Изменить**.
4. Введите новые значения для имени пользователя и пароля или связанного с учетными данными сертификата, после чего нажмите кнопку **Сохранить**.

Создание резервной копии и восстановление учетных данных Windows

Резервное копирование сохраненных учетных данных пользователя можно выполнять отдельно от резервного копирования его данных. Резервную копию учетных данных можно

использовать для их восстановления на исходном компьютере или для их переноса на другой компьютер. В большинстве случаев резервную копию учетных данных следует создавать на съемном носителе.

Резервную копию учетных данных пользователя можно создать следующим способом:

1. Выполните вход в систему по учетной записи пользователя, для чьих учетных данных нужно создать резервную копию. В Панели управления щелкните по ссылке **Учетные записи пользователей**, а в правой панели — по ссылке **Администрирование учетных записей** и в открывшемся окне **Диспетчер учетных данных** выберите вкладку **Учетные данные Windows**.

   Эта вкладка содержит список текущих записей, упорядоченных по типу.
2. Щелкните по ссылке **Архивация учетных данных** (Back up Credentials).
3. В открывшемся диалоговом окне **Сохранение имен пользователей и паролей** (Stored User Names and Passwords) нажмите кнопку **Обзор**. В следующем диалоговом окне, **Сохранение файла резервной копии** (Save Backup File As), укажите папку для сохранения файла резервной копии учетных данных и имя самого файла. (Файлы резервных копий учетных данных имеют расширение crd.) Нажмите кнопку **Сохранить**.
4. В окне сохранения файла резервной копии нажмите кнопку **Далее**. Нажмите комбинацию клавиш <Ctrl>+<Alt>+<Del>, как указывается в следующем диалоговом окне, чтобы переключиться на безопасный рабочий стол. В следующем диалоговом окне введите пароль для файла резервной копии учетных данных и его подтверждение.
5. Нажмите кнопку **Далее**, а в следующем окне — кнопку **Готово**.

Восстановить учетные данные пользователя на исходном или на другом компьютере можно следующим образом:

1. Выполните вход в систему по учетной записи пользователя, для которой необходимо восстановить учетные данные. В Панели управления щелкните по ссылке **Учетные записи пользователей**, а в правой панели — по ссылке **Администрирование учетных записей** и в открывшемся окне **Диспетчер учетных данных** выберите вкладку **Учетные данные Windows**.
2. На этой вкладке щелкните по ссылке **Восстановление учетных данных** (Restore Credentials).
3. В открывшемся диалоговом окне **Сохранение имен пользователей и паролей** нажмите кнопку **Обзор**. В открывшемся диалоговом окне **Открытие файла резервной копии** (Open Backup File) укажите папку и файл резервной копии учетных данных и нажмите кнопку **Открыть**.
4. В окне сохранения файла резервной копии нажмите кнопку **Далее**. Нажмите комбинацию клавиш <Ctrl>+<Alt>+<Del>, как указывается в следующем диалоговом окне, чтобы переключиться на безопасный рабочий стол. В следующем диалоговом окне введите пароль для восстановления учетных данных.
5. Нажмите кнопку **Далее**, а в следующем окне — кнопку **Готово**.

Удаление записей учетных данных

Записи учетных данных, которые больше не нужны пользователю, следует удалять. Удалить запись учетных данных пользователя можно следующим способом:

1. Выполните вход в систему по учетной записи пользователя, чьи учетные данные нужно удалить. В Панели управления щелкните по ссылке **Учетные записи пользователей**, а в

правой панели — по ссылке **Администрирование учетных записей** и в открывшемся окне **Диспетчер учетных данных** выберите вкладку **Учетные данные Windows**.

Эта вкладка содержит список текущих записей, упорядоченных по типу.

2. Щелкните на записи учетных данных, которую нужно удалить.
3. Нажмите кнопку **Удалить** (Remove). В открывшемся диалоговом окне **Удаление учетных записей Windows** (Remove Windows Credential) подтвердите удаление, нажав кнопку **Да**.

Как упоминалось ранее, локальные записи учетных данных можно удалить только работая на компьютере, на котором они были созданы. Но записи учетных данных пользователей с перемещаемым профилем можно удалять с любого компьютера.

Управление локальными учетными записями и группами

Управление локальными учетными записями и группами осуществляется во многом подобно управлению доменными учетными записями. Можно создавать учетные записи, управлять их свойствами, сбрасывать заблокированные или поврежденные учетные записи и т. п. Кроме управления локальными учетными записями из Панели управления, локальные учетные записи можно создавать с помощью оснастки **Локальные пользователи и группы** или посредством предпочтений политик. Эти дополнительные средства управления локальными учетными записями нужно использовать следующим образом:

- оснастка **Локальные пользователи и группы** служит для управления локальными учетными записями на одном компьютере;
- предпочтения используются для управления локальными учетными записями на нескольких компьютерах домена.

При использовании предпочтений пользователями и группами можно управлять посредством параметров узлов **Конфигурация компьютера** и **Конфигурация пользователя**. Параметры узла **Конфигурация компьютера** используются для настройки предпочтений компьютера, независимо от вошедших на него пользователей, а параметры узла **Конфигурация пользователя** — для настройки предпочтений пользователей, независимо от компьютера, на который они входят.

Создание локальных учетных записей пользователей

Запустить оснастку **Локальные пользователи и группы** и создать локальную учетную запись пользователя можно следующим образом:

1. Откройте консоль **Управление компьютером**. Щелкните правой кнопкой мыши на корневом узле **Управление компьютером** в дереве консоли и в контекстном меню выберите команду **Подключиться к другому компьютеру**. В открывшемся диалоговом окне **Выбор компьютера** нажмите кнопку **Обзор** и с помощью последующих диалоговых окон выберите компьютер под управлением Windows 8, чьими локальными учетными записями требуется управлять. (Контроллеры доменов не имеют локальных пользователей или групп.)

2. Разверните узел **Служебные программы** (System Tools), далее узел **Локальные пользователи и группы** и выберите в нем папку **Пользователи**. В области сведений консоли отобразится список учетных записей, определенных на текущий момент на данном компьютере.
3. Щелкните правой кнопкой мыши на папке **Пользователи** и в контекстном меню выберите команду **Новый пользователь**. Откроется одноименное диалоговое окно (рис. 7.9).

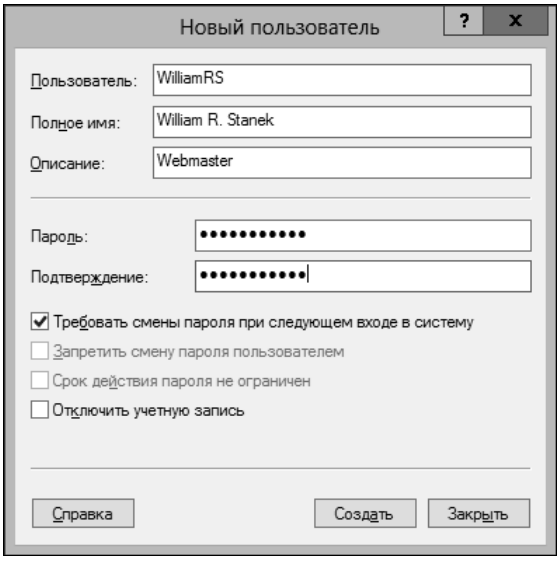


Рис. 7.9. Диалоговое окно для создания нового пользователя

В этом диалоговом окне можно задать следующие параметры.

- **Имя пользователя.** Имя входа для учетной записи пользователя. Это имя должно отвечать требованиям политики имен локальных пользователей.
- **Полное имя.** Полное имя пользователя, например `William R. Stanek`.
- **Описание.** Описание пользователя. Обычно сюда вводится должность пользователя, например `Webmaster`. Также можно указать отдел, в котором работает пользователь.
- **Пароль.** Пароль для учетной записи. Пароль должен отвечать требованиям политики паролей предприятия.
- **Подтверждение (пароля).** Подтверждение пароля учетной записи. Повторно введите пароль, чтобы убедиться в том, что действительно введен правильный пароль.
- **Требовать смены пароля при следующем входе в систему** (User must change password on next logon). Эта опция применяется в качестве дополнительной меры безопасности по предотвращению несанкционированного доступа к системе.
- **Запретить смену пароля пользователем** (User cannot change password). Еще одна дополнительная мера безопасности по предотвращению несанкционированного доступа к системе.
- **Срок действия пароля не ограничен** (Password never expires). Установка этого флажка задает неограниченный срок действия пароля. Этот параметр имеет старшинство над настройкой политики локальной учетной записи.

- **Отключить учетную запись** (Account is disabled). Установка этого флажка отключает учетную запись. Опция применяется, когда нужно временно полностью запретить использование учетной записи.

4. Закончив настройку новой учетной записи, нажмите кнопку **Создать**.

Учетную запись пользователя можно также создать, используя узел предпочтений групповой политики. Делается это следующим образом:

1. В редакторе управления групповыми политиками откройте для редактирования требуемый объект групповой политики. Для настройки параметров компьютера разверните узел **Конфигурация компьютера\Настройка\Параметры панели управления** и выберите в нем узел **Локальные пользователи и группы**. Для настройки параметров пользователя разверните узел **Конфигурация пользователя\Настройка\Параметры панели управления** и выберите в нем узел **Локальные пользователи и группы**.
2. Щелкните правой кнопкой мыши по узлу **Локальные пользователи и группы**, выберите в контекстном меню команду **Создать**, а во вложенном меню — **Локальный пользователь**. Откроется диалоговое окно **Новые свойства локального пользователя** (New Local User Properties) (рис. 7.10).

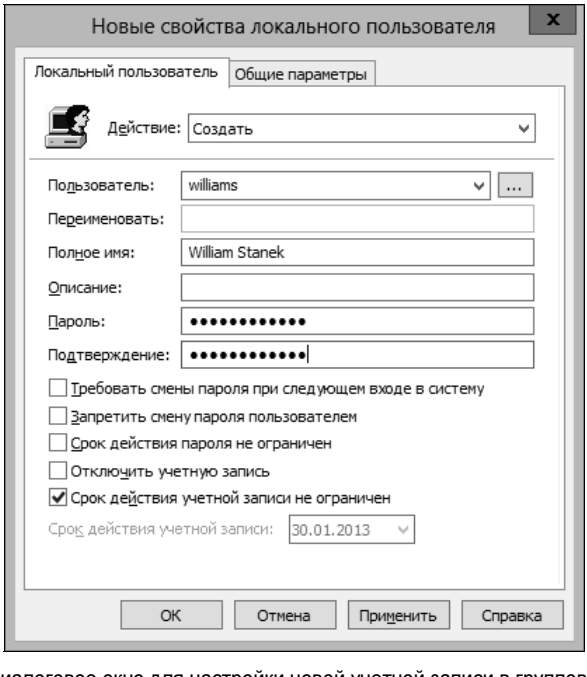


Рис. 7.10. Диалоговое окно для настройки новой учетной записи в групповой политике

3. В раскрывающемся списке **Действие** выберите вариант **Создать**. Остальные поля этого диалогового поля имеют такое же назначение, как и соответствующие поля диалогового окна для создания нового пользователя в консоли **Управление компьютером** (см. рис. 7.9).
4. Для управления способом применения настройки используются опции на вкладке **Общие параметры**. В большинстве случаев новую учетную запись нужно создать только один раз. Тогда устанавливается флажок **Применить один раз и не применять повторно**.

5. Нажмите кнопку **OK**, чтобы сохранить настройку. При следующем обновлении групповой политики элемент настройки будет применен должным образом к объекту групповой политики, для которого он был определен.

Создание локальных групп для рабочих станций

Локальные группы можно создавать с помощью оснастки **Локальные пользователи и группы** консоли **Управление компьютером** или посредством групповой политики. Запустить оснастку **Локальные пользователи и группы** и создать локальную учетную запись пользователя можно следующим образом:

1. Откройте консоль **Управление компьютером**. Нажмите или щелкните правой кнопкой мыши по корневому узлу **Управление компьютером** в дереве консоли и в контекстном меню выберите опцию **Подключиться к другому компьютеру**. В открывшемся диалоговом окне **Выбор компьютера** нажмите кнопку **Обзор** и с помощью последующих диалоговых окон выберите компьютер под управлением Windows 8, чьими локальными учетными записями требуется управлять. (Контроллеры доменов не имеют локальных пользователей или групп.)
2. Разверните узел **Служебные программы**, далее узел **Локальные пользователи и группы** и выберите в нем папку **Группы**. В области сведений консоли будет выведен список групповых учетных записей, определенных на текущий момент.
3. Щелкните правой кнопкой мыши на папке **Группы** и в контекстном меню выберите команду **Создать группу**. Откроется диалоговое окно **Новая группа** (рис. 7.11).

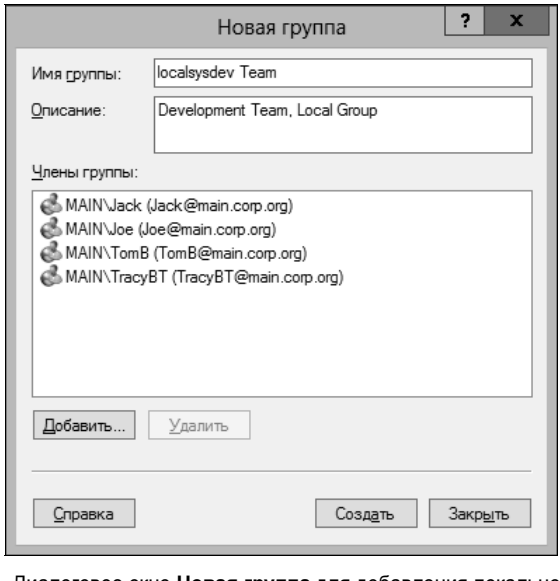


Рис. 7.11. Диалоговое окно **Новая группа** для добавления локальной группы на рабочую станцию под управлением Windows 8

4. Введите имя и описание группы в соответствующие поля, а затем нажмите кнопку **Добавить**, чтобы добавить пользователей в группу.
5. В открывшемся диалоговом окне **Выбор: "Пользователи", "Компьютеры", "Учетные записи"** нажмите кнопку **Создать**, чтобы выбрать компьютер или домен, в котором находятся требуемые учетные записи.

6. Введите имя пользователя, которого нужно добавить в группу, в текстовое поле **Введите имена выбираемых объектов** (Enter the object names to select), а затем нажмите кнопку **Проверить имена** (Check names). Если для указанного имени найдутся совпадения, они будут отображены в поле ввода. Выберите из них требуемую учетную запись и нажмите кнопку **OK**. При отсутствии совпадений исправьте введенное имя и повторите попытку. Повторите процесс поиска, пока не будут найдены все требуемые учетные записи, после чего нажмите кнопку **OK**.
7. Выбранные учетные записи отобразятся в поле **Члены группы** диалогового окна **Новая группа**. Если какая-либо учетная запись была добавлена в создаваемую группу по ошибке, щелкните на ней мышью, а затем нажмите кнопку **Удалить**.
8. Когда список содержит все требуемые учетные записи, создайте группу, нажав кнопку **Создать**, после чего закройте диалоговое окно **Новая группа**, нажав кнопку **Закрыть**.

Локальную группу можно также создать, используя узел предпочтений групповой политики. Делается это следующим образом:

1. В редакторе управления групповыми политиками откройте для редактирования требуемый объект групповой политики. Для настройки параметров компьютера разверните узел **Конфигурация компьютера\Настройка\Параметры панели управления** и выберите в нем узел **Локальные пользователи и группы**. Для настройки параметров пользователя разверните узел **Конфигурация пользователя\Настройка\Параметры панели управления** и выберите в нем узел **Локальные пользователи и группы**.
2. Щелкните правой кнопкой мыши по узлу **Локальные пользователи и группы**, выберите в контекстном меню команду **Создать**, а во вложенном меню — опцию **Локальная группа**. Откроется диалоговое окно **Новые свойства локальной группы** (New Local Group Properties) (рис. 7.12).

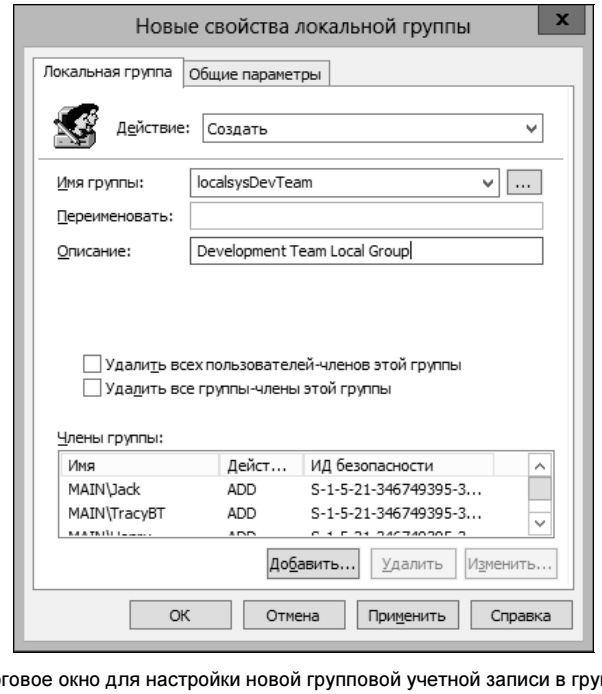


Рис. 7.12. Диалоговое окно для настройки новой групповой учетной записи в групповой политике

3. В раскрывающемся списке **Действие** выберите команду **Создать**. Введите в соответствующие поля имя и описание группы.
4. Нажмите кнопку **Добавить**, чтобы добавить члена группы. В диалоговом окне **Член локальной группы** нажмите кнопку обзора (кнопка с тремя точками справа от поля **Имя**). С помощью открывшегося диалогового окна **Выбор: "Пользователь", "Компьютер" или "Группа"** (Select User, Computer or Group) выберите пользователя, которого следует добавить в группу, и дважды нажмите кнопку **OK**, чтобы добавить пользователя в группу и возвратиться в окно **Новые свойства локальной группы**. Повторите этот шаг, чтобы добавить в группу всех необходимых пользователей.
5. Для управления способом применения настройки используются опции на вкладке **Общие параметры**. В большинстве случаев новую групповую учетную запись нужно создать только один раз. Тогда устанавливается флажок **Применить один раз и не применять повторно**.
6. Нажмите кнопку **OK**, чтобы сохранить настройку. При следующем обновлении групповой политики элемент настройки будет применен должным образом к объекту групповой политики, для которого он был определен.

Добавление и удаление членов локальных групп

Членов локальной группы можно добавлять с помощью оснастки **Локальные пользователи и группы** следующим образом:

1. В консоли **Управление компьютером** разверните узел **Локальные пользователи и группы** и выберите в нем папку **Группы**. В панели сведений дважды щелкните на требуемой группе.
2. В открывшемся окне свойств группы нажмите кнопку **Добавить**, чтобы добавить пользователей в группу. Откроется диалоговое окно **Выбор: "Пользователи"** (Select User). Введите имя пользователя, которого нужно добавить в группу, в текстовое поле **Введите имена выбираемых объектов**, а затем нажмите кнопку **Проверить имена**. Если для указанного имени найдутся совпадения, они будут отображены в поле ввода. Выберите из них необходимую учетную запись и нажмите кнопку **OK**. При отсутствии совпадений исправьте введенное имя и повторите попытку. Повторите процесс поиска, пока не будет найдена нужная учетная запись, после чего нажмите кнопку **OK**.
3. Чтобы удалить пользователя из группы, выберите его и нажмите кнопку **Удалить**.
4. Завершив добавление и удаление пользователей, нажмите кнопку **OK**, чтобы сохранить настройки и закрыть окно свойств группы.

Добавлять пользователей в локальную группу и удалять их можно так же, используя узел предпочтений групповой политики. Делается это следующим образом:

1. В редакторе управления групповыми политиками откройте для редактирования требуемый объект групповой политики. Для настройки параметров компьютера разверните узел **Конфигурация компьютера\Настройка\Параметры панели управления** и выберите в нем узел **Локальные пользователи и группы**. Для настройки параметров пользователя разверните узел **Конфигурация пользователя\Настройка\Параметры панели управления** и выберите в нем узел **Локальные пользователи и группы**.
2. Щелкните правой кнопкой мыши по узлу **Локальные пользователи и группы**, выберите в контекстном меню команду **Создать**, а во вложенном меню — опцию **Локальная группа**. Откроется диалоговое окно **Новые свойства локальной группы**.

3. Для обновления параметров группы выберите в списке **Действие** опцию **Обновить**, а чтобы удалить группу и создать ее заново согласно требуемым параметрам, выберите опцию **Заменить**. При обновлении группы можно ввести ее новое имя в поле **Переименовать** (Rename to).
4. Укажите, требуется ли добавить текущего члена в группу или удалить его, или же выберите опцию **Не настраивать для текущего пользователя** (Do not configure for the current user).
5. Укажите, следует ли удалить всех пользователей-членов данной группы, все группы-члены данной группы или и то и другое, установив соответствующие флажки.
6. Чтобы добавить или удалить члена группы, нажмите кнопку **Добавить**. В выпадающем списке **Действие** открывшегося диалогового окна **Член локальной группы** (Local Group Member) выберите опцию **Добавить в эту группу** (Add to this group) или **Удалить из этой группы** (Remove from this group), чтобы добавить или удалить члена группы соответственно. Затем нажмите кнопку обзора файловой системы (кнопка с тремя точками справа от поля **Имя**. С помощью открывшегося диалогового окна **Выбор: "Пользователь", "Компьютер" или "Группа"** выберите пользователя, которого следует добавить в группу, и дважды нажмите кнопку **OK**, чтобы добавить пользователя в группу и возвратиться в окно **Новые свойства локальной группы**. Повторите этот шаг, чтобы добавить или удалить из группы всех необходимых пользователей.
7. Для управления способом применения настройки используются опции на вкладке **Общие параметры**. При следующем обновлении политики элемент настройки будет применен должным образом к объекту групповой политики, для которого он был определен.

Включение и отключение локальных учетных записей пользователей

Локальные учетные записи пользователей могут оказаться отключенными по разным причинам. Если пользователь забудет пароль и будет пытаться угадать его, его учетная запись может быть заблокированной после нескольких неудачных попыток, число которых устанавливается политикой для учетных записей. Или же другой администратор мог отключить учетную запись пользователя, который был в отпуске. Отключенную или заблокированную учетную запись можно включить с помощью рассматриваемых далее методов.

Отключенную локальную учетную запись можно включить следующим способом:

1. В консоли **Управление компьютером** разверните узел **Локальные пользователи и группы** и выберите в нем папку **Пользователи**.
2. В панели сведений дважды щелкните на требуемой учетной записи и в открывшемся диалоговом окне свойств учетной записи снимите флажок **Отключить учетную запись** (Account is disabled).
3. Нажмите кнопку **OK**, чтобы сохранить настройку.

Заблокированную локальную учетную запись можно разблокировать следующим способом:

1. В консоли **Управление компьютером** разверните узел **Локальные пользователи и группы** и выберите в нем папку **Пользователи**.
2. В панели сведений дважды щелкните на требуемой учетной записи и в открывшемся диалоговом окне свойств учетной записи снимите флажок **Заблокировать учетную запись** (Account is locked out).
3. Нажмите кнопку **OK**, чтобы сохранить настройку.

Учетные записи можно включать и отключать, а также настраивать их параметры посредством предпочтений следующим образом:

1. В редакторе управления групповыми политиками откройте для редактирования требуемый объект групповой политики. Для настройки параметров компьютера разверните узел **Конфигурация компьютера\Настройка\Параметры панели управления** и выберите в нем узел **Локальные пользователи и группы**. Для настройки параметров пользователя разверните узел **Конфигурация пользователя\Настройка\Параметры панели управления** и выберите в нем узел **Локальные пользователи и группы**.
2. В панели сведений дважды щелкните на требуемой учетной записи.
3. В списке **Действие** открывшегося диалогового окна свойств учетной записи выберите опцию **Обновить**. Выполните требуемые изменения и сохраните их, нажав кнопку **OK**. При следующем обновлении политики элемент настройки будет применен должным образом к объекту групповой политики, для которого он был определен.

Создание безопасной гостевой учетной записи

При определенных обстоятельствах может потребоваться настроить гостевую учетную запись для работы посетителей. В большинстве случаев учетную запись **Гость** желательно настроить на определенном компьютере или компьютерах и внимательно следить за ее использованием. Для создания безопасной учетной записи **Гость** рекомендуется выполнить следующие действия.

- **Включите учетную запись Гость.** По умолчанию учетная запись **Гость** отключена, поэтому прежде всего ее нужно включить. Для этого в консоли **Управление компьютером** разверните узел **Локальные пользователи и группы** и выберите в нем папку **Пользователи**. В панели сведений дважды щелкните на учетной записи **Гость** и в открывшемся диалоговом окне свойств учетной записи снимите флажок **Отключить учетную запись**. Нажмите кнопку **OK**, чтобы сохранить настройку.
- **Создайте для учетной записи Гость надежный пароль.** По умолчанию учетная запись **Гость** не имеет пароля. Чтобы повысить уровень безопасности компьютера, для нее нужно создать пароль. Для этого в панели сведений узла **Локальные пользователи и группы** щелкните правой кнопкой мыши на учетной записи **Гость** и в контекстном меню выберите команду **Задать пароль** (Set Password). В диалоговом окне **Установка пароля для Гость** (Set Password for Guest) нажмите кнопку **Продолжить**. (Proceed). В следующем окне введите новый пароль и его подтверждение, после чего последовательно дважды нажмите кнопку **OK**, чтобы закрыть все окна.
- **Обеспечьте невозможность использования гостевой учетной записи в сетевой среде.** Гостевая учетная запись должна быть недоступной с других компьютеров по сети, чтобы не допустить входа пользователей в систему по этой учетной записи с других компьютеров. Чтобы запретить сетевой доступ к гостевой учетной записи, в меню **Средства диспетчера серверов** запустите оснастку **Локальная политика безопасности**. (Эту оснастку также можно запустить командой `secpol.msc`.) В левой панели консоли оснастки разверните узел **Локальные политики\Назначение прав пользователя** (User Rights Assignment), а затем в правой панели дважды щелкните на политике **Отказать в доступе к этому компьютеру из сети** (Deny access to this computer from the network) и в открывшемся окне свойств добавьте учетную запись **Гость** в список запрещенных учетных записей.
- **Запретите учетной записи Гость выключать компьютер.** В процессе выключения или запуска компьютера гостевой пользователь (или любой пользователь, имеющий локальный доступ) может получить несанкционированный доступ к компьютеру. Чтобы не

допустить этого, учетная запись **Гость** не должна иметь прав на выполнение завершения работы системы. Для того в левой панели консоли оснастки **Локальная политика безопасности** разверните узел **Локальные политики\Назначение прав пользователя** и в правой панели дважды щелкните на политике **Завершение работы системы** (Shut down the system). В открывшемся окне свойств убедитесь, что учетная запись **Гость** отсутствует в списке разрешенных записей.

- **Запретите учетной записи Гость просмотр журналов событий.** В целях обеспечения безопасности системы пользователю учетной записи **Гость** должно быть запрещено просматривать журналы событий. Для этого запустите редактор реестра (выполнив команду `regedit`) и откройте раздел реестра `HKLM\SYSTEM\CurrentControlSet\Services\Eventlog`. Этот раздел содержит, среди прочих, три важных подраздела: `Application`, `Security` и `System`. Убедитесь, что каждый из этих подразделов имеет переменную RestrictGuestAcces типа DWORD со значением `1`.

Переименование локальных учетных записей и групп

При переименовании учетной записи ей просто присваивается новый маркер. Так как идентификатор безопасности SID учетной записи не меняется, ее разрешения и свойства также остаются прежними. Переименовать учетную запись, выполнив локальный вход на компьютер, можно следующим образом:

1. В оснастке **Локальные пользователи и группы** выберите требуемую папку — **Пользователи** или **Группы**.
2. В правой панели щелкните на требуемой учетной записи, выберите в контекстном меню команду **Переименовать** и введите новое имя учетной записи. Повторите, если необходимо, это действие для других учетных записей.

Переименовать учетную запись посредством групповой политики можно следующим образом:

1. В редакторе групповых политик откройте для редактирования требуемый объект групповой политики. Для настройки параметров компьютера разверните узел **Конфигурация компьютера\Настройка\Параметры панели управления** и выберите в нем узел **Локальные пользователи и группы**. Для настройки параметров пользователя разверните узел **Конфигурация пользователя\Настройка\Параметры панели управления** и выберите в нем узел **Локальные пользователи и группы**.
2. Далее выполните одно из следующих действий.
   - Если элемент предпочтений для пользователя или группы уже существует, откройте окно свойств пользователя или группы, дважды щелкнув на соответствующем элементе. В списке **Действие** выберите опцию **Обновить**. В поле **Переименовать** введите новое имя учетной записи и нажмите кнопку **ОК**.
   - Если элемент предпочтений для пользователя или группы еще не существует, его нужно создать, используя один из рассмотренных ранее методов. Так как пользователя или группу требуется переименовать, в списке **Действие** выберите опцию **Обновить**, а затем введите новое имя учетной записи в поле **Переименовать**.

Удаление локальных учетных записей пользователей и групп

Удаление учетной записи полностью уничтожает ее. Если после удаления учетной записи создать другую учетную запись с таким же именем, эта учетная запись не будет иметь тех же полномочий, что и удаленная, т. к. ее идентификатор безопасности SID будет другим.

Так как удаление учетной записи может иметь далеко идущие последствия для рабочей станции, Windows 8 не разрешает удаление встроенных учетных записей пользователей или групп. Другие типы учетных записей можно удалять в оснастке **Локальные пользователи и группы**. Для этого нужно щелкнуть на требуемой учетной записи правой кнопкой мыши и в контекстном меню выбрать опцию **Удалить**, а в окне запроса подтверждения удаления нажать кнопку **Да**.

> ***Примечание***
>
> При удалении локальной учетной записи пользователя с помощью оснастки **Локальные пользователи и группы** Windows 8 не удаляет профиль, личные файлы и домашнюю папку пользователя. Если эти файлы и папки требуется удалить, это нужно делать вручную.

Удалить учетную запись посредством групповой политики можно следующим образом:

1. В редакторе групповых политик откройте для редактирования требуемый объект групповой политики. Для настройки параметров компьютера разверните узел **Конфигурация компьютера\Настройка\Параметры панели управления** и выберите в нем узел **Локальные пользователи и группы**. Для настройки параметров пользователя разверните узел **Конфигурация пользователя\Настройка\Параметры панели управления** и выберите в нем узел **Локальные пользователи и группы**.
2. Далее выполните одно из следующих действий.
   - Если элемент предпочтений для пользователя или группы уже существует, откройте окно свойств пользователя или группы, дважды щелкнув на соответствующем элементе. В списке **Действие** выберите опцию **Удалить**. На вкладке **Общие** установите требуемый флажок, например **Применить один раз и не применять повторно**, а затем нажмите кнопку **OK**.
   - Если элемент предпочтений для пользователя или группы еще не существует, его нужно создать, используя один из рассмотренных ранее методов. Обязательно выберите опцию **Удалить** в списке **Действие**, а затем установите необходимые флажки на вкладке **Общие**.

Управление удаленным доступом к рабочим станциям

Операционная система Windows 8 имеет несколько функциональностей удаленного доступа. С помощью удаленного помощника (Remote Assistance) пользователи могут отправлять приглашения удаленным техническим специалистам поддержки, позволяя им выполнять техническое обслуживание компьютера удаленно. Возможность удаленного рабочего стола (Remote Desktop) позволяет пользователям подключаться к удаленному компьютеру и работать на нем. В этом разделе мы рассмотрим, как выполнять настройку удаленного помощника и удаленного рабочего стола. По умолчанию в Windows 8 возможности удаленного помощника и удаленного рабочего стола отключены, поэтому их необходимо включить вручную.

Возможности удаленного помощника и удаленного рабочего стола могут работать через брандмауэры NAT[1]. Функциональность удаленного помощника также имеет встроенные средства диагностирования. Чтобы упростить процесс поиска и устранения неполадок и разрешить передачу вопросов поддержки по инстанции, к удаленному компьютеру могут

[1] Network Address Translation — преобразование сетевых адресов.

одновременно подключаться два разных технических специалиста. Если в процессе диагностирования неполадки требуется перезагрузить компьютер, сеанс удаленного помощника автоматически возобновляется после перезагрузки диагностируемого компьютера.

Прежде чем прибегать к использованию удаленного помощника, пользователям желательно применить средство записи действий по воспроизведению неполадок (Problem Steps Recorder), чтобы создать пошаговую запись испытываемой ими проблемы. Работа со средством записи действий не представляет никакой трудности и осуществляется следующим образом:

1. Пользователь запускает средство записи действий. Один из способов сделать это — нажать клавишу <Windows>, ввести команду `psr`, а затем нажать клавишу <Enter>. Запустив инструмент, пользователь может подготовить среду, после чего начать запись проблемы.
2. Чтобы начать запись, на панели средства нужно нажать кнопку **Начать запись** (Start Record). Начав запись, пользователь может выполнить действие или последовательность действий, вызывающих проблему, и в процессе работы добавлять свои комментарии, нажимая для этого кнопку **Добавить комментарий** (Add Comment).
3. Когда на компьютере пользователя возникает проблема и выводятся связанные с ней сообщения, пользователь может закончить запись действий, нажав кнопку **Остановить запись** (Stop Record).
4. После остановки записи средство записи действий показывает все действия, выполненные пользователем в процессе записи проблемы. Теперь пользователь может сохранить запись, нажав кнопку **Сохранить** и указав в открывшемся диалоговом окне **Сохранить как** папку и имя zip-файла, содержащего запись проблемы в архивном mthtl-файле.
5. Пользователь может отправить zip-файл техническому специалисту поддержки по электронной почте или скопировав его на общий сетевой диск. Чтобы просмотреть записанные действия, вызывающие проблему, дважды щелкните на zip-файле, в результате чего его содержимое (т. е. mhtml-файл) отобразится в Проводнике Windows, а затем дважды щелкните на mhtml-файле — он откроется в Internet Explorer.
6. Этот файл содержит снимки экрана для всех действий, выполненных пользователем в процессе записи проблемы. Затем следуют дополнительные сведения для каждого действия, которые создаются автоматически. Эту информацию вместе с комментариями пользователя можно использовать в качестве вспомогательного средства при диагностировании проблемы.

Настройка удаленного помощника

Удаленный помощник является полезной функциональностью для службы технической поддержки, как собственной, так и привлекаемой извне. Посредством этой функциональности пользователь может позволить техническому специалисту просматривать и управлять его рабочим столом. Эту возможность можно использовать, чтобы пошагово провести пользователя через сложный процесс или для управления параметрами системы, в то время как пользователь наблюдает за выполняемыми изменениями. Ключевой особенностью удаленного помощника является уровень доступа, предоставляемого ему пользователем.

По умолчанию, после включения удаленного помощника его настройки позволяют удаленному техническому специалисту просматривать и управлять компьютером. Так как пользователи могут отправлять приглашения удаленного помощника с компьютеров компании и личных ПК, эти настройки могут представлять угрозу безопасности данных компании. Чтобы уменьшить уровень проблем безопасности, желательно разрешить удаленному помощ-

нику просматривать компьютер, но не управлять им. Компьютеры под управлением Windows Vista разрешают подключения удаленного помощника только с компьютеров, на которых установлена Windows Vista или более поздняя версия Windows.

Это обстоятельство полезно тем, что оно позволяет ограничить возможные проблемы совместимости и обеспечить наличие в сеансах с удаленным помощником улучшенных мер безопасности Windows Vista или более поздних версий Windows.

Другим ключевым аспектом удаленного помощника является возможность управления периодом действия приглашения. По умолчанию максимальная длительность действия приглашения составляет 6 часов, а абсолютный максимальный период — 30 дней. Целью многодневного действия приглашения является предоставить персоналу технической поддержки временное окно, в течение которого ответить на запрос о помощи. Но в то же самое время это означает, что сотрудники технической поддержки могут использовать приглашение для доступа к компьютеру в любое время в течение действия приглашения. Например, допустим, специалист поддержки получает приглашение удаленному помощнику со сроком действия 30 дней. Если он решит проблему в первый день действия приглашения, у него все равно будет возможность доступа к компьютеру в течение 29 оставшихся дней действия приглашения. Такое развитие событий будет нежелательным по причинам безопасности. Чтобы уменьшить степень риска, которому подвержена система, обычно желательно значительно сократить максимальное время действия приглашения по умолчанию, скажем, до 1 часа. Если проблема не решится в течение этого периода, всегда можно создать другое приглашение.

Настройка удаленного помощника выполняется следующим образом:

1. В Панели управления щелкните по ссылке категории **Система и безопасность**, а затем в разделе **Система** — по ссылке **Настройка удаленного доступа** (Allow remote access). Откроется окно **Свойства системы** на вкладке **Удаленный доступ** (Remote) (рис. 7.13).
2. Чтобы отключить функциональность удаленного помощника, снимите флажок **Разрешить подключения удаленного помощника к этому компьютеру** (Allow Remote Assistance connections to this computer). Пропустите последующие шаги.
3. Чтобы включить функциональность удаленного помощника, установите флажок **Разрешить подключения удаленного помощника к этому компьютеру**.
4. Далее нажмите кнопку **Дополнительно** (Advanced). Откроется диалоговое окно **Параметры удаленного помощника** (Remote Assistance Settings) (рис. 7.14).
5. Установка флажка **Разрешить удаленное управление этим компьютером** (Allow this computer to be controlled remotely) разрешает удаленному помощнику кроме просмотра данного компьютера еще и управлять им. Чтобы разрешить только просмотр компьютера, снимите этот флажок.
6. В разделе **Приглашения** (Invitations) устанавливается максимальное время действия создаваемого приглашения. Этот период можно указать в минутах, часах или днях, вплоть до абсолютного максимума в 30 дней. (Хотя в поле установки значения периода можно задать 99 дней, при нажатии кнопки **OK** выводится предупреждение, что максимальное значение 30 дней, и при нажатии кнопки **OK** окна этого сообщения значение дней сбрасывается до 30.) Если задать здесь период действия приглашения, например, 10 дней, срок действия создаваемых пользователями приглашений не сможет превышать 10 дней. По умолчанию максимальный срок действия приглашения равен 6 часам.
7. Завершив настройки параметров удаленного помощника, дважды нажмите кнопку **OK**, чтобы сохранить настройки и закрыть окна.

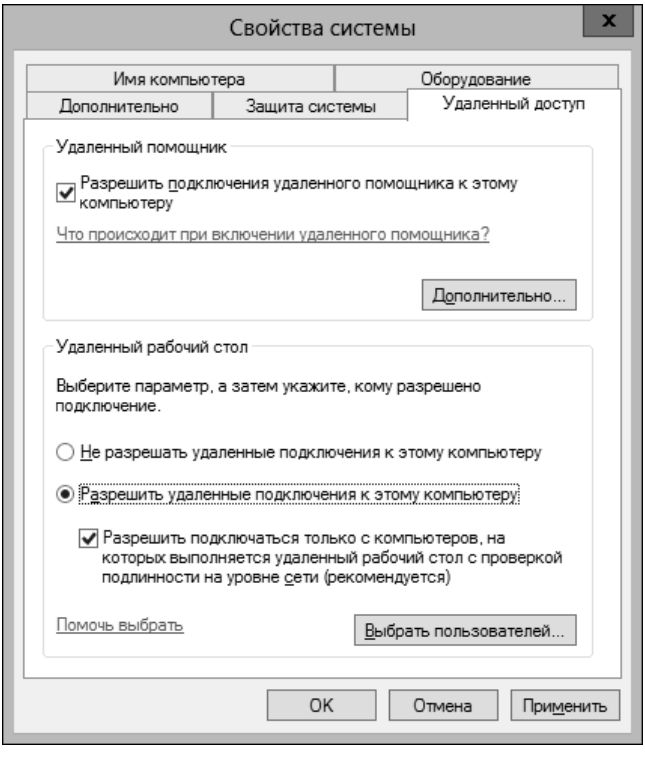


Рис. 7.13. Вкладка **Удаленный доступ** окна **Свойства системы**

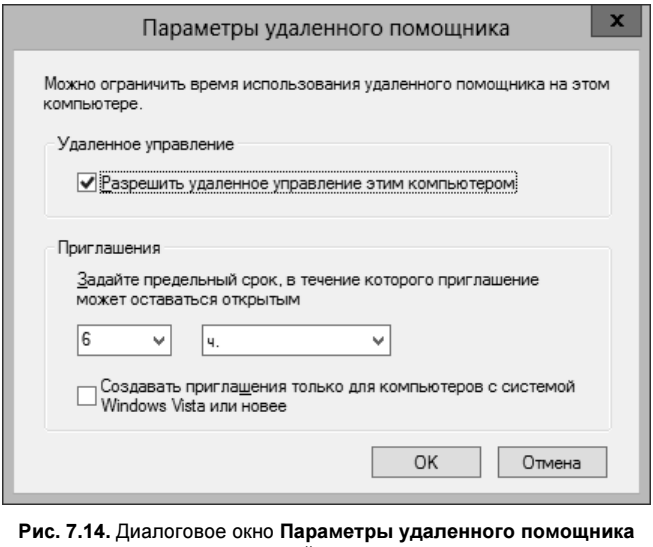


Рис. 7.14. Диалоговое окно **Параметры удаленного помощника** применяется для установки времени действия приглашения удаленному помощнику

В групповой политике управлять удаленным помощником можно, используя параметры политики, перечисленные в табл. 7.2. Эти параметры находятся в указанных в таблице узлах в разделе **Конфигурация компьютера\Административные шаблоны**.

Таблица 7.2. *Параметры политики для управления удаленным помощником*

Параметр	Путь
Разрешить подключение только с компьютеров под управлением Windows Vista или более поздней версии (Allow only Windows Vista or later connections)	Система\Удаленный помощник
Настроить предлагаемую удаленную помощь (Configure Offer Remote Assistance)	Система\Удаленный помощник
Настроить запрашиваемую удаленную помощь (Configure Solicited Remote Assistance)	Система\Удаленный помощник
Включить ведение журнала сеансов (Turn on session logging)	Система\Удаленный помощник

Настройка доступа к удаленному рабочему столу

В отличие от функциональности удаленного помощника, которая позволяет только удаленно просматривать рабочий стол пользователя, удаленный рабочий стол предоставляет несколько уровней доступа.

- Если пользователь выполнил вход на компьютер локально, а затем выполняет удаленный вход, локальный рабочий стол блокируется, и пользователь может работать с удаленным рабочим столом, включая выполнение всех программ, как будто бы это локальный компьютер. Эта функциональность полезна для пользователей, которые хотят работать из дома или другого места вне офиса и использовать приложения и документы, с которыми они работали в офисе.
- Если пользователь внесен в список удаленного доступа рабочей станции и иным образом не выполнил вход в систему, он может инициировать новый сеанс Windows. Сеанс Windows имитирует работу пользователя за локальным компьютером. Сеанс Windows также можно использовать, когда в систему выполнили вход другие пользователи. Таким образом, несколько пользователей могут одновременно использовать одну рабочую станцию и ее ресурсы.

По умолчанию удаленный рабочий стол отключен. Его нужно явно включить, чтобы разрешить удаленный доступ к рабочей станции. Когда удаленный рабочий стол включен, к рабочей станции может подключаться любой член группы **Администраторы**. Чтобы другие пользователи могли подключаться, их нужно поместить в список пользователей удаленного доступа. Настройка функциональности удаленного доступа выполняется следующим образом:

1. В Панели управления щелкните по ссылке категории **Система и безопасность** и в открывшемся списке элементов этой категории выберите ссылку **Система**.
2. В левой панели окна **Система** щелкните по ссылке **Настройка удаленного доступа** (Remote Settings). Откроется диалоговое окно **Свойства системы** на вкладке **Удаленный доступ** (см. рис. 7.13).
3. Чтобы отключить удаленный рабочий стол, установите переключатель **Не разрешать удаленные подключения к этому компьютеру** (Don't allow remote connections to this computer) и нажмите кнопку **OK**. Пропустите все следующие шаги.

4. Чтобы включить удаленный рабочий стол:
   - установите переключатель **Разрешить удаленные подключения к этому компьютеру** (Allow remote connections to this computer);
   - также установите флажок **Разрешить подключаться только с компьютеров, на которых выполняется удаленный рабочий стол с проверкой подлинности на уровне сети** (Allow connections only from computers running Remote Desktop with Network Level Authentication), чтобы разрешить подключения только для компьютеров под управлением Windows Vista или более поздними версиями Windows (а также компьютеров, на которых применяется безопасная сетевая аутентификация).
5. Нажмите кнопку **Выбрать пользователей**. Откроется диалоговое окно **Пользователи удаленного рабочего стола** (Remote Desktop Users) (рис. 7.15).

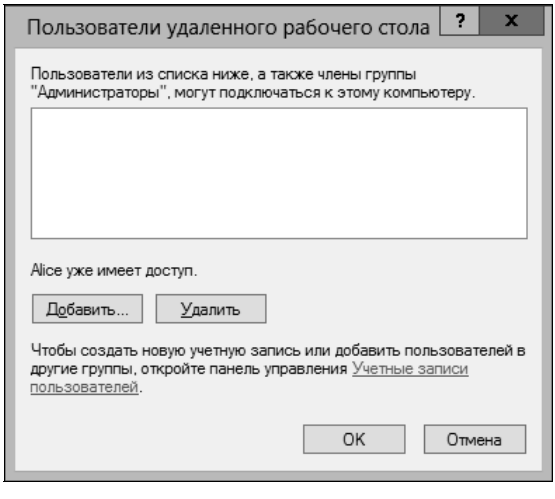


Рис. 7.15. Диалоговое окно для выбора пользователей, которым разрешено удаленное подключение к компьютеру

6. Чтобы добавить пользователя удаленного рабочего стола, нажмите кнопку **Добавить**. В открывшемся диалоговом окне **Выбор: "Пользователи"** нажмите кнопку **Размещение** (Locations), чтобы выбрать компьютер или домен, в котором находятся требуемые учетные записи. Введите имя пользователя, которому нужно разрешить работу с удаленным рабочим столом, в текстовое поле **Введите имена выбираемых объектов**, а затем нажмите кнопку **Проверить имена**. Если для указанного имени найдутся совпадения, они будут отображены в поле ввода. Выберите из них требуемую учетную запись и нажмите кнопку **OK**. При отсутствии совпадений исправьте введенное имя и повторите попытку. Повторите процесс поиска, пока не будут добавлены все требуемые пользователи, после чего нажмите кнопку **OK**.
7. Чтобы удалить пользователя из списка разрешенных пользователей удаленного рабочего стола, в диалоговом окне **Пользователи удаленного рабочего стола** выберите требуемую учетную запись и нажмите кнопку **Удалить**.
8. Завершив добавление и удаление пользователей, нажмите кнопку **OK**, чтобы сохранить настройки и закрыть диалоговое окно.

Для работы удаленного рабочего стола в брандмауэре Windows необходимо разрешить входящие исключения для удаленного стола. Для отдельных компьютеров это можно сделать

в брандмауэре Windows для доменного и общего профиля. В групповой политике это исключение можно настроить, используя параметры политики, представленные в табл. 7.3. Эти параметры находятся в указанных в таблице узлах в разделе **Конфигурация компьютера\Административные шаблоны**.

Таблица 7.3. *Параметры политики для управления удаленным рабочим столом*

Параметр	Путь конфигурации компьютера
	Путь в подузле **Компоненты Windows\Службы удаленных рабочих столов** (Windows Components\Remote Desktop Services)
Разрешать RDP-файлы от неизвестных издателей (Allow .rdp files from unknown publishers)	**Клиент подключения к удаленному рабочему столу** (Remote Desktop Connection Client)
Разрешать RDP-файлы от допустимых издателей и пользовательские параметры RDP, заданные по умолчанию (Allow .rdp files from unknown publishers and user's default rdp settings)	**Клиент подключения к удаленному рабочему столу** (Remote Desktop Connection Client)
Всегда запрашивать пароль при подключении (Always prompt for password upon connection)	**Узел сеансов удаленных рабочих столов\Безопасность** (Remote Desktop Session Host\Security)
Автоматическое переподключение (Automatic reconnection)	**Узел сеансов удаленных рабочих столов\Подключения** (Remote Desktop Session Host\Connections)
Настройка проверки подлинности клиента (Configure server authentication for client)	**Клиент подключения к удаленному рабочему столу** (Remote Desktop Connection Client)
Запретить завершение консольного сеанса администратора (Deny logoff of an administrator logged in to the console session)	**Узел сеансов удаленных рабочих столов\Подключения** (Remote Desktop Session Host\Connections)
Не разрешать локальным администраторам настраивать разрешения (Do not allow local administrators to customize permissions)	**Узел сеансов удаленных рабочих столов\Безопасность** (Remote Desktop Session Host\Security)
Запретить сохранение паролей (Do not allow passwords to be saved)	**Клиент подключения к удаленному рабочему столу** (Remote Desktop Connection Client)
Наибольшая глубина цвета (Limit maximum color depth)	**Узел сеансов удаленных рабочих столов\Среда удаленных сеансов** (Remote Desktop Session Host\Remote Session Environment)
Ограничить максимальное разрешение экрана (Limit maximum display resolution)	**Узел сеансов удаленных рабочих столов\Среда удаленных сеансов** (Remote Desktop Session Host\Remote Session Environment)
Ограничить количество мониторов (Limit number of monitors)	**Узел сеансов удаленных рабочих столов\Среда удаленных сеансов** (Remote Desktop Session Host\Remote Session Environment)

Таблица 7.3 *(окончание)*

Параметр	Путь конфигурации компьютера
Ограничить размер всего кэша перемещаемых профилей пользователей (Limit the size of the entire roaming user profile cache)	**Узел сеансов удаленных рабочих столов\Профили** (Remote Desktop Session Host\Profiles)
Требовать использования специального уровня безопасности для удаленных подключений по протоколу RDP (Require use of specific security layer for remote (RDP) connections)	**Узел сеансов удаленных рабочих столов\Безопасность** (Remote Desktop Session Host\Security)
Установить уровень шифрования для клиентских подключений (Set client connection encryption level)	**Узел сеансов удаленных рабочих столов\Безопасность** (Remote Desktop Session Host\Security)
Выбор транспортных протоколов RDP (Select RDP transport protocols)	**Узел сеансов удаленных рабочих столов\Подключения** (Remote Desktop Session Host\Connections)
Выбор способа определения сети на сервере (Select network detection on the server)	**Узел сеансов удаленных рабочих столов\Подключения** (Remote Desktop Session Host\Connections)
Указать отпечатки SHA1 сертификатов, представляющих доверенных издателей RDP (Specify SHA1 thumbprints of certificates representing trusted .rdp publishers)	**Клиент подключения к удаленному рабочему столу** (Remote Desktop Connection Client)
Отключить планирование ЦП со справедливым разделением (Turn off fair share CPU scheduling)	**Узел сеансов удаленных рабочих столов\Подключения** (Remote Desktop Session Host\Connections)
	Другие пути
Запретить удаленное управление рабочим столом (Disable remote Desktop Sharing)	**Компоненты Windows\NetMeeting** (Windows Components\NetMeeting)
Брандмауэр Windows: Разрешить исключения для входящих сообщений удаленного управления рабочим столом (Windows Firewall: Allow inbound Remote Desktop exceptions)	**Сеть\Сетевые подключения\Брандмауэр Windows\Профиль домена** (Network\Network Connections\Windows Firewall\Domain Profile)
Брандмауэр Windows: Разрешить исключения для входящих сообщений удаленного управления рабочим столом (Windows Firewall: Allow inbound Remote Desktop exceptions)	**Сеть\Сетевые подключения\Брандмауэр Windows\Стандартный профиль** (Windows\Network Connections\Windows Firewall\Standard Profile)

Создание подключений к удаленному рабочему столу

Администратор может создавать подключения к удаленному рабочему столу серверов и рабочих станций под управлением Windows. Для компьютеров под управлением Windows 2000 Server функциональность подключения к удаленному рабочему столу обеспечивается установкой служб удаленных рабочих столов с последующей настройкой этих служб для удаленного доступа. С Windows XP Professional и более поздними версиями функциональность удаленного стола устанавливается автоматически. Но по умолчанию эта функ-

циональность отключена, и для ее использования ее нужно включить, как рассмотрено в предыдущем разделе. Когда на компьютере включен удаленный доступ, все администраторы могут выполнять удаленное подключение к нему. Другим пользователям также можно предоставить полномочия для подключения.

Создать подключение к удаленному рабочему столу сервера или рабочей станции можно следующим образом:

1. Откройте окно подключения к удаленному рабочему столу, выполнив в консоли командной строки команду `mstc`. Эту команду также можно выполнить, нажав клавишу <Windows>, а затем введя ее в поле поиска панели **Приложения** и нажав клавишу <Enter>.
2. Щелкните по ссылке **Показать параметры** (Show Options). Окно подключения примет вид, показанный на рис. 7.16.

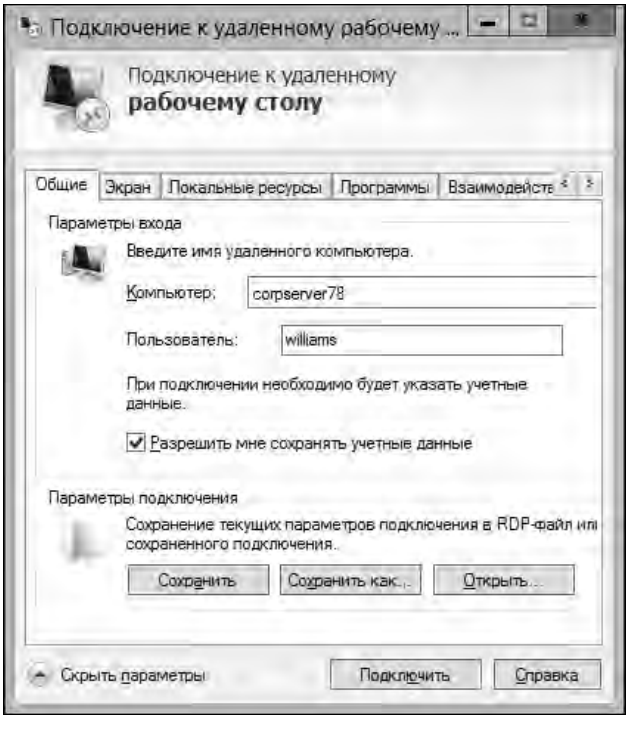


Рис. 7.16. Окно подключения к удаленному рабочему столу с отображаемым разделом параметров

3. Введите в поле **Компьютер** имя компьютера, к которому требуется подключиться. Если имя компьютера неизвестно, его можно выбрать из раскрывающегося списка, или же выбрать в этом списке опцию **Найти другие** (Browse for more), чтобы вывести список доменов и компьютеров в этих доменах.
4. Установите другие необходимые параметры. Если для компьютера, к которому выполняется подключение, были сохранены учетные данные, эти учетные данные будут использованы автоматически. Учетные данные можно редактировать и удалять, как требуется.
5. Нажмите кнопку **Подключить**. Если учетные данные для компьютера, к которому выполняется подключение, не были сохранены, введите эти учетные данные в окно запро-

са, а затем нажмите кнопку **OK**. При успешном подключении на экране локального компьютера будет выведен рабочий стол удаленного компьютера, и можно будет работать с ресурсами этого компьютера. В случае проблем с подключением проверьте установленные вами параметры подключения, а также настройки удаленного доступа к компьютеру и повторите попытку.

Примечание

При нажатии в диалоговом окне **Подключение к удаленному рабочему столу** кнопки **Показать параметры** это окно расширяется набором вкладок, на которых можно задать значения дополнительных параметров для создания и сохранения подключений. В частности, эти параметры позволяют изменять размер экрана удаленного рабочего стола, управлять подключением локальных ресурсов (таких, как принтеры, последовательные порты и приводы дисков), автоматически исполнять программы после подключения, а также управлять локальным кэшированием и сжатием данных.

ГЛАВА 8

Установка и обслуживание приложений

Программы настольных компьютеров представляют собой приложения, которые можно устанавливать и настраивать. Для установки большинства настольных программ используется установщик Windows (Windows Installer), что значительно упрощает задачу установки. Администраторам и персоналу технической поддержки часто приходится устанавливать и настраивать программы, используемые в настольных компьютерах. Вам, может, придется устанавливать и настраивать программы при развертывании новых компьютеров, устанавливать новые программы на компьютеры, находящиеся в эксплуатации, для удовлетворения требований пользователей, а также обновлять программы при выходе их новых версий. Кроме этого, ваша помощь может понадобиться для диагностирования проблем с устанавливаемыми пользователями программами или для удаления установленных программ.

Большинство проблем с установкой программ решаются сравнительно легко, если знать, на что нужно обращать внимание. Но при установке программ могут возникнуть и более трудные проблемы, на решение которых может потребоваться больше времени, чем ожидается. В этой главе мы рассмотрим влияние функциональности контроля учетных записей пользователей на установку и выполнение программ, а также методы установки, обслуживания и удаления программ. Кроме этого, мы рассмотрим установку и настройку приложений рабочего стола. Хотя термины *"приложения"* и *"программное обеспечение"* обычно обозначают как настольные программы, так и приложения рабочего стола, которые также являются программами в наиболее общем смысле этого слова, важно понимать различия между настольными программами и приложениями рабочего стола[1].

В этой главе внимание главным образом уделяется настольным программам. Но сначала мы рассмотрим приложения рабочего стола.

---

[1] В оригинале — "desktop programs" и "desktop apps", именно "apps", а не "applications". И далее вместо полного термина "desktop apps" используется просто "apps". Различие между "desktop programs/applications" и "desktop apps"/"apps", как употребляется автором, следующее: первые — это классические приложения, исполняющиеся на настольных компьютерах, а вторые — это специализированные приложения, значки которых расположены в виде плиток на экране **Пуск** Windows 8, и выполняются на рабочем столе. Это такие приложения, как Календарь, Почта, Люди, Погода и т. д.

По-русски, первые будут (в данном переводе этой книги) "настольными приложениями", т. е. приложениями для настольных компьютеров, а вторые — "приложениями рабочего стола", т. е. специальными приложениями Windows 8, выполняющимися на рабочем столе компьютера.

Управление приложениями рабочего стола

Приложения рабочего стола впервые начали применяться в Windows 8. Их можно приобрести в Магазине Windows (Windows Store) и установить через Интернет. Эти приложения также можно разрабатывать силами сотрудников организации или приобретать у сторонних разработчиков и устанавливать посредством групповой политики. Хотя приложениями рабочего стола можно управлять, используя методы, применяемые для управления настольными приложениями, приложения рабочего стола имеют много отличительных особенностей.

Основы работы с приложениями рабочего стола

В Windows 8 традиционное меню **Пуск** предыдущих версий операционной системы заменено экраном **Пуск**. При установке приложения рабочего стола на экран **Пуск** автоматически помещается его значок в виде плитки, что упрощает запуск приложения и его управление. При щелчке правой кнопкой мыши по плитке приложения отображаются опции для его управления, которые зависят от типа плитки. Например, активные плитки могут обновлять выводимое в них содержимое, и эту функциональность можно включить или отключить. Размер некоторых плиток можно изменить, выбрав соответствующую опцию. Плитку можно убрать с экрана **Пуск**, выбрав в панели меню опцию **Открепить от экрана "Пуск"** (Unpin from Start).

Управлять убранным с экрана **Пуск** приложениями, включая их запуск, можно несколькими разными способами. Один из таких способов — посредством списка **Все приложения** (All apps)[1]. В Windows 8 список **Все приложения** равнозначен меню **Все программы** в предыдущих версиях Windows. С экрана **Пуск** список **Все приложения** можно отобразить, щелкнув правой кнопкой мыши на пустой области экрана **Пуск**, а затем щелкнув левой кнопкой по значку **Все приложения** в правом нижнем углу экрана.

> ***Примечание***
>
> Настольные программы нельзя автоматически добавлять на экран **Пуск** или в список **Все приложения**. Дополнительную информацию *см. в разд. "Предоставление программ всем или только отдельным пользователям" далее в этой главе*.

При работе с приложениями рабочего стола и их плитками на экране **Пуск** можно использовать следующие комбинации клавиш быстрого вызова, которые также применимы и для обычных программ:

- <Windows>+<←> или <Windows>+<→> переключают позицию закрепления окна приложения. Комбинация клавиш <Windows>+<←> закрепляет окно у левого края экрана, а комбинация клавиш <Windows>+<→> — у правого;
- <Windows>+<↑> отображает приложение в полноэкранном режиме;
- <Windows>+<↓> выводит приложение из полноэкранного режима и возвращает его в исходный оконный режим.

[1] В данном случае слово "apps" имеет не узкое значение приложений рабочего стола, как используется автором, но все установленные на компьютере приложения, как объясняется дальше в тексте.

Настройка доверенных приложений рабочего стола и доступа к Магазину Windows

Обычно приложения рабочего стола устанавливаются и обновляются по Интернету. По умолчанию компьютеры под управлением Windows 8 могут устанавливать только пакеты доверенных приложений, полученные из Магазина Windows. Чтобы разрешить установку доверенных приложений рабочего стола собственной или сторонней разработки, нужно включить параметр **Разрешить установку всех доверенных приложений** (Allow all trusted apps to install) политики **Развертывание пакета приложения** (App package deployment), которая находится в узле **Конфигурация компьютера\Административные шаблоны\Компоненты Windows** редактора локальной групповой политики.

Управлять доступом пользователей к Магазину Windows можно несколькими способами, включая перечисленные далее.

- Контролировать использование на компьютере учетных записей Microsoft, включив политику **Учетные записи: блокировать учетные записи Майкрософт** (Accounts:Block Microsoft accounts). Эта политика находится в узле **Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики\Параметры безопасности** (Computer Configuration\Windows Configuration\Security Settings\Local Policies\Security Options) редактора локальных групповых политик. Эта политика имеет две опции. Опция **Пользователи не могут добавлять учетные записи Майкрософт** (Users can't add Microsoft accounts) запрещает пользователям создавать учетные записи Microsoft, а опция **Пользователи не могут добавлять учетные записи Майкрософт и использовать их для входа** (Users can't add or log on with Microsoft accounts) запрещает пользователям как создавать учетные записи Microsoft, так и выполнять по ним вход в систему.
- Запретить пользователям доступ к Магазину Windows, включив параметр **Turn off the Store application** политики **Store**. Эта политика находится в узле **Конфигурация компьютера\Административные шаблоны\Компоненты Windows** редактора локальных групповых политик.
- Запретить автоматическую загрузку обновлений для приложений рабочего стола, включив параметр **Turn off Automatic Download of updates** политики **Store**.

Повышение безопасности приложений рабочего стола и переопределение настроек по умолчанию

Приложения рабочего стола выполняются в особом контексте и имеют более низкий уровень безопасности, чем обычные настольные приложения. Более низкий уровень безопасности ведет к тому, что приложения могут выполнять операции, способные нарушить безопасность системы, т. к. для обычных приложений выполнение таких операций нуждается в согласии пользователя, чего не требуется для приложений рабочего стола. Например, по умолчанию приложения рабочего стола могут открывать файл в обычной программе, связанной с данным типом файла. В случае файла или протокола, для которого отсутствует зарегистрированное приложение, открывается окно **Выбор программы** (Open With) для выбора локальной программы открытия файла незарегистрированного типа. Альтернативно, пользователь может использовать службу Магазина для выбора подходящей программы.

Безопасность системы можно повысить, запретив такое поведение одним или несколькими из следующих способов.

- Чтобы не допустить автоматического открытия приложением рабочего стола программы, связанной с данным типом файла, нужно включить параметр **Блокировать запуск приложений рабочего стола, связанных с файлом** (Block launching desktop apps associated with a file) политики **Среда выполнения приложения** (App runtime). Эта политика находится в узле **Конфигурация компьютера** (и **Конфигурация пользователя**)**\Административные шаблоны\Компоненты Windows**.
- Чтобы не допустить автоматического открытия приложением рабочего стола программы, связанной с данным типом протокола, нужно включить параметр **Блокировать запуск приложений рабочего стола, связанных с протоколом** (Block launching desktop apps associated with a protocol) политики **Среда выполнения приложения**. Эта политика находится в узле **Конфигурация компьютера** (и **Конфигурация пользователя**)\ **Административные шаблоны\Компоненты Windows**.
- Чтобы удалить опцию **Магазин Windows** из диалогового окна **Выбор программы**, следует включить параметр **Отключить доступ к Магазину** (Turn off access to the Store) политики **Параметры связи через Интернет** (Internet Communication settings). Эта политика находится в узле **Конфигурация компьютера\Административные шаблоны\ Система\Управление связью через Интернет** (Computer Configuration\Administrative Templates\System\Internet Communication Management).

Важно отметить, что некоторые приложения рабочего стола могут выводить уведомления на экране блокировки и по умолчанию ведется журнал состояния уведомлений. Благодаря ведению журнала состояния уведомлений, выполнив вход в систему, пользователь будет видеть уведомления в том же состоянии, в котором они были при его последнем выходе из системы. Чтобы заблокировать вывод уведомлений на экране блокировки, следует включить параметр **Отключить уведомления приложений на экране блокировки** политики **Вход в систему**. Эта политика находится в узле **Конфигурация компьютера\Административные шаблоны\Система\Вход в систему** редактора локальной групповой политики. Чтобы при выходе пользователя из системы очищать журнал состояний уведомлений, нужно включить параметр **Очистить журнал уведомлений на плитке при выходе** (Clear history of tile notifications on exit) политики **Меню "Пуск" и панель задач** (Start Menu and Taskbar). Эта политика находится в узле **Конфигурация пользователя\Административные шаблоны** редактора локальной групповой политики.

Приложения рабочего стола получают уведомления посредством службы WNS[1]. Активные приложения рабочего стола используют службу WNS для обновления содержимого на своей плитке, вывода уведомлений и получения извещений. Различными аспектами службы WNS можно управлять посредством параметров политики **Уведомления**, которая находится в узле **Конфигурация пользователя\Административные шаблоны\Меню "Пуск" и панель задач** редактора локальной групповой политики. В частности:

- Заблокировать вывод всплывающих уведомлений[2] обычно можно, включив параметр **Отключить всплывающие уведомления** (Turn off toast notifications) этой политики. Данный параметр не влияет на всплывающие сообщения панели задач.
- А уведомления, которые выводятся на экране блокировки, можно отключить, включив параметр **Отключить всплывающие сообщения на экране блокировки** (Turn off toast notifications on the lock screen).
- Заблокировать обновления плиток и их заголовков на экране приветствия можно, включив параметр **Turn off tile notifications**.

---

[1] Windows Push Notification Service — служба push-уведомлений Windows.

[2] Англ. *toast notifications.*

- Запретить отправление приложениями рабочего стола извещений для обновлений и уведомлений можно, включив параметр **Turn off notifications network usage** и тем самым отключив соединение Windows со службой WNS.

Практический совет

В Windows 8 использование приложений рабочего стола отслеживается различными способами. Управлять отслеживанием использования приложений рабочего стола можно посредством параметров политики **Пользовательский интерфейс границ** (Edge UI), расположенной в узле **Конфигурация пользователя\Административные шаблоны\Компоненты Windows** редактора локальной групповой политики.

Повышение сетевой безопасности для приложений рабочего стола

Операционная система Windows 8 поддерживает несколько новых сетевых функциональностей, связанных с приложениями в общем и с приложениями рабочего стола в частности. Для автоматического обнаружения прокси-серверов и частных сетевых узлов при подключении компьютера к домену в Windows 8 используется сетевая изоляция Windows (Windows network isolation). По умолчанию любой обнаруженный прокси-сервер считается достоверным и любой сетевой узел может быть обнаружен посредством частных подсетей, доступных данному компьютеру.

Обнаружение прокси-серверов и обнаружение частных сетевых узлов являются отдельными функциональностями. Процесс обнаружения прокси-серверов управляется посредством параметров политики **Сетевая изоляция** (Network Isolation), которая находится в узле **Конфигурация компьютера\Административные шаблоны\Сеть** редактора локальной групповой политики. Для этого нужно включить параметр **Internet proxy servers for apps** и ввести разделенный запятыми список достоверных прокси-серверов домена, которые приложения рабочего стола, исполняющиеся на подключенных к домену компьютерах, могут использовать для доступа к Интернету. По умолчанию этот список прокси-серверов сливается со списком автоматически обнаруженных прокси-серверов. Если требуется, чтобы достоверными считались только прокси-серверы введенного списка, следует включить параметр **Определения прокси-серверов достоверны** (Proxy definitions are authoritative).

Для определения достоверных прокси-серверов для частных сетей нужно включить параметр **Intranet proxy servers for apps** и ввести разделенный запятыми список прокси-серверов, предоставляющих доступ к ресурсам внутрикорпоративной сети. Если требуется, чтобы достоверными считались только прокси-серверы введенного списка, включите параметр **Определения прокси-серверов достоверны**.

Параметры политики **Сетевая изоляция** также используются для управления обнаружением частных сетевых узлов. Обнаруженные таким способом узлы обозначаются как частные. Обычно процесс обнаружения частных сетевых узлов не пересекает границ подсетей.

Процесс обнаружения можно улучшить, включив параметр **Private network ranges for apps** и введя разделенный запятыми список подсетей IPv4 и IPv6 своей компании. Таким образом для Windows указываются доступные подсети, в которых можно выполнять обнаружение частных сетевых узлов. По умолчанию этот список подсетей сливается со списком автоматически обнаруженных подсетей. При включении параметра **Определения подсети являются достоверными** (Subnet definitions are authoritative) только сетевые узлы, находящиеся в диапазоне адресов, указанных в параметре **Private network ranges for apps**, будут обнаружены и считаться частными.

Управление виртуализацией и уровнем выполнения приложений

Контроль учетных записей изменяет способ установки и выполнения приложений, разрешенные для записи данных области, а также полномочия приложения. В этом разделе мы рассмотрим, каким образом контроль учетных записей влияет на установку приложений, включая маркеры безопасности приложений, виртуализацию файлов и реестра и уровни выполнения. Эта информация представляет большую важность для установки и обслуживания приложений в Windows 8.

Маркеры доступа приложений и виртуализация приложений

Все используемые с Windows 8 приложения делятся на две общие категории.

- **Приложения, отвечающие требованиям контроля учетных записей.** Любое приложение, разработанное специально для Windows Vista или более поздних версий Windows, считается отвечающим этим требованиям. Приложения, сертифицированные как отвечающие архитектурным требованиям Windows 8, имеют логотип соответствия требованиям контроля учетных записей.
- **Унаследованные приложения.** Любое приложение, разработанное для Windows XP или более ранних версий Windows, считается унаследованным (legacy application).

Разница между приложениями, отвечающими требованиям контроля учетных записей, и унаследованными приложениями важна вследствие архитектурных изменений, необходимых для поддержки контроля учетных записей. Приложения, отвечающие требованиям контроля учетных записей, используют эту функциональность для сокращения возможных "дыр" в операционной системе, уязвимых для злоумышленных атак. Это достигается предотвращением установки и выполнения несанкционированных приложений путем запроса согласия пользователя и ограничением полномочий, предоставляемых приложениям по умолчанию. Эти меры усложняют внедрение злоумышленного программного обеспечения в компьютер.

> ***Примечание***
>
> За контроль учетных записей отвечает служба сведений о приложениях. Эта служба упрощает выполнение интерактивных приложений с маркерами доступа администратора (т. е. запущенных с правами администратора). Разницу между маркерами доступа администратора и стандартного пользователя можно увидеть, открыв одновременно два окна консоли командной строки: одно с полномочиями администратора (щелкнув по значку приложения правой кнопкой мыши и выбрав команду **Запуск от имени администратора**), а другое с полномочиями обычного пользователя. Выполните в каждом окне команду `whoami /all` и сравните результаты. Оба маркера доступа имеют одинаковые идентификаторы безопасности SID, но маркер доступа пользователя с повышенными полномочиями администратора имеет больше полномочий, чем маркер доступа стандартного пользователя.

Контекст безопасности всех выполняющихся в Windows 8 приложений определяется маркером доступа текущего пользователя. По умолчанию контроль учетных записей делает всех пользователей стандартными пользователями, даже если они и являются членами группы **Администраторы**. Если пользователь-администратор соглашается использовать полномочия администратора, для него создается новый маркер доступа. Этот маркер содержит все полномочия пользователя, и для запуска приложений и процессов применяется этот маркер, а не стандартный маркер доступа этого пользователя.

В Windows 8 большинство приложений могут выполняться, используя маркер доступа стандартного пользователя. Необходимый для приложения тип полномочий — стандартного пользователя или администратора — зависит от выполняемых приложением действий. Приложения, требующие полномочий администратора (они называются *приложениями пользователя-администратора*), отличаются от приложений, для которых требуются полномочия стандартного пользователя (называются *приложениями стандартного пользователя*), следующим образом.

- Приложениям пользователя-администратора для запуска и выполнения основных задач требуются повышенные полномочия. После запуска в режиме повышенных полномочий приложение с маркером доступа пользователя-администратора может выполнять действия, требующие полномочий администратора, а также осуществлять запись в системные области реестра и файловой системы.
- Приложениям стандартного пользователя для запуска и выполнения основных задач не требуются повышенные полномочия. После запуска в режиме стандартного пользователя приложение с маркером доступа стандартного пользователя должно запрашивать повышение полномочий для выполнения задач администрирования. Для решения всех других задач приложение не должно выполняться с использованием повышенных полномочий. Кроме этого, приложение должно записывать данные только в несистемные области реестра и файловой системы.

Приложения, которые не были разработаны специально для Windows 8, по умолчанию запускаются с маркером доступа стандартного пользователя. Для работы с архитектурой контроля учетных записей эти приложения выполняются в специальном режиме совместимости, и для них применяются виртуализованные представления файлов и разделов реестра. Когда приложение пытается выполнить запись в системную область, Windows 8 предоставляет ему личную копию файла или раздела реестра. Любые изменения записываются в эту личную копию, которая сохраняется в данных профиля пользователя. Если приложение снова пытается выполнить запись в эту системную область, ему предоставляется копия этой области из профиля пользователя. По умолчанию, в случае ошибки в процессе работы приложения с виртуализированными данными, в извещении об ошибке и записанных в журнал сведениях указывается виртуализированная область, а не действительная, с которой приложение пыталось работать.

Безопасность и уровень выполнения приложений

Акцент на полномочиях стандартного пользователя и пользователя-администратора также изменяет общие полномочия, требуемые для установки и запуска приложений. В Windows XP и более ранних версиях Windows специальные полномочия администратора на выполнение основных системных заданий при установке и запуске приложений пользователям предоставляло членство в группе **Опытные пользователи**.

Для приложений, разработанных специально для Windows 8, использование группы **Опытные пользователи** не требуется. Эта группа содержится в Windows 8 только для целей обратной совместимости с унаследованными приложениями.

Контроль учетных записей предписывает Windows 8 по умолчанию определять попытку установки приложения и выводить запрос на повышение полномочий пользователя, чтобы продолжить установку. Пакеты установки для приложений, отвечающие требованиям контроля учетных записей, используют манифесты приложений, которые содержат определения уровня выполнения, используемые для отслеживания требуемых полномочий. В манифесте приложения полномочия приложения определяются, как одно из следующих значений.

- **RunAsInvoker.** Приложение выполняется с такими же полномочиями, какими обладает запускающий его пользователь. Приложение может запускаться пользователем любого типа. Для стандартного пользователя или пользователя члена группы **Администраторы** приложение выполняется с маркером доступа стандартного пользователя. Приложение запускается с более высокими полномочиями только в том случае, если запустивший его родительский процесс имеет маркер доступа пользователя-администратора. Например, приложение, запущенное из консоли командной строки, которая была открыта с повышенными полномочиями, выполняется с маркером доступа пользователя-администратора.
- **RunAsHighest.** Приложение выполняется с наивысшими полномочиями, которыми обладает запускающий его пользователь. Приложение может запускаться как пользователями-администраторами, так и стандартными пользователями. Тип заданий, которые может выполнять приложение, зависит от полномочий пользователя. Для стандартного пользователя приложение выполняется с маркером доступа стандартного пользователя. Для пользователя, который является членом группы с дополнительными полномочиями, такой как **Операторы архива**, **Операторы сервера** или **Операторы учетной записи**, приложение выполняется с частичным маркером пользователя-администратора, содержащим только те полномочия, которые были предоставлены пользователю его членством в определенной группе. Для пользователя-члена группы **Администраторы** приложение выполняется с маркером доступа пользователя-администратора.
- **RunAsAdmin.** Приложение выполняется с полномочиями администратора и может запускаться только администратором. Для стандартного пользователя или пользователя-члена группы с дополнительными полномочиями приложение запускается только в том случае, если для пользователя можно вывести запрос для предоставления учетных данных, требуемых для выполнения в режиме повышенных полномочий, или если приложение запускается из процесса с повышенными полномочиями, например, из консоли командной строки, имеющей такие полномочия. Для пользователя-члена группы **Администраторы** приложение выполняется с маркером доступа пользователя-администратора.

Чтобы защитить процессы приложения, Windows 8 присваивает им уровень целостности (integrity level) в диапазоне от высокого до низкого. Приложения, которые модифицируют системные данные, например средство **Управление дисками** (Disk Management), считаются приложениями высокой целостности. Приложения, выполняющие действия, которые могут подвергать опасности операционную систему, например Internet Explorer 8 в Windows 8, считаются приложениями низкой целостности. Приложения более низкого уровня целостности не могут изменять данные в приложениях более высокого уровня целостности.

Операционная система Windows 8 определяет издателя любого приложения, которое пытается запуститься с полным маркером доступа администратора. Затем, в зависимости от издателя, Windows 8 присваивает приложению одну из следующих трех категорий:

- Windows Vista или более поздняя версия Windows;
- издатель подтвержден (подписан);
- издатель не подтвержден (не подписан).

Чтобы облегчить определение потенциальной угрозы безопасности, представляемой установкой или запуском приложения, запрос на повышение полномочий с цветовым кодом содержит определенное сообщение, в зависимости от категории приложения.

- Если приложение принадлежит заблокированному издателю или блокируется групповой политикой, запрос на повышение полномочий имеет красный фон и отображает сообщение "Запуск приложения заблокирован" (The application is blocked from running).

- Для приложений администрирования (например, утилиты **Управление компьютером**) запрос на повышение полномочий имеет зеленый фон и содержит сообщение "Windows требуется разрешение на продолжение" (Windows needs your permission to continue).
- Если приложение имеет подпись "Authenticode" и является доверенным для локального компьютера, запрос на повышение полномочий имеет серый фон и отображает сообщение "Программе требуется разрешение на продолжение" (A program needs your permission to continue).
- Если приложение не подписано (или подписано, но еще не доверенное), запрос на повышение полномочий имеет желтый фон с красным значком в виде щита и отображает сообщение "Неопознанная программа хочет получить доступ к этому компьютеру" (An unidentified program wants access to your computer).

Улучшить безопасность процесса повышения полномочий может вывод запросов на повышение полномочий на безопасном рабочем столе. Безопасный рабочий стол защищает процесс повышения полномочий, предотвращая подделку запроса на повышение. Безопасный рабочий стол включен по умолчанию в групповой политике *(см. разд. "Оптимизация контроля учетных записей пользователей и режима одобрения администратором" главы 7)*.

Установка уровней выполнения

По умолчанию в режиме повышенных полномочий выполняются только приложения, использующие маркер доступа администратора. Но иногда требуется, чтобы приложение, использующее маркер доступа стандартного пользователя, исполнялось в режиме повышенных полномочий. Например, может потребоваться открыть консоль командной строки в режиме повышенных полномочий, чтобы выполнить задания администрирования.

Кроме манифеста приложения, который рассматривался в предыдущем разделе этой главы, Windows 8 предоставляет два других способа для установки уровня выполнения для приложения:

- одноразовый запуск приложения от имени администратора;
- постоянный запуск приложения от имени администратора.

Для одноразового запуска приложения от имени администратора щелкните правой кнопкой мыши по значку приложения или по команде меню и в контекстном меню выберите команду **Запуск от имени администратора** (Run as administrator). При использовании стандартной учетной записи и включенной функциональности вывода запросов на повышение перед запуском приложения выводится запрос на согласие. При использовании стандартной учетной записи и выключенной функциональности вывода запросов приложение не запустится. При использовании учетной записи администратора и включенной функциональности вывода запросов на повышение перед запуском приложения выводится запрос на согласие.

В Windows 8 приложение можно пометить, чтобы оно всегда запускалось с полномочиями администратора. Эта возможность полезна для решения проблем совместимости с унаследованными приложениями, для которых требуются полномочия администратора. Она также полезна для приложений, отвечающих требованиям контроля учетных записей, которые обычно выполняются в стандартном режиме, но используются для выполнения заданий администрирования. Рассмотрим примеры.

- Стандартное приложение, разработанное специально для Windows 8, обычно исполняется в режиме повышенных полномочий и используется для выполнений заданий администрирования. Чтобы избавиться от необходимости выполнять всю процедуру запуска приложения от имени администратора при каждом его использовании, его можно пометить для постоянного запуска таким образом.

- Стандартное приложение, разработанное для Windows XP или более ранней версии Windows, требует полномочий администратора. Так как это приложение настроено для работы по умолчанию в стандартном режиме в Windows 8, приложение не работает должным образом и генерирует многочисленные ошибки. Чтобы решить эту проблему совместимости окончательно, можно создать оболочку совместимости (compatibility shim), используя набор ACT 5.5 или более поздней версии. В качестве временного решения приложение можно пометить для постоянного запуска от имени администратора.

Примечание

Системные приложения или процессы нельзя пометить для постоянного запуска от имени администратора. Это допускается только для несистемных приложений и процессов.

Практический совет

Набор ACT (Application Compatibility Toolkit) позволяет администраторам решать проблемы совместимости, не прибегая к перепрограммированию приложения. С его помощью можно решать распространенные проблемы совместимости. Например, некоторые приложения выполняются только на определенной операционной системе или когда запускающий их пользователь обладает правами администратора. С помощью набора ACT можно создать оболочку совместимости, которая на запросы приложения о соответствующей операционной системе или уровне исполнения предоставляет утвердительный ответ, что позволяет запуск и выполнение приложения. Набор ACT также может быть полезным для создания более доскональных решений для приложений, которые пытаются выполнять запись в защищенные области операционной системы или используют повышенные полномочия, когда такие полномочия им не нужны. Набор ACT можно загрузить с центра загрузок Майкрософт (**http://www.microsoft.com/en-us/download/**).

Пометить программу для постоянного запуска от имени администратора можно следующим образом:

1. В Проводнике Windows укажите программу, которую нужно всегда запускать от имени администратора.
2. Щелкните правой кнопкой мыши по значку приложения и в открывшемся контекстном меню выберите команду **Свойства** (Properties).
3. В диалоговом окне свойств выберите вкладку **Совместимость** (рис. 8.1).
4. Далее выполните одно из следующих действий.

   - Чтобы применить настройку для текущего пользователя, установите флажок **Выполнять эту программу от имени администратора** (Run this program as an administrator), а затем нажмите кнопку **OK**.
   - Чтобы применить настройку для всех пользователей компьютера и независимо от используемого для ее запуска ярлыка, нажмите кнопку **Изменить параметры для всех пользователей** (Change settings for all users), в открывшемся диалоговом окне свойств исполняемого файла приложения установите флажок **Выполнять эту программу от имени администратора**, а затем нажмите кнопку **OK** в этом и предыдущем окне.

Примечание

Если опция **Выполнять эту программу от имени администратора** недоступна, это означает, что данное приложение заблокировано от выполнения на повышенном уровне, либо для выполнения приложения не требуются полномочия администратора, либо пользователь, пытающийся установить этот параметр, не обладает полномочиями администратора.

Теперь эта программа всегда будет выполняться с маркером доступа администратора. Но имейте в виду, что при использовании стандартной учетной записи и выключенной функциональности вывода запросов на повышение полномочий приложение не будет запускаться.

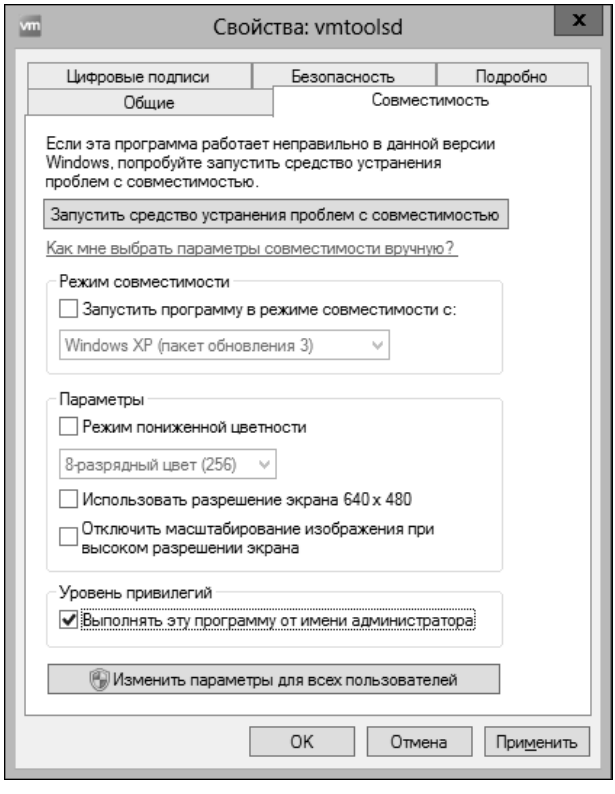


Рис. 8.1. Вкладка **Совместимость** окна свойств приложения

Оптимизация вывода запросов на повышение прав для виртуализации и установки

Можно оптимизировать несколько областей контроля учетных записей, касающихся приложений, в том числе:

- автоматическое обнаружение установки и вывод запросов;
- виртуализация ошибок записи.

Эти возможности можно настроить посредством настройки параметров узла **Конфигурация компьютера\Параметры Windows\Параметры безопасности\Локальные политики\Параметры безопасности** редактора локальной групповой политики. В частности, можно настроить следующие параметры.

- **Контроль учетных записей: обнаружение установки приложений и запрос на повышение прав** (User Account Control: Detect application installations and prompt for elevation). Определяет возможность автоматического обнаружения попытки установки приложения и вывода запроса на повышение прав или одобрение. (В Windows 8 этот параметр включен по умолчанию.) Если данный параметр отключить, для пользователей не будет выводиться запрос на повышение полномочий, вследствие чего они не смогут повысить свои полномочия, предоставив учетные данные администратора.
- **Контроль учетных записей: при сбоях записи в файл или реестр виртуализация в место размещения пользователя** (User Account Control: Virtualize file and registry

write failures to per-user locations). Определяет использование виртуализации файлов и разделов реестра. Так как этот параметр включен по умолчанию, извещения об ошибках и журналирование ошибок, связанных с виртуализированными файлами и значениями реестра, записываются в виртуальное расположение, а не в действительное расположение, в которое приложение пыталось выполнить запись. Если этот параметр отключить, при попытке записи в защищенную папку или область реестра происходит сбой приложения без предоставления какой-либо информации об этом.

Примечание

Другие связанные параметры рассматриваются в *разд. "Оптимизация контроля учетных записей пользователей и режима одобрения администратором" главы 7*.

В доменной среде задать требуемую конфигурацию безопасности определенному набору компьютеров можно с помощью групповой политики службы каталогов Active Directory. Эти параметры также можно настраивать для отдельных компьютеров посредством локальной политики безопасности. Для этого нужно выполнить следующую процедуру:

1. Откройте консоль локальной политики безопасности. Это можно сделать, выполнив команду `secpol.exe` в поле поиска панели **Приложения** или в командной строке. Если включено отображение средств администрирования на экране **Пуск**, эту консоль можно запустить с помощью ее плитки на этом экране.
2. В дереве консоли последовательно разверните узлы **Параметры безопасности\Локальные политики** и выберите папку **Параметры безопасности**.
3. Дважды щелкните мышью на необходимом параметре, настройте его требуемым образом и сохраните настройки, нажав кнопку **OK**.

Основы установки программ

Установка программ представляет собой последовательный процесс. Но поиск причин неполадок, которые могут возникнуть при установке программ, и их устранение не является таким прямолинейным процессом. Прежде чем решать потенциальные проблемы с установкой, сначала нужно понимать сам процесс установки. Во многих случаях типичный процесс установки начинается запуском программы Autorun, которая в свою очередь запускает программу установки. С началом работы программы установки стартует процесс установки. Частью этого процесса является проверка учетных данных пользователя с целью удостовериться в том, что он обладает соответствующими полномочиями для установки программы, и вывод запроса на одобрение, если пользователь такими полномочиями не обладает. При установке программы, возможно, понадобится сделать ее доступной для всех пользователей компьютера или же только для некоторых из них.

Иногда Windows не в состоянии определить, какие полномочия требуются для установки. Это может случиться в том случае, когда манифест установки программы содержит параметр **RequestedExecutionLevel**, для которого установлено значение `RequireAdministrator`. Так как значение параметра **RequestedExecutionLevel** превалирует над тем, что установщик обнаруживает в Windows, при запуске установщика с разрешениями стандартного пользователя процесс установки завершается неудачей. Эта проблема решается прекращением установки путем ее отмены или выполнением другого соответствующего действия. Затем следует щелкнуть правой кнопкой мыши на исполняемом файле установщика и в контекстном меню выбрать опцию **Запуск от имени администратора**, чтобы перезапустить процесс установки с правами администратора.

В Windows 8 используются политики управления приложениями (Application Control policies) вместо политик ограниченного использования программ (Software Restriction

policies) из предыдущих версияй Windows. Политики ограниченного использования программ следят за тем, какие приложения пользователи могут устанавливать и выполнять на компьютерах под управлением Windows 2000/XP/Vista. А политики управления приложениями определяют, какие программы пользователи могут устанавливать и выполнять на Windows 7 и более поздних версиях ОС, а также на Windows Server 2008 Release 2 и более поздних версиях. Нужно иметь в виду следующее.

- Политики ограниченного использования программ для компьютера или пользователя можно создавать и управлять ими посредством параметров узла объекта групповой политики **Конфигурация компьютера** (или **Конфигурация пользователя**)**\Политики\Параметры Windows\Параметры безопасности\Политики ограниченного использования программ**. Применение ограничений управляется с помощью параметров принудительного применения. Что является или не является исполняемой программой, определяется присвоенным типом файла.
- Политики управления приложениями для компьютера или пользователя можно создавать и управлять ими посредством параметров узла объекта групповой политики **Конфигурация компьютера** (или **Конфигурация пользователя**)**\Политики\Параметры Windows\Параметры безопасности\Политики управления приложениями**. Здесь можно создавать отдельные правила для исполняемых файлов, файлов установщика Windows и файлов сценариев. Правила могут применяться издателем, путем или хэшем файла. Правило издателя предоставляет наибольшую гибкость, позволяя указывать, какие продукты и версии разрешать. Например, можно разрешить Microsoft Word 2007 или более позднюю версию.

Работа с файлом Autorun

Когда в привод оптических дисков вставляется диск, Windows 8 проверяет наличие на нем файла Autorun.ini. Этот файл (если таковой имеется на диске) указывает действие, которое должна выполнить операционная система, а также может содержать другие параметры для установки. Файл Autorun.ini является текстовым файлом, который можно открыть в любом стандартном текстовом редакторе. Далее приводится пример содержимого такого файла:

```
[autorun]
OPEN=SETUP.EXE AUTORUN=1
ICON=SETUP.EXE,4
SHELL=OPEN
DisplayName=Microsoft Digital Image Suite 9
ShortName=PIS
PISETUP=PIP\pisetup.exe
```

Данный файл Autorun.ini указывает, что при вставке диска в привод операционная система должна открыть файл Setup.exe. Так как файл Setup.exe является исполняемым, он запускается на выполнение. В файле Autorun.ini также указывается, какую пиктограмму использовать, состояние оболочки, отображаемое имя программы, короткое имя программы и дополнительный параметр, которым в данном случае является местонахождение другой программы установки, требующей выполнения.

Файл, указываемый для открытия в файле Autorun.ini, не обязательно должен быть исполняемым. Возьмем следующий пример:

```
[autorun]
OPEN=Autorun\ShelExec default.htm
```

В данном случае файл Autorun.ini исполняется через оболочку и открывает файл default.htm в браузере компьютера. Но важно отметить, что даже в этом случае открываемый в браузере документ содержит ссылку на программу установки.

Совет

Когда установочный диск приложения находится в приводе, файл Autorun.ini можно перезапустить в любое время. Для этого нужно просто открыть и снова закрыть лоток привода.

Установка и совместимость приложения

В программах установки большинства приложений используются установщики Install Shield, Wise Install или установщик Windows. В процессе работы программы установки установщик помогает отслеживать ход установки, а также должен обеспечить легкое удаление программы в случае необходимости. При инсталляции более старого приложения программа установки может использовать старую версию одного из этих установщиков, вследствие чего при удалении программа может быть удалена не полностью.

Даже если вы полностью уверены в том, что используется текущая версия установщика, следует учитывать возможность необходимости выполнять восстановление системы в случае каких-либо проблем с установкой. Чтобы обеспечить восстановление системы, проверьте, что для диска, на который устанавливается программа, включена функциональность защиты системы, чтобы перед установкой программы была автоматически создана точка восстановления.

Хотя установщики большинства новых программ автоматически запускают процесс создания точки восстановления, прежде чем вносить какие-либо изменения в компьютер, установщики более старых программ могут этого не делать. В таком случае точку восстановления можно создать вручную. Этот процесс рассматривается в *главе 10*. Тогда, в случае проблем, можно попробовать удалить программу или использовать средство **Восстановление системы**, чтобы восстановить систему к тому состоянию, в котором она была до установки программы.

Прежде чем устанавливать какую-либо программу, следует проверить, что она совместима с Windows 8. Определить совместимость программы можно следующим образом:

- проверить наличие сведений о совместимости на упаковке программы. В случае совместимости программы с Windows 8 на ее упаковке должен быть логотип Windows 8;
- проверить на веб-сайте разработчика программы наличие Windows 8 в списке совместимых операционных систем.

Примечание

Чтобы убедиться в совместимости программы с Windows 8, посмотрите, нет ли для нее обновлений или исправлений. Установите все имеющиеся обновления и исправления сразу же после установки самой программы.

При установке программы ОС пытается определить наличие потенциальных проблем совместимости. В случае обнаружения возможной несовместимости программы выводится диалоговое окно **Помощник по совместимости программ** (Program Compatibility Assistant), предупреждающее об этом. Часто это диалоговое окно содержит информацию об известных проблемах совместимости данной программы и во многих случаях предлагает их возможное решение. Например, может рекомендоваться установить самый последний пакет обновлений для программы, прежде чем запускать ее. В некоторых случаях окно помощника по совместимости содержит сообщение "Эта программа заблокирована из-за проблем совместимости" (This program is blocked due to compatibility issues). В данном случае установка

программы заблокирована, т. к. она вызывает известную проблему со стабильной работой Windows, для которой нет немедленного решения. Единственной доступной опцией является поиск возможных решений в Интернете, для чего следует нажать кнопку **Поиск решений в Интернете** (Check for solutions online) или отменить установку программы, нажав кнопку **Отменить**. Обычно типичным решением, которое можно найти в Интернете в таких случаях, будет рекомендация приобрести новую версию программы. Отмена завершает процесс установки без поиска возможных решений.

Если установка стартует, но затем возникает проблема, или если установка завершается без информирования операционной системы о результате установки, также выводится окно **Помощник по совместимости программ**. В этом случае, если программа установилась правильно, следует нажать кнопку **Эта программа установлена правильно** (This program installed correctly). Если же программа не установилась должным образом — кнопку **Переустановите, используя рекомендуемые параметры** (Reinstall using recommended settings), чтобы позволить помощнику по совместимости применить одно или несколько исправлений совместимости, а затем попытаться снова установить программу.

Помощник по совместимости программ также используется при запуске программ, чтобы автоматически вносить необходимые изменения для известных проблем совместимости. Если помощник по совместимости обнаруживает известную проблему совместимости при выполнении приложения, он извещает об этом и предлагает возможные способы автоматического решения этой проблемы. Затем можно либо предоставить помощнику по совместимости переконфигурировать приложение, либо сделать это вручную *(см. разд. "Настройка совместимости программ" далее в этой главе)*.

Настройками совместимости также можно управлять посредством параметров политики **Совместимость приложений** (Application Compatibility), которая находится в узле **Конфигурация компьютера\Административные шаблоны\Компоненты Windows** редактора локальной групповой политики. Эти параметры включают следующие.

- **Запрещение доступа к 16-разрядным приложениям** (Prevent access to 16-bit applications). Включение этого параметра запрещает исполнение на компьютере подсистемы MS-DOS. Это также означает, что 16-разрядные установщики 32-разрядных программ и другие 16-разрядные компоненты тоже не будут выполняться.
- **Удаление страницы "Свойства совместимости программ"** (Remove Program Compatibility Property Page). Включение этого параметра удаляет вкладку **Совместимость** из диалогового окна свойств программ.
- **Отключение обработчика совместимости приложений** (Turn off Application Compatibility Engine). Включение этого параметра запрещает Windows сверяться с базой данных известных проблем совместимости при запуске программ. Данное действие может ускорить запуск приложений, однако также способно вызвать ошибку останова в случае попытки запуска несовместимой программы, которая не была должным образом подготовлена.
- **Отключение помощника по совместимости программ** (Turn Off Program Compatibility Assistant). Если этот параметр включен, унаследованные приложения будут выполняться без защиты обработчика совместимости Switchback, который применяется для решения известных общих проблем совместимости, возникающих при выполнении унаследованных приложений на современных версиях Windows. В то время как отключение этого обработчика может повысить производительность, несовместимые приложения могут зависать или вызывать другие проблемы с системой.

Предоставление программ всем или только отдельным пользователям

В Windows 8 традиционное меню **Пуск** предыдущих версий операционной системы заменено экраном **Пуск**. При установке приложений рабочего стола на экран **Пуск** автоматически помещаются их значки в виде плитки, что упрощает запуск этих приложений и управление ими. При щелчке правой кнопкой мыши по плитке приложения отображаются опции для его управления, которые зависят от типа плитки. Например, активные плитки могут обновлять выводимое в них содержимое, и эту функциональность можно включить или отключить. Размер некоторых плиток можно изменить, выбрав соответствующую опцию. Плитку программы можно убрать с экрана **Пуск**, выбрав в панели меню команду **Открепить от экрана "Пуск"**.

Для большинства установленных на компьютере настольных программ на экран **Пуск** должны помещаться соответствующие плитки, а в списке **Все приложения** создаваться соответствующие опции. Это достигается помещением ярлыка программы в соответствующую подпапку папки Главное меню\Программы (Start Menu\Programs) (полный путь — *%SystemDrive%*\ProgramData\Microsoft\Windows\Главное меню\Программы[1]). Эта папка доступна всем пользователям, и, соответственно, все пользователи имеют доступ к содержащимся в ней программам. Некоторые программы при установке выводят сообщение, предоставляющее выбор установки программы для всех пользователей или только для текущего пользователя. Другие программы устанавливаются лишь для текущего пользователя.

Предоставить другим пользователям доступ к программе, которая была установлена только для устанавливающего ее пользователя, можно одним из следующих способов.

- Выполните вход в систему по учетной записи каждого пользователя, для которого нужно предоставить доступ к программе, и осуществите установку программы для каждого из них. В случае добавления на компьютер нового пользователя, которому требуется доступ к программе, ее нужно будет установить таким же образом и для него.
- В некоторых случаях программы, для запуска которых не требуется вставлять в реестр параметры отдельного пользователя, можно сделать доступными для всех пользователей, скопировав их ярлыки из профиля пользователя, для которого программа была установлена, в папку Главное меню\Программы для всех пользователей.

Предоставить доступ к программе всем пользователям компьютера можно следующим образом:

1. В Проводнике Windows откройте скрытую папку Программы пользователя, для которого была установлена программа, по пути *%UserProfile%*\AppData\Roaming\Microsoft\Windows\Главное меню. Чтобы отображать скрытые папки и файлы в Проводнике Windows, нужно установить флажок **Скрытые элементы** на вкладке **Представление** ленты окна Проводника.
2. В папке Программы щелкните правой кнопкой мыши на папке требуемой программной группы или на ярлыке программы и в контекстном меню выберите команду **Копировать** или **Вырезать**.
3. Затем в Проводнике Windows перейдите в скрытую папку Главное меню\Программы для всех пользователей, которая находится по пути *%SystemDrive%*\ProgramData\Microsoft\Windows.

[1] %SystemDrive%\ProgramData\Microsoft\Windows\Start Menu\Programs.

4. Щелкните правой кнопкой мыши в свободной области этой папки и в контекстном меню выберите команду **Вставить**. Теперь программная группа или программа должна быть доступной для всех пользователей компьютера.

Предоставить доступ к программе только определенному пользователю компьютера и ограничить его для всех других пользователей можно следующим образом:

1. В Проводнике Windows откройте скрытую папку Программы для всех пользователей, которая находится по пути *%SystemDrive%*\ProgramData\Microsoft\Windows\Главное меню.
2. В папке Программы щелкните правой кнопкой мыши на папке требуемой программной группы или на ярлыке программы и в контекстном меню выберите команду **Вырезать**.
3. В Проводнике Windows откройте скрытую папку Программы требуемого пользователя, которая находится по пути *%UserProfile%*\AppData\Roaming\Microsoft\Windows\Главное меню.
4. Щелкните правой кнопкой мыши по свободной области этой папки и в контекстном меню выберите команду **Вставить**. Теперь программная группа или программа должна быть доступной только для данного пользователя.

> ***Примечание***
>
> В действительности эта процедура только скрывает факт наличия программы на компьютере от несведущих пользователей. Более продвинутые пользователи, которым известно о наличии программы, могут запустить ее, введя имя ее исполняемого файла в диалоговом окне **Выполнить**, консоли командной строки или в поле поиска панели **Приложения** либо просто дважды щелкнув по значку приложения в Проводнике Windows.

Развертывание приложений посредством групповой политики

Приложения можно устанавливать для пользователей по сети с помощью групповой политики. Развертывание приложений посредством групповой политики можно выполнять двумя способами.

- *Назначить приложение пользователям или компьютерам.* Назначенное компьютеру приложение устанавливается на данный компьютер при его следующем запуске и доступно каждому пользователю данного компьютера при следующем входе в систему. Назначенное пользователю приложение устанавливается при следующем входе пользователя в сеть. Назначенное пользователю приложение можно настроить для установки при первой попытке его использования. В этом случае для приложения создается ярлык на рабочем столе пользователя или на экране **Пуск**, и приложение устанавливается, когда пользователь щелкает по этому ярлыку.
- *Опубликовать приложение и сделать его доступным для установки.* Опубликованное приложение можно устанавливать посредством активации расширения файла документа приложения. В этом случае программа устанавливается при первой попытке пользователя открыть документ, связанный с данным приложением. Например, при попытке пользователя открыть файл документа с расширением doc или docx выполняется автоматическая установка приложения Microsoft Word.

Развертывание приложений *для компьютеров* осуществляется посредством пакета установщика Windows (msi-файл) и параметров политики **Установка программ**, которая находится в узле **Конфигурация компьютера\Политики\Конфигурация программ** оснастки

консоли MMC **Редактор управления групповыми политиками**. Развертывание приложений *для пользователей* осуществляется с помощью пакета установщика Windows (msi-файл) и параметров политики **Установка программ**, которая находится в узле **Конфигурация пользователя\Политики\Конфигурация программ** оснастки консоли MMC **Редактор управления групповыми политиками**. Базовая процедура для развертывания приложений посредством групповой политики следующая:

1. Чтобы клиенты могли иметь доступ к пакету установщика Windows, он должен находиться на сетевом диске. Скопируйте пакет установщика Windows (msi-файл) программы на сетевой диск, который доступен конкретным пользователям.
2. В редакторе управления групповыми политиками откройте объект групповой политики, для которого требуется выполнить развертывание приложения. Развернутое приложение будет доступным для всех клиентов, к которым применим данный объект групповой политики. Иными словами, приложение будет доступным компьютерам и пользователям в связанном домене, сайте или организационной единице.
3. Разверните узел **Конфигурация компьютера\Политики\Конфигурация программ** (или узел **Конфигурация пользователя\Политики\Конфигурация программ**), щелкните в нем правой кнопкой мыши по узлу **Установка программ** и последовательно выберите команды **Создать | Пакет**.
4. В диалоговом окне **Открытие** укажите пакет установщика Windows (msi-файл) устанавливаемого приложения и нажмите кнопку **Открыть**. После этого будет предоставлен выбор метода развертывания: **публичный** (Published), **назначенный** (Assigned) или **особый** (Advanced).
5. Чтобы опубликовать или назначить программу, установите переключатель **публичный** или **назначенный**, соответственно, и нажмите кнопку **OK**. При настройке политики компьютера программа будет доступной при следующем запуске компьютера, на который распространяется данный объект групповой политики. При настройке политики пользователя программа будет доступной при следующем входе в систему пользователя в затронутом домене, сайте или организационной единице. Пользователи, которые в настоящее время находятся в системе, должны выйти, а затем войти в нее.
6. Установка переключателя **особый** позволяет настроить дополнительные опции развертывания программы.

Настройка совместимости программ

При установке 16-разрядных программ, или программ под MS-DOS, нужно принимать во внимание дополнительные аспекты. Кроме этого, чтобы добиться исполнения старых программ, иногда может быть необходимым настроить параметры совместимости. Особенности установки таких программ рассматриваются в следующих разделах.

Особые соображения при установке 16-разрядных программ и программ под MS-DOS

Многие 16-разрядные и MS-DOS-программы, для которых не требуется прямой доступ к аппаратным ресурсам, можно устанавливать и выполнять в Windows 8 без проблем. Но большинство 16-разрядных и MS-DOS-программ[1] не поддерживает длинные имена файлов.

[1] Далее, для краткости, просто 16-разрядные программы.

Чтобы обеспечить совместимость для таких программ, Windows 8 устанавливает соответствие между длинными и короткими именами файлов по мере надобности. Это обеспечивает защиту длинных имен, когда они изменяются 16-разрядной программой. Кроме этого, важно отметить, что для некоторых 16-разрядных программ требуются 16-разрядные драйверы, которые не поддерживаются Windows 8. Поэтому такие программы выполняться не смогут.

Большинство существующих 16-разрядных программ были первоначально разработаны для Windows 3.0 или 3.1. В Windows 8 эти программы выполняются с помощью виртуальной машины, которая эмулирует расширенный режим процессора 80386, используемый в Windows 3.0 и 3.1. В отличие от других недавних версий Windows, в Windows 8 каждая 16-разрядная программа выполняется в виде потока на одной виртуальной машине. Это означает, что все они используют общее адресное пространство, и если одна из этих программ зависает, то обычно зависают и все остальные.

Такое отрицательное воздействие 16-разрядных программ друг на друга можно устранить, выделив каждой из них свое адресное пространство. Делается это следующим образом:

1. Щелкните правой кнопкой мыши по ярлыку приложения и в открывшемся контекстном меню выберите команду **Свойства**. (Если программа не имеет ярлыка, создайте его для нее.)
2. В окне свойств ярлыка выберите вкладку **Ярлык** и нажмите на ней кнопку **Дополнительно**.
3. В открывшемся диалоговом окне **Дополнительные свойства** (Advanced Properties) установите флажок **Запускать в отдельной области памяти** (Run in separate memory space).
4. Закройте все открытые диалоговые окна, последовательно нажимая в них кнопку **OK**.

Примечание

Выполнение программы в отдельном адресном пространстве потребляет дополнительную память, но обычно время отклика программы сокращается. Другим дополнительным преимуществом этого подхода является возможность выполнять несколько экземпляров программы, каждый в своей области памяти.

Совет

Программа командной строки Windows (cmd.exe) является 32-разрядной. Чтобы запустить 16-разрядную консоль командной строки для MS-DOS (command.com), выполните команду `command` в окне **Выполнить**.

Принудительное обеспечение совместимости программ

Некоторые программы отказываются устанавливаться или выполняться под Windows 8, даже если они работают без проблем под предыдущими версиями Windows. При попытке установить программу, имеющую известную проблему совместимости, Windows 8 должна вывести предупреждение об этой проблеме. В большинстве случаев продолжать установку проблемной программы не следует, особенно если это системная утилита, например антивирусная программа или программа для разбивки диска. Выполнение такой несовместимой системой утилиты может вызвать серьезные проблемы. Выполнение других типов несовместимых программ также может вызвать проблемы, особенно если программы выполнят запись в системные области диска.

Если программа не устанавливается или не выполняется под Windows 8, попытайтесь заставить ее делать это, настроив ее параметры совместимости. Операционная система Windows 8 предоставляет два механизма для управления параметрами совместимости. Можно исполь-

зовать мастер совместимости программ (Program Compatibility Wizard) или редактировать параметры совместимости программы напрямую, используя диалоговое окно свойств программы. Оба метода работают одинаково. Но изменить параметры совместимости программ, которые находятся на сетевых дисках, оптических дисках или других извлекаемых носителях, можно только посредством мастера совместимости программ. В результате, иногда с помощью этого мастера можно установить и исполнять программы, которые нельзя установить и запускать никаким иным способом.

Использование средства устранения проблем с совместимостью программ

Выполнять настройку параметров совместимости можно только для установленных программ. Для программ, входящих в состав операционной системы, выполнять настройку параметров совместимости нельзя. Проблемы совместимости можно попытаться определить автоматически, используя средство устранения проблем с совместимостью программ. Процедура для этого следующая:

1. Щелкните правой кнопкой мыши на ярлыке программы и в контекстном меню выберите команду **Исправление неполадок совместимости**. Откроется диалоговое окно **Средство устранения проблем с совместимостью программ** (Program Compatibility Troubleshooter) (рис. 8.2).

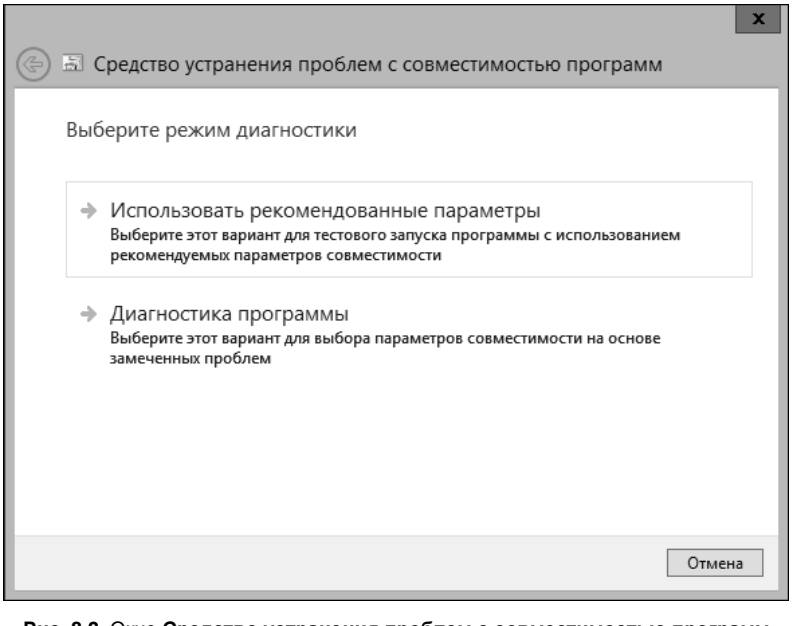


Рис. 8.2. Окно **Средство устранения проблем с совместимостью программ**

2. Средство устранения проблем с совместимостью попытается обнаружить проблемы совместимости и предоставит рекомендуемые решения для их исправления. Чтобы применить рекомендуемые исправления, щелкните по ссылке **Использовать рекомендованные параметры** (Try recommended settings). В следующем окне ознакомьтесь с параметрами, которые будут применены, а затем нажмите кнопку **Проверить программу** (Test the program).

3. После выполнения программы нажмите кнопку **Далее** и выполните одно из следующих действий.
   - Щелкните по ссылке **Да, сохранить эти параметры для программы** (Yes, save these settings for this program), если предложенные параметры совместимости решили проблему и вы хотите продолжать использовать их.
   - Щелкните по ссылке **Нет, попытаться использовать другие параметры** (No, try again using different settings), если предложенные параметры совместимости не решили проблему и вы хотите повторить процесс с новыми параметрами.
   - Если предложенные параметры совместимости не решили проблему и вы хотите попробовать найти ее решение в Интернете, щелкните по ссылке **Нет, отправить сообщение об этой проблеме в корпорацию Майкрософт и найти решение в Интернете** (No, report the problem to Microsoft and check online for a solution).
   - Чтобы отказаться от предложенных параметров совместимости и завершить работу средства устранения проблем с совместимостью, нажмите кнопку **Отмена**.

Для расширенного диагностирования с использованием средства устранения проблем с совместимостью программ для указания требуемых параметров совместимости применяется следующая процедура:

1. В Проводнике Windows найдите ярлык программы в папке *%SystemDrive%*\ProgramData\Microsoft\Windows\Главное меню\Программы. Щелкните правой кнопкой мыши по ярлыку программы и в контекстном меню выберите команду **Исправление неполадок совместимости**. Откроется диалоговое окно **Средство устранения проблем с совместимостью программ**.
2. Щелкните по ссылке **Диагностика программы** (Troubleshoot Program). На следующей странице, **Какие проблемы заметны?** (What problems do you notice?), можно предоставить информацию о наблюдаемых проблемах совместимости. Эта информация определяет дальнейшие действия средства устранения проблем с совместимостью. Можно указать следующие типы проблем.
   - **Программа работала в предыдущих версиях Windows, но не устанавливается или не запускается сейчас** (The program worked in earlier versions Windows but won't install or run now).

     При выборе этой опции на следующей странице средства предлагается указать последнюю версию Windows, с какой программа работала успешно. Так как сделанный здесь выбор устанавливает режим совместимости, следует указать операционную систему, для которой программа была разработана. Теперь при выполнении данной программы Windows 8 будет эмулировать среду указанной операционной системы.
   - **Программа открывается, но отображается неправильно** (The program opens but does not display correctly).

     Если вы пытаетесь запустить игру, образовательную или любую другую программу, для которой требуются специальные настройки дисплея, например программу, разработанную для Windows 98, можно выбрать эту опцию, а затем указать тип наблюдаемой проблемы с отображением. Если выбрать опцию 256 отображаемых цветов, разрешение экрана 640×480 пикселов или обе эти опции, Windows ограничит возможности видеодисплея указанными параметрами. Это может помочь с выполнением программ, которые испытывают затруднения с выполнением при более высоких разрешениях экрана и большей глубине цвета. Также предоставляется выбор отключения тем и визуальных эффектов рабочего стола и масштабирования экрана с высоким коэффициентом.

- **Для программы необходимы дополнительные разрешения** (The program requires additional permissions).

  При выборе этой опции программа будет настроена для выполнения с полномочиями администратора.

- **Я не вижу моей проблемы в списке** (I don't see my problem listed).

  При выборе этой опции открываются дополнительные страницы средства для выбора операционной системы и проблемы с отображением. Кроме этого, программа конфигурируется для выполнения с правами администратора. В конечном итоге, выбор этой опции имеет такой же эффект, как если бы были выбраны все три предыдущие опции.

3. Проверьте предлагаемые параметры совместимости. Если вы не хотите применять эти параметры, нажмите кнопку **Отмена** и повторите процедуру, выбрав другие опции. В противном случае нажмите кнопку **Проверить программу**, чтобы средство проверило работу программы с рекомендованными параметрами.
4. После выполнения программы нажмите кнопку **Далее**. В следующем окне запрашивается, исправили ли данные изменения проблему. Здесь выберите одну из следующих настроек.
   - Если предложенные параметры совместимости решили проблему и вы хотите продолжать использовать их, щелкните по ссылке **Да, сохранить эти параметры для программы**.
   - Если предложенные параметры совместимости не решили проблему и вы хотите повторить процесс с новыми параметрами, щелкните по ссылке **Нет, попытаться использовать другие параметры**.
   - Если предложенные параметры совместимости не решили проблему и вы хотите попробовать найти ее решение в Интернете, щелкните по ссылке **Нет, отправить сообщение об этой проблеме в корпорацию Майкрософт и найти решение в Интернете**.
   - Чтобы отказаться от предложенных параметров совместимости и завершить работу средства устранения проблем с совместимостью, нажмите кнопку **Отмена**.

   Примечание

   При настройке альтернативных параметров экрана программа будет выполняться в альтернативном режиме экрана при каждом ее запуске. Чтобы восстановить исходные параметры экрана, просто закройте программу.

Установка параметров совместимости напрямую

Если установленная программа не выполняется должным образом, эту проблему можно попытаться решить, отредактировав параметры совместимости напрямую, вместо использования средства устранения проблем с совместимостью. Прямое редактирование параметров выполняется следующим образом:

1. Щелкните правой кнопкой мыши на значке приложения и в открывшемся контекстном меню выберите команду **Свойства**.
2. В окне свойств программы выберите вкладку **Совместимость**. Любой установленный таким образом параметр будет применим к программе при ее выполнении пользователем, выполняющим настройку, и только при запуске посредством данного ярлыка. Чтобы изменить параметры совместимости программы для всех пользователей компьютера и для любого вида запуска, нужно нажать кнопку **Изменить параметры для всех поль-**

зователей и задать необходимые параметры совместимости в открывшемся диалоговом окне свойств исполняемого файла программы.

Примечание

Программы, которые являются частью Windows 8, нельзя исполнять в режиме совместимости, поэтому опции на вкладке **Совместимость** недоступны для встроенных программ Windows 8.

3. Установите флажок **Запустить программу в режиме совместимости с:** (Run this program in compatibility mode for:), а затем в раскрывающемся списке выберите операционную систему, для которой программа была изначально предназначена.
4. При необходимости ограничьте видеовывод программы, используя опции в разделе **Параметры** (Settings), установив глубину цвета в 256 цветов, разрешение экрана 640×480 пикселов или оба параметра одновременно.
5. При необходимости также можно отключить темы и визуальные эффекты рабочего стола и масштабирование экрана с высоким коэффициентом.
6. Завершив установку параметров совместимости, нажмите кнопку **OK**, чтобы сохранить их, а затем запустите программу, чтобы проверить ее работу с этими параметрами. В случае продолжающихся проблем с выполнением программы, попробуйте повторить настройку ее совместимости с другими параметрами.

Управление установленными и выполняющимися программами

Операционная система Windows 8 предоставляет несколько инструментов для управления программами.

- **Диспетчер задач** (Task Manager). Предоставляет средства для просмотра и управления исполняющимися программами, а также средства для просмотра использования ресурсов системой и ее производительности.
- **Программы** (Programs). Предоставляет средства для просмотра установленных программ, установки и удаления программ, просмотра установленных обновлений и др.
- **Программы по умолчанию** (Default Programs). Средства для отслеживания и настройки общих программ по умолчанию для компьютера, личных программ по умолчанию для отдельных пользователей, параметров автоматического воспроизведения дисков для мультимедиа, а также сопоставления расширений файлов программам.
- **Компоненты Windows** (Windows Features). Используется для просмотра и управления установленными на компьютере компонентами Windows.
- **Assoc.** Применяется для просмотра и управления сопоставлением файлов.
- **Ftype.** Средство для просмотра и управления определениями типов файлов.

Эти инструменты и связанные конфигурационные параметры рассматриваются в следующих разделах.

Управление текущими выполняющимися программами

В Windows 8 просматривать и управлять программами, выполняющимися в данный момент на компьютере, можно с помощью Диспетчера задач. Открыть Диспетчер задач можно, нажав комбинацию клавиш <Ctrl>+<Alt>+<Delete>, а затем выбрав опцию **Диспетчер задач**.

Или же можно щелкнуть правой кнопкой мыши в левом нижнем углу экрана и в контекстном меню выбрать команду **Диспетчер задач**. По умолчанию открывается краткая форма окна диспетчера, содержащего общий список исполняющихся приложений (рис. 8.3).

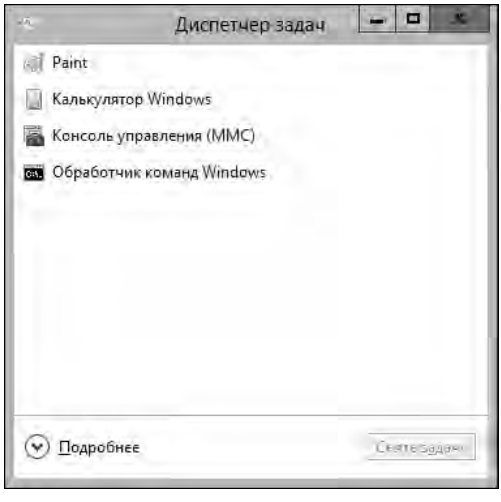


Рис. 8.3. Общий вид окна Диспетчера задач

Для управления приложением в списке его нужно выбрать, щелкнув на нем. Чтобы завершить выполнение выбранного приложения (например, если приложение зависло), нажмите кнопку **Снять задачу** (End task). Щелчок на приложении правой кнопкой мыши открывает контекстное меню, содержащее список других опций для управления приложением.

А щелчок по ссылке **Подробнее** (More details) открывает развернутое представление окна Диспетчера задач, содержащее подробную информацию о выполняющихся приложениях и процессах (рис. 8.4).

На вкладке **Процессы** отображается список приложений и процессов, исполняющихся в данный момент на компьютере. Обычно в разделе **Приложения** приводится список приложений, запущенных пользователем, в разделе **Фоновые процессы** (Background processes) — процессы Windows, выполняющиеся в фоновом режиме, а в разделе **Процессы Windows** (Windows processes) — все остальные процессы Windows.

Для каждого приложения или процесса указывается его имя, состояние и процент использования ресурсов центрального процессора, памяти, диска и сети. Пробел в столбце состояния означает нормальное состояние приложения. Как и в случае с общим видом окна Диспетчера задач, можно завершить работу выбранного приложения, нажав кнопку **Снять задачу**.

Двойной щелчок на приложении или процессе разворачивает список связанных с ним окон или процессов. Щелчок правой кнопкой мыши на приложении открывает контекстное меню, содержащее список других команд для управления приложением. Доступны, среди прочих, следующие опции:

- **Открыть расположение файла** (Open file location) — открывает в Проводнике Windows папку, содержащую исполняемый файл приложения или процесса;
- **Создать файл дампа** (Create dump file) — создает файл дампа памяти для выбранного процесса;
- **Подробно** (Go to details) — открывает вкладку **Подробности** с выбранным процессом;
- **Свойства** (Properties) — открывает окно свойств исполняемого файла выбранного приложения или файла.

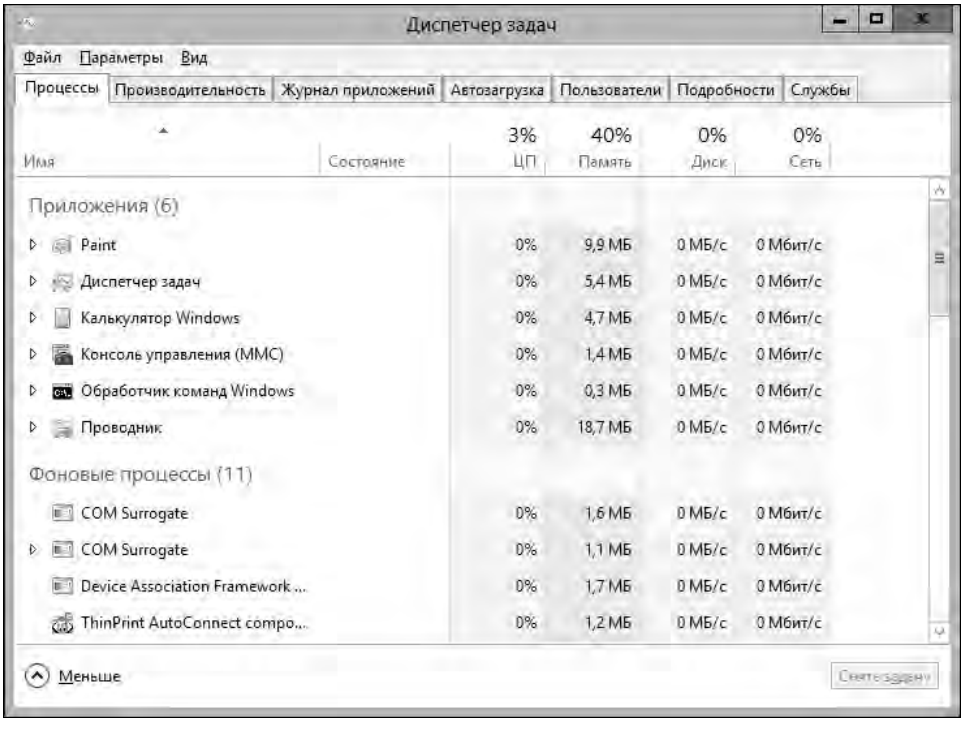


Рис. 8.4. Развернутый вид окна Диспетчера задач с подробной информацией об исполняющихся процессах

Управление программами, их исправление и удаление

Операционная система Windows 8 рассматривает все зарегистрированные на компьютере программы или программы, доступные для установки по сети, установленными программами. В Windows XP и более ранних версиях Windows для установки и управления программ применялась утилита Панели управления **Установка и удаление программ** (Add or Remove Programs).

В Windows 8 для установки программ используется прилагаемая к ним программа установки, а для удаления и прочего управления — утилита Панели управления **Программы и компоненты** (Programs and Features).

С помощью утилиты **Программы и компоненты** можно просматривать, добавлять, удалять или исправлять установленные программы. Общая процедура для этого следующая:

1. В Панели управления щелкните на ссылке **Программы**, а в открывшемся окне **Программы** — на ссылке **Программы и компоненты**. Откроется окно **Программы и компоненты** со списком установленных программ.
2. Щелкните правой кнопкой мыши на требуемой программе, чтобы открыть список команд для работы с ней. Доступные команды зависят от программы и включают следующие:
   - **Удалить** (Unistall) — удаление программы;
   - **Удалить/Изменить** (Uninstall/Change) — удаление или изменение конфигурации программы;

- **Изменить** (Change) — изменение конфигурации программы;
- **Восстановить** (Repair) — восстановление установки программы (если доступно).

При удалении программ нужно иметь в виду следующее.

- При попытке удаления программы, когда в систему выполнили вход другие пользователи, Windows выдает предупреждение. Обычно, прежде чем удалять программу, следует убедиться, что с компьютером никто больше не работает. В противном случае другие пользователи могут потерять свои данные или у них могут возникнуть иные проблемы.
- Средствами Windows можно удалять только те программы, которые были установлены совместимой программой установки. Хотя программы установки большинства программ используют совместимые с Windows установщики InstallShield, Wise Install или установщик Windows, более старые программы могут иметь собственную утилиту для их удаления. Установка некоторых старых программ осуществляется простым копированием их файлов в папку программы. Такие программы удаляются посредством удаления их папки.
- Многие программы удаления не удаляют программы полностью, а оставляют некоторые данные, либо по небрежности разработчика, либо преднамеренно. В результате, после удаления таких программ их папка остается в системной папке Program Files. Эти папки можно удалить, но следует иметь в виду, что они могут содержать важные данные или индивидуальные настройки пользователя, которые могут быть полезными при повторной установке программы.
- Бывают случаи, когда процесс удаления программы завершается неудачей. В таких ситуациях программу можно успешно удалить повторным выполнением процедуры удаления. Но иногда процесс удаления может потребоваться зачистить вручную. Для этого, возможно, нужно будет удалить файлы программы и ее записи в реестре Windows.

  Для очистки реестра может быть полезным применить программу Fix it portable. Загрузить загрузчик программы можно по ссылке **http://go.microsoft.com/?linkid=9775982**. При открытии ссылки выберите опцию **Сохранить** и сохраните загрузчик (объем около 350 Кбайт) на жестком диске. Затем запустите этот загрузчик и следуйте инструкциям (на английском языке), чтобы загрузить и сохранить программу на жестком диске своего компьютера. Объем загружаемых файлов составляет около 30 Мбайт. Для работы с программой следуйте инструкциям в файле ReadMe.

Настройка программ по умолчанию

Утилита Панели управления **Программы по умолчанию** используется для сопоставления программ типам файлов и назначения программ для работы с файлами на CD- и DVD-дисках и других съемных носителях. Программы по умолчанию задаются на основе типов файлов, поддерживаемых этими программами, или глобально для всех пользователей компьютера или только для определенного пользователя. Индивидуальные настройки пользователя превалируют над глобальными настройками. Например, можно установить проигрыватель Windows Media в качестве глобального проигрывателя по умолчанию для всех поддерживаемых им файлов. В таком случае все пользователи компьютера будут использовать этот проигрыватель для воспроизведения аудио- и видеофайлов, поддерживаемых этим проигрывателем. Но если какой-либо пользователь предпочитает воспроизводить аудио- и видеофайлы посредством проигрывателя Apple iTunes, для данного пользователя этот проигрыватель можно настроить в качестве проигрывателя по умолчанию для воспроизведения всех типов поддерживаемых им файлов мультимедиа.

Настройка глобальных программ по умолчанию выполняется следующим образом:

1. В Панели управления щелкните на ссылке **Программы**, в открывшемся окне **Программы** — на ссылке **Программы по умолчанию**, а затем — на ссылке **Настройка доступа программ и параметров по умолчанию** (Set program access and computer defaults). Откроется диалоговое окно **Настройка доступа программ и умолчаний** (Set Program Access and Computer Defaults) (рис. 8.5).

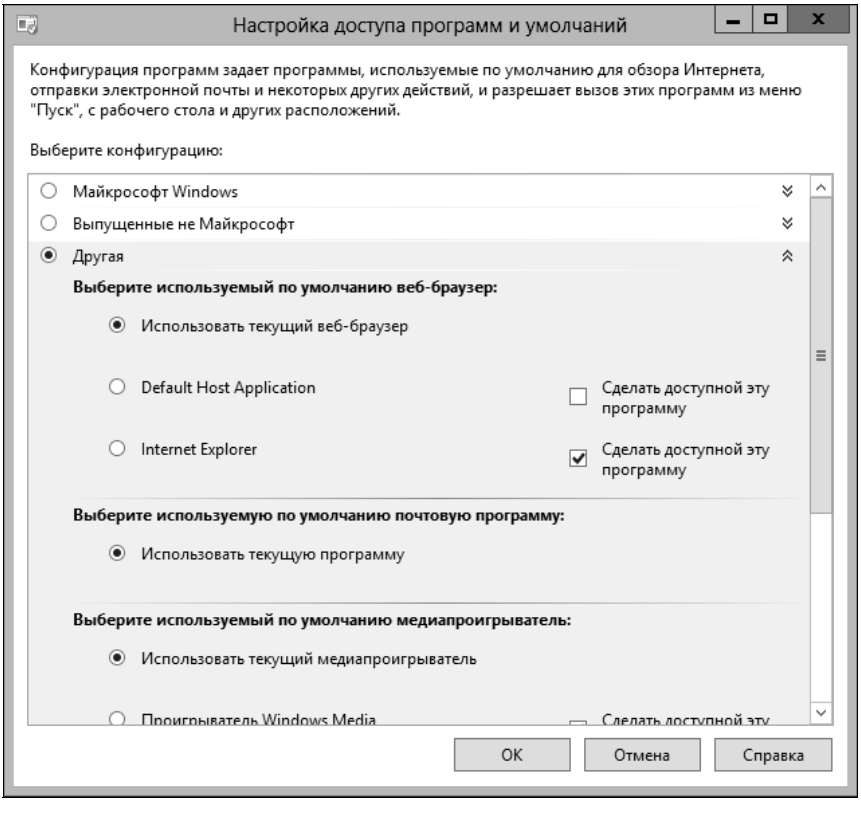


Рис. 8.5. Диалоговое окно для настройки глобальных программ по умолчанию

2. Установите один из следующих переключателей:
   - **Майкрософт Windows** (Microsoft Windows). В качестве программ по умолчанию для просмотра веб-страниц, работы с электронной почтой, воспроизведения файлов мультимедиа и т. п. задаются программы Microsoft, которые установлены на компьютере;
   - **Выпущенные не Майкрософт** (Non-Microsoft). В качестве программ по умолчанию для просмотра веб-страниц, работы с электронной почтой, воспроизведения файлов мультимедиа и т. п. задаются другие программы, которые установлены на компьютере;
   - **Другая** (Custom). Можно самостоятельно выбирать программы по умолчанию для просмотра веб-страниц, работы с электронной почтой, воспроизведения файлов мультимедиа и т. п.
3. Нажмите кнопку **OK**, чтобы сохранить и применить выполненные настройки.

Кроме глобальных программ по умолчанию, можно задать программы по умолчанию для отдельных пользователей. Эти настройки превалируют над глобальными. Настройка программ по умолчанию для текущего пользователя выполняется следующим образом:

1. В Панели управления щелкните на ссылке **Программы**, в открывшемся окне **Программы** — на ссылке **Программы по умолчанию**, а затем — на ссылке **Задание программ по умолчанию** (Set your default programs).
2. Откроется окно **Выбор программ по умолчанию** (Set Default Programs). Выберите в левой панели этого окна требуемую программу, чтобы просмотреть информацию о ней в правой панели сведений.
3. Чтобы использовать эту программу по умолчанию для всех поддерживаемых ею файлов и протоколов, щелкните на ссылке **Использовать эту программу по умолчанию** (Set this program as default).
4. Чтобы сделать данную программу программой по умолчанию для определенных типов файлов и протоколов, щелкните на ссылке **Выбрать значения по умолчанию для этой программы** (Choose defaults for this program) и в следующем окне, **Сопоставление программ** (Set Program Associations), выберите расширения файлов, которые должны по умолчанию открываться данной программой. Завершив сопоставление расширений файлов, нажмите кнопку **OK**, чтобы сохранить настройки.

Управление списком путей к командам

Для поиска исполняемых файлов программ в Windows 8 применяется список путей к командам. Текущий список можно просмотреть с помощью команды `path`. Для этого в обычной консоли командной строки введите команду `path` и нажмите клавишу <Enter>. А в консоли Windows PowerShell нужно ввести команду `$env:path` и нажать клавишу <Enter>. Вывод обеих этих команд содержит список путей к командам, разделенным точкой с запятой.

Список путей к командам задается при входе в систему с помощью системных и пользовательских переменных среды. Базовый список определяется системной переменной `PATH`. К этому базовому списку путей можно добавлять другие пути, используя следующий формат:

`%PATH%;`*`Дополнительные_пути`*

Здесь переменная `%PATH%` задает базовый список путей, а переменная *`Дополнительные_пути`* обозначает добавление других путей к базовому списку.

> ***Осторожно!***
>
> Неправильно заданный путь к командам может вызвать серьезные проблемы. Поэтому прежде чем применять изменение пути в рабочей среде, всегда необходимо протестировать его. Путь к командам задается при входе в систему. Поэтому, чтобы новый путь к командам вступил в силу, нужно выйти из системы, а затем снова войти.

Также не следует забывать о порядке поиска, применяемом в Windows. Поиск исполняемого файла по путям выполняется в том порядке, в котором они перечислены в пользовательской переменной среды `PATH`. Иногда это может замедлить исполнение программ и сценариев. Чтобы помочь Windows находить определенные программы или сценарии быстрее, следует рассмотреть возможность помещения соответствующего пути ближе к началу списка путей.

При редактировании списка путей следует соблюдать осторожность, чтобы случайно не удалить всю информацию о путях. Например, если при задании пути пользователя не ука-

зать базовый список путей `%PATH%`, то будет удалена информация обо всех других путях. Один из способов обеспечить сохранность списка путей — это сохранить его копию в текстовый файл.

- Это можно сделать, выполнив в консоли командной строки команду `path > orig_path.txt`. Следует иметь в виду, что если консоль запущена с правами обычного пользователя, а не от имени администратора, записать создаваемый ею файл в системные области (например, в корневую папку диска C:) не получится. В таком случае этот файл можно сохранить в подпапке, к которой у вас есть доступ, или в папке личного профиля. Чтобы просто вывести список путей к командам в окне консоли, выполните в ней команду `path`.
- В консоли PowerShell сохранить список путей в файл можно, выполнив в ней команду `$env:path > orig_path.txt`. Но как и в случае с обычной консолью командной строки, если консоль PowerShell запущена с правами обычного пользователя, а не администратора, сохранить файл в защищенных системных областях не удастся. В таком случае этот файл можно сохранить в подпапке, к которой у вас есть доступ, или в папке личного профиля. Чтобы просто вывести список путей к командам в окне консоли PowerShell, выполните в ней команду `$env:path`.

Список путей к командам можно редактировать в консоли командной строки или консоли PowerShell посредством утилиты Setx.exe. Редактировать список можно также вручную. Процедура для этого следующая:

1. В Панели управления щелкните на ссылке категории **Система и безопасность** и в открывшемся списке элементов этой категории щелкните на ссылке **Система**.
2. В левой панели окна **Система** щелкните на ссылке **Дополнительные параметры системы** (Advanced system settings)
3. На вкладке **Дополнительно** открывшегося диалогового окна **Свойства системы** нажмите кнопку **Переменные среды**.
4. Выберите переменную `PATH` в списке **Системные переменные** и нажмите кнопку **Изменить** под этим списком.
5. Откроется диалоговое окно **Изменение системной переменной** (Edit System Variable), поле **Значение переменной** которого содержит текущее значение переменной `PATH`. Не нажимая никаких других клавиш, нажмите клавишу <→>. Это должно снять выделение со значения переменной в поле и поместить курсор в конец строки.
6. Введите точку с запятой, а за ней (без пробелов!) введите новый путь.
7. Повторите предыдущий шаг, пока не будут добавлены все требуемые пути, после чего последовательно нажмите кнопку **OK** трижды, чтобы закрыть все окна.

В групповой политике список путей к командам можно редактировать посредством элемента предпочтений. Для этого применяется следующая процедура:

1. В редакторе управления групповыми политиками откройте для редактирования требуемый объект групповой политики. Для настройки предпочтений компьютера разверните узел **Конфигурация компьютера\Настройка\Конфигурация Windows** и выберите узел **Среда**. Для настройки предпочтений пользователя разверните узел **Конфигурация пользователя\Настройка\Конфигурация Windows** и выберите узел **Среда**.
2. Щелкните правой кнопкой мыши на узле **Среда**, выберите в контекстном меню команду **Создать**, а затем — команду **Переменные среды**. Откроется диалоговое окно **Новые свойства среды** (New Environment Properties).

3. В списке **Действие** выберите вариант **Обновить**, чтобы обновить переменную, или **Заменить**, чтобы удалить, а затем снова создать ее. Далее установите переключатель **Пользовательская переменная**, чтобы работать с этим типом переменных.
4. В поле **Имя** введите `PATH`, а в поле **Значение** — значение переменной. Обычно сюда следует ввести сначала значение `%PATH%;`, а за ним пути, которые требуется добавить, разделяя их точкой с запятой. Если для затрагиваемых компьютеров уже определены пользовательские переменные `PATH`, необходимо предоставить связанные пути, чтобы обеспечить сохранение существующих путей.
5. Для управления способом применения настройки применяются опции на вкладке **Общие параметры**. В большинстве случаев переменную `PATH` нужно создать только один раз (вместо того, чтобы групповая политика создавала ее повторно при каждом обновлении). В таких случаях устанавливается флажок **Применить один раз и не применять повторно** (Apply once and do not reapply).
6. Нажмите кнопку **OK**, чтобы сохранить настройку. При следующем обновлении политики элемент предпочтения будет применен должным образом к объекту групповой политики, для которого он был определен.

> ***Осторожно!***
>
> Неправильно заданный путь может вызвать серьезные проблемы. Прежде чем применять обновленный список путей ко многим компьютерам, следует проверить его работоспособность. Один из способов выполнить — это создать в каталоге Active Directory объект групповой политики, который применяется только к одному тестовому компьютеру. Затем для этого объекта групповой политики нужно создать элемент предпочтения и ожидать обновления политики или применить ее посредством команды `gpupdate`. Чтобы проверить результаты применения политики, нужно выйти, а затем снова войти в систему.

Управление расширениями и сопоставлениями расширений файлов

Важным фактором в выполнении приложений также являются расширения файлов и их сопоставления типам файлов. Какие файлы Windows считает исполняемыми, определяется расширением файла. Расширения файлов позволяют исполнять команды, просто введя имя команды в командной строке. А сопоставление расширений файлов типам файлов позволяет открывать файлы документов в соответствующей программе простым двойным щелчком по значку документа. В Windows используются два типа расширений файлов.

- **Расширения для исполняемых файлов.** Исполняемые файлы определяются посредством переменной среды `PATHEXT`, задаваемой с помощью диалогового окна **Переменные среды** или элементов предпочтений групповой политики подобно определению переменной `PATH`. Текущее значение переменной `PATHEXT` можно просмотреть, выполнив команду `set pathext` в консоли командной строки или команду `$env:pathext` в консоли PowerShell. По умолчанию эта переменная имеет значение `.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC`. Таким образом, командная строка знает, какие файлы являются исполняемыми, а какие — нет, вследствие чего при выполнении команд в командной строке указывать расширение исполняемого файла команды не требуется.
- **Расширения файлов для приложений.** Расширения файлов для приложений называются *сопоставлениями файлов* (file associations). Сопоставления файлов делают возможным передавать аргументы исполняемым файлам и открывать документы приложений в соответствующем приложении простым двойным щелчком. Для каждого расширения файла в системе имеется сопоставление файла. Это сопоставление можно просмотреть,

выполнив в командной строке команду `assoc` со следуемым за ней расширением файла, например `assoc .doc` или `assoc .docx`. Каждое сопоставление файла в свою очередь определяет тип файла для расширения. Его можно просмотреть, выполнив в командной строке команду `ftype` со следуемым за ней сопоставлением файла, например `ftype Word.Document.8` или `ftype Word.Document.1`.

> ***Примечание***
>
> Команды `assoc` и `ftype` являются внутренними командами командной строки (`cmd.exe`). Чтобы выполнить команду `assoc` в консоли PowerShell, нужно ввести `cmnd /c assoc`, а затем расширение файла. Например, `cmd /c assoc .doc`. А чтобы выполнить в консоли PowerShell команду `ftype`, нужно ввести `cmd /c ftype`, а затем сопоставление файла. Например, `cmd /c ftype Word.Document.8`.

Приоритет выполнения в командной строке типов исполняемых файлов в каждом пути списка переменной `PATH` устанавливается их порядком в переменной `PATHEXT`. Таким образом, если определенная папка, указанная в перечне `PATH`, содержит несколько исполняемых файлов с одинаковым именем, но разными типами, первым будет выполняться файл типа com, затем файл типа exe, и т. д.

Каждому известному расширению файла в системе сопоставляется соответствующий тип файла, даже для расширений исполняемых файлов. В некоторых случаях типом файла является расширение файла без начальной точки, за которым следует ключевое слово `file`, например, `cmdfile`, `exefile` или `batfile`. А сопоставление файла указывает, что первым передаваемым параметром является имя команды, а остальные параметры передаются приложению. Например, выполнив команду `assoc .exe`, мы увидим, что для исполняемых файлов с расширением exe сопоставляется тип файлов exefile. А выполнив команду `ftype exefile`, мы увидим следующее сопоставление файла:

```
exefile="%1" %*
```

Таким образом, при запуске файла с расширением exe Windows знает, что первое значение является командой, которую требуется выполнить, а все остальное, введенное в командную строку, — параметром, который нужно передать запускаемой команде.

Сопоставления для расширений файлов и типы файлов содержатся в реестре Windows; их можно установить с помощью команд `assoc` и `ftype` соответственно. Чтобы сопоставить расширение файла типу файла, введите в командной строке команду `assoc` вместе с параметром сопоставления, например, `assoc .pl=perlfile`. Чтобы создать в командной строке тип файла, установите соответствие типа файла, включая указание, каким образом использовать параметры, поставляемые вместе с именем команды. Например:

```
ftype perlfile=C:\Perl\Bin\Perl.exe "%1" %*
```

Сопоставить тип файла или протокол определенному приложению можно следующим образом:

1. В Панели управления щелкните на ссылке **Программы**, в окне **Программы** — на ссылке **Программы по умолчанию**, а в этом окне — на ссылке **Сопоставление типов файлов или протоколов с конкретными программами** (Associate a file type or a protocol with a program).
2. Открывшееся окно **Настройка сопоставлений** (Set Associations) содержит список текущих сопоставлений по умолчанию расширений файлов приложениям. Чтобы изменить сопоставление расширения файла программе, выберите в списке требуемое расширение, а затем нажмите кнопку **Изменить программу**.

3. Далее, выполните одно из следующих действий.
   - Следующее диалоговое окно, **Как вы хотите открывать файлы такого типа** (How do you want to open this type of file), содержит список программ, зарегистрированных в системе, как поддерживающих файлы с выбранным расширением. Просто щелкните на рекомендуемой программе из этого списка, чтобы сделать ее программой по умолчанию для данного расширения файла.
   - Щелчок по ссылке **Дополнительно** (More options) внизу окна открывает список дополнительных программ, которые, возможно, могут поддерживать данное расширение. Щелкните на рекомендуемой программе из этого списка, чтобы сделать ее программой по умолчанию для данного расширения файла. Альтернативно, можно выбрать одно из предложений: найти программу в Магазине Windows или другую программу на данном компьютере и сделать ее программой по умолчанию для данного расширения.

Создавать новые типы файлов и сопоставлять расширения файлов типам файлов можно в групповой политике посредством элемента предпочтений. Создать элемент предпочтений для нового типа файла можно следующим образом:

1. В редакторе управления групповыми политиками откройте для редактирования требуемый объект групповой политики.
2. Разверните узел **Конфигурация компьютера\Настройка\Параметры панели управления** и выберите в нем узел **Параметры папок** (Folder options).
3. Щелкните на этом узле правой кнопкой мыши и выберите в контекстном меню команду **Создать**, а во вложенном меню — команду **Тип файла**. Откроется диалоговое окно **Новые свойства типа файла** (New File Type Properties).
4. В списке **Действие** выберите требуемую опцию: **Создать**, **Обновить** или **Удалить**. Каждое из этих действий рассматривается в *главе 6*. Действие **Удалить** используется для создания предпочтения, которое удаляет существующее предпочтение типа файла.
5. В поле **Расширение** введите расширение типа файла без начальной точки, например `pi`.
6. В раскрывающемся списке **Связанный класс** выберите зарегистрированный класс для сопоставления с типом файла.
7. Для управления способом применения настройки предназначены опции на вкладке **Общие параметры**. В большинстве случаев новую переменную нужно создать только один раз. В таких ситуациях установите флажок **Применить один раз и не применять повторно**.
8. Нажмите кнопку **OK**. При следующем обновлении политики элемент предпочтения будет применен должным образом к объекту групповой политики, для которого он был определен.

Создать элемент предпочтений для нового сопоставления расширения файла можно следующим образом:

1. В редакторе управления групповыми политиками откройте для редактирования требуемый объект групповой политики. Разверните узел **Конфигурация пользователя\Настройка\Параметры панели управления** и выберите в нем узел **Параметры папок**.
2. Щелкните на этом узле правой кнопкой мыши и выберите в контекстном меню команду **Создать**, а во вложенном меню — команду **Открыть с помощью** (Open with). Откроется диалоговое окно **Новые свойства окна "Выбор программы"** (New Open With Properties).

3. В списке **Действие** выберите требуемую опцию: **Создать**, **Обновить** или **Удалить**.
4. В поле **Расширение** введите расширение типа файла без начальной точки, например `pi`.
5. Нажмите кнопку обзора справа от поля **Связанная программа** и с помощью открывшегося окна просмотра файловой системы выберите программу, которую требуется сопоставить данному расширению файла.
6. При необходимости можно установить флажок **Использовать по умолчанию**, чтобы сделать сопоставленную программу программой по умолчанию для файлов с ранее указанным расширением файла.
7. Для управления способом применения настройки предназначены опции на вкладке **Общие параметры**. В большинстве случаев новую переменную нужно создать только один раз. В таких ситуациях установите флажок **Применить один раз и не применять повторно**.
8. Нажмите кнопку **OK**. При следующем обновлении политики элемент предпочтения будет применен должным образом к объекту групповой политики, для которого он был определен.

Настройка опций автоматического воспроизведения

В Windows 8 параметры автоматического воспроизведения определяют способ обработки файлов на CD- и DVD-дисках и других съемных носителях. Настроить индивидуальные параметры автоматического воспроизведения для каждого типа CD- и DVD-дисков и других съемных носителей, которые поддерживаются компьютером, можно следующим образом:

1. В Панели управления щелкните на ссылке **Программы**, в окне **Программы** — на ссылке **Программы по умолчанию**, а затем — на ссылке **Настройка параметров автозапуска** (Change autoplay settings).
2. В открывшемся окне **Автозапуск** (рис. 8.6) можно назначить программу автозапуска для каждого типа носителя в списке.

   Для съемных носителей (флешки и т. п.) можно назначить либо общую программу по умолчанию, либо программу по умолчанию для каждого типа мультимедиа. Чтобы задать общую программу по умолчанию, снимите флажок **Выберите, что требуется сделать с каждым из типов носителей** (Chose what to do with each type of media) и в раскрывающемся списке **Съемный носитель** (Removable drive) укажите требуемое действие по умолчанию. Чтобы задать индивидуальные действия по умолчанию, установите этот флажок и в раскрывающемся списке для каждого типа мультимедиа определите требуемое действие.
3. Нажмите кнопку **OK**, чтобы сохранить и применить выполненные настройки.

Добавление и удаление компонентов Windows

В Windows XP и более ранних версиях Windows для добавления и удаления компонентов системы применяется утилита **Установка компонентов Windows** (Add/Remove Windows Components). В Windows Vista и более поздних версиях Windows компоненты операционной системы являются функциональностями, которые включаются и отключаются, а не устанавливаются и удаляются.

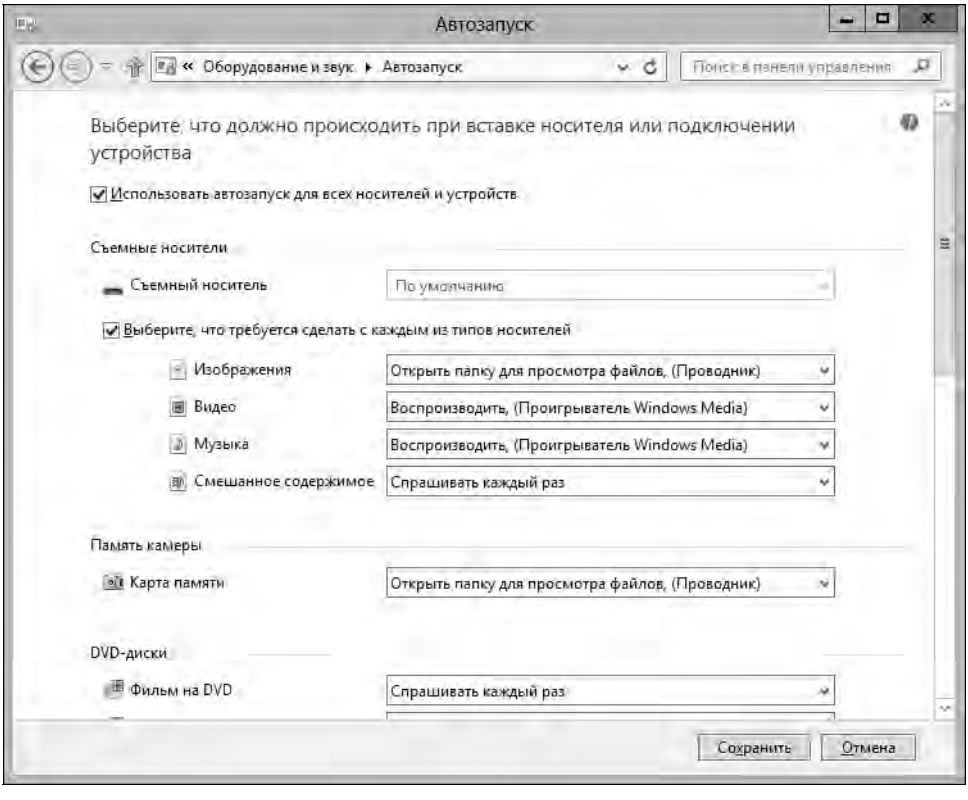


Рис. 8.6. Окно для настройки опций автозапуска для CD- и DVD-дисков и других съемных носителей

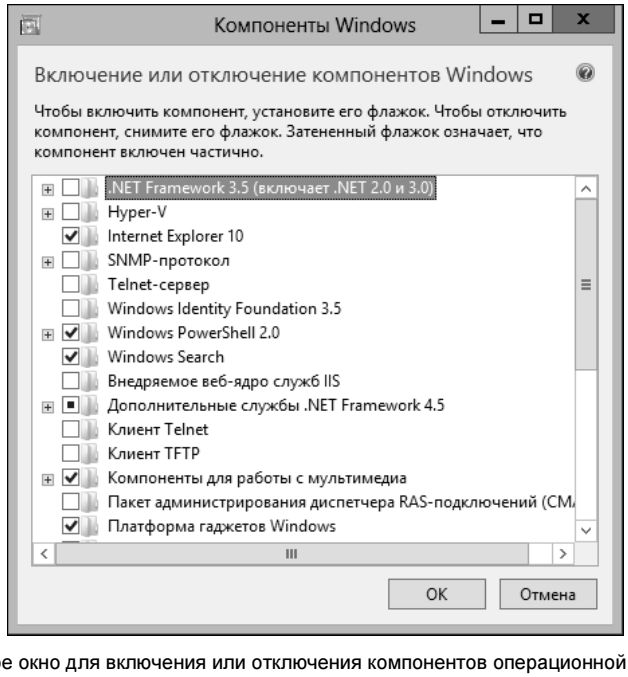


Рис. 8.7. Диалоговое окно для включения или отключения компонентов операционной системы Windows 8

Для включения или отключения компонентов Windows применяется следующая процедура:

1. В Панели управления щелкните на ссылке **Программы** и в разделе **Программы и компоненты** этого окна — на ссылке **Включение или отключение компонентов Windows** (Turn Windows features on or off). Откроется диалоговое окно **Компоненты Windows** (Windows Features) (рис. 8.7).
2. Чтобы отключить компонент Windows, снимите его флажок, а чтобы включить — установите.
3. Нажмите кнопку **OK**, и Windows 8 выполнит требуемые настройки для удовлетворения указанных изменений.

ГЛАВА 9

Управление аппаратными устройствами и драйверами

Управление конфигурацией аппаратных устройств компьютера в большей мере состоит в установке и обслуживании компонентов системы, аппаратных устройств и драйверов устройств. Но управление конфигурацией оборудования компьютеров с системами Windows 7 и Windows 8 значительно отличается от выполнения этой задачи на компьютерах с Windows XP или более ранних версий ОС. В Windows 8 выполняется автоматический мониторинг и обновление многих аспектов системы, вследствие чего их не нужно настраивать или обслуживать подобно тому, как это делалось в более ранних версиях Windows. В Windows 8 применяются следующие возможности:

- автоматическое обслуживание, которое исправляет проблемы, выявленные операционной системой, или уведомляет о них пользователя через Центр поддержки;
- интеллектуальная проверка, предупреждающая пользователя перед запуском неизвестных приложений из Интернета;
- встроенные средства диагностики для мониторинга аппаратных устройств, физической памяти, сетевой среды и производительности;
- средства уведомления о проблемах, которые пытаются автоматически решить проблемы конфигурации и производительности;
- средства диагностики, которые предлагают решения для проблем, которые не поддаются автоматическому решению;
- автоматическое обновление компонентов операционной системы;
- средства обновления драйверов, которые самостоятельно получают требуемые драйверы и обновления драйверов для обнаруженных аппаратных устройств;
- улучшенные средства диагностики проблем совместимости приложений и драйверов.

Эти возможности начинают работать, помогая пользователю отслеживать состояние компьютера и выполнять его техническое обслуживание, сразу же после установки Windows 8. Для администратора эти возможности могут быть полезным руководством по настройке и обслуживанию системы. Для каждой из областей, которые отслеживаются средствами мониторинга, предоставляются отдельные средства, включая средства для диагностирования аппаратных устройств, памяти, сети и производительности.

Для настройки и обслуживания аппаратных устройств и драйверов можно также использовать диспетчер устройств, утилиту Панели управления **Устройства и принтеры** и мастера

добавления устройств и принтеров. Эти инструменты применяются при каждой установке, удалении или диагностировании аппаратных устройств и драйверов. Также предоставляются инструменты для управления специфичными типами аппаратных устройств, такими как клавиатура и звуковые платы. А для автоматического обновления компонентов системы и драйверов применяется утилита Панели управления Центр обновления Windows.

Работа с автоматизированной системой справки и поддержки

Большой объем модернизаций автоматической справки и поддержки в Windows 8 коренным образом изменяет работу операционной системы и ее поддержку и обслуживание. Поэтому администратор в обязательном порядке должен понимать принцип работы архитектуры справки и методы ее настройки.

Использование автоматической справки и поддержки

Операционная система Windows 8 основана на обширной архитектуре диагностирования и решения проблем, которая была разработана для Windows 7. Хотя ранние версии Windows содержали некоторые возможности справки и диагностирования, большинство этих возможностей были не способны самостоятельно выполнять диагностирование и устранение определенных неполадок. Настоящая же инфраструктура, с другой стороны, может определять многие типы проблем с аппаратным обеспечением, памятью и производительностью и автоматически устранять их или же предоставлять пользователю помощь в процессе их устранения.

Операционная система Windows 8 содержит дополнительные надежные драйверы устройств, обладающие лучшими техническими характеристиками, что позволяет устранить многие распространенные причины зависаний и сбоев. Улучшенная отмена ввода-вывода для драйверов устройств обеспечивает организованное восстановление операционной системы после блокировки вызовов и меньшее количество блокируемых дисковых операций ввода-вывода.

Чтобы сократить время простоя и количество перезапусков при установке и обновлении приложений, Windows 8 может в процессе обновления пометить используемые файлы, как требующие обновления, а затем автоматически заменить их при следующем запланированном запуске приложения. В некоторых случаях Windows 8 может сохранить данные приложения, закрыть его, обновить используемые файлы, а затем перезапустить приложение. Для улучшения общей производительности и времени отклика системы Windows эффективно использует память, предоставляет возможность упорядоченного выполнения для групп потоков, а также предлагает несколько механизмов планирования выполнения потоков. Оптимизируя использование памяти и процессов, Windows 8 обеспечивает меньшее влияние фоновых процессов на производительность системы.

По умолчанию Windows использует интеллектуальную проверку, запрашивая одобрение администратора на выполнение неизвестных приложений из Интернета. Уровень проверки можно регулировать, настроив ее просто на вывод предупреждения вместо требования одобрения администратора или же вообще отключив ее.

Windows 8 предоставляет более качественные рекомендации касательно причин зависания устройств. Записи в журналы событий теперь содержат больше подробностей, что облегчает определение причин проблем и их устранение. Для автоматического восстановления сбо-

ев служб Windows 8 использует политики восстановления служб более интенсивно, чем предыдущие версии Windows. При восстановлении службы после сбоя Windows 8 автоматически обрабатывает как компоненты, зависящие от данной службы, так и компоненты, от которых зависит служба. Прежде чем перезапускать службу, испытавшую сбой, Windows запускает службы и системные компоненты, от которых данная служба зависит.

В предыдущих версиях Windows зависшее приложение помечается как "Не отвечает", и пользователь должен завершить выполнение и перезапустить это приложение. Теперь же Windows пытается решить проблему зависшего приложения, используя помощник по совместимости программ и диспетчер перезагрузки (Restart Manager). Помощник по совместимости может обнаруживать ошибки установки, ошибки выполнения и блокировку драйверов, вызываемые проблемами несовместимости. Для решения этих проблем помощник по совместимости предоставляет на выбор: запустить приложения в режиме совместимости или попытаться получить помощь в Интернете через веб-сайт Microsoft. Диспетчер перезапуска может автоматически завершать работу зависших приложений и перезапускать их. Благодаря этому пользователь освобождается от самостоятельного решения проблемы зависших приложений.

Примечание

Для того чтобы автоматическая диагностика и помощь по проблемам совместимости работали должным образом, необходимо, чтобы были запущены и правильно настроены служба политики диагностики и служба помощника по совместимости программ. Эти службы можно запустить и настроить в узле **Службы** консоли **Управление компьютером**. Консоль **Управление компьютером** можно запустить, нажав клавишу <Windows> и выполнив в поле поиска панели **Приложения** команду `compmgmt.msc`. (Это поле становится видимым при нажатии следующей клавиши, после клавиши <Windows>.) Но данный метод работает, только если это поле имеет фокус. Если по каким-либо причинам запустить консоль этим методом не удается, это можно сделать, выполнив указанную команду в консоли командной строки или в окне **Выполнить**.

Практический совет

Технически, узлы верхнего уровня в консоли **Управление компьютером** являются расширениями оснастки, которые были вставлены в консоль MCC, чтобы создать консоль **Управление компьютером**. Делается это таким образом. Откройте консоль MMC, выполнив команду `mmc` в консоли командной строки. В консоли MMC выполните последовательность команд меню **Файл | Добавить или удалить оснастку**, в открывшемся диалоговом окне **Добавление и удаление оснасток** выберите в левой панели оснастку **Управление компьютером** и нажмите кнопку **Добавить**, расположенную между панелями окна. В следующем окне выберите локальный компьютер и нажмите кнопку **Готово**. Оснастка **Управление компьютером** будет добавлена в правую панель окна. Щелкните по ней и нажмите кнопку **Изменить расширения**. В открывшемся диалоговом окне **Управление компьютером — расширения** установите переключатель **Включать только выбранные расширения**. Теперь в списке расширений можно выбирать, какие включать в консоль, а какие — нет. Вот таким образом разработчики Microsoft собрали консоль **Управление компьютером** из отдельных расширений.

Приложения и драйверы, не отвечающие вследствие неудачной установки, также отслеживаются с помощью Центра поддержки. В таких случаях встроенные механизмы диагностики иногда могут предоставить решение проблемы. Список текущих проблем можно просмотреть в любое время одним из следующих способов:

- щелкните по значку Центра поддержки в области уведомлений панели задач, а затем щелкните по ссылке **Открыть центр поддержки** (Open Action Center);
- в Панели управления щелкните по ссылке **Проверка состояния компьютера** (Review your computer's status) в разделе **Система и безопасность**.

Окно **Центр поддержки** (рис. 9.1) содержит список проблем, разбитых на две общие группы: **Безопасность** и **Обслуживание**.

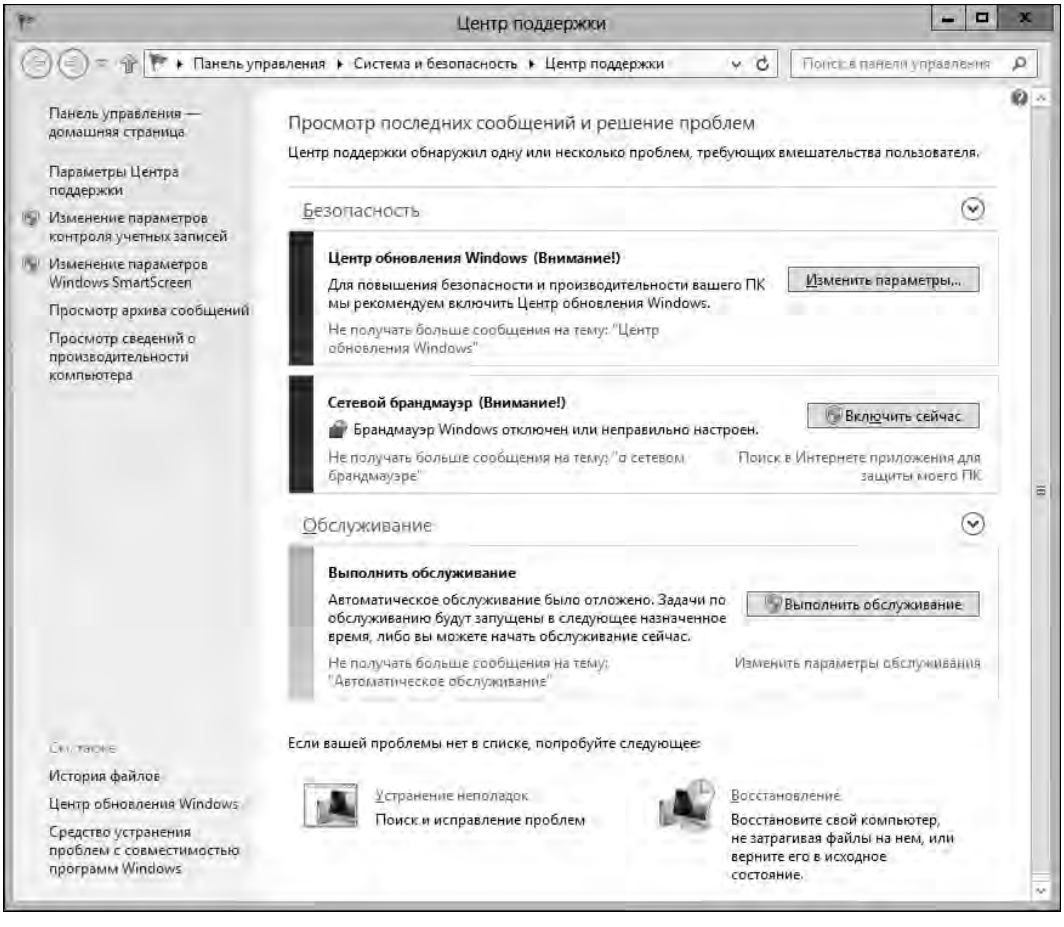


Рис. 9.1. Центр поддержки применяется для просмотра обнаруженных проблем с компьютером

Обнаруженные проблемы отображаются с цветовыми кодами:

- красный цвет обозначает важное предупреждение, требующее внимания. Например, извещение об отсутствии на компьютере средств антивирусной защиты будет помечено красным цветом;
- оранжевым цветом помечаются предупредительные извещения, не требующие немедленного внимания. Например, извещение о том, что после последнего сканирования компьютера Защитником Windows прошло значительное время, будет помечено оранжевым цветом.

Щелчок по заголовку раздела Центра поддержки разворачивает соответствующий раздел, предоставляя дополнительную информацию. Дополнительные сведения раздела **Безопасность** включают:

- состояние сетевого брандмауэра, обновлений Windows, антивирусной защиты, а также защиты компьютера от шпионского и нежелательного программного обеспечения;
- настройку параметров безопасности Интернета, контроля учетных записей пользователей, средства фильтрации Windows SmartScreen, защиты доступа к сети и активации Windows.

Дополнительные сведения раздела **Обслуживание** включают:

- ссылки для управления настройками отчетов о проблемах;
- состояние истории файлов и дисков компьютера;
- состояние автоматического обслуживания и ссылки для управления обслуживанием.

Если нужно проверить наличие проблем на только что введенном в действие компьютере или в случае подозрений на наличие неопределенных проблем на работающем компьютере, можно запустить автоматическое обнаружение проблем, выполнив следующую процедуру:

1. В Центре поддержки разверните раздел **Обслуживание**, щелкнув на его заголовке.
2. Внизу списка текущих проблем находятся область **Поиск решений для указанных в отчетах проблем** (Check for solutions to problem reports) и набор связанных ссылок. Щелкните по ссылке **Поиск решений** (Check for solutions), чтобы запустить процесс автоматического поиска решений. По завершению этого процесса список проблем обновляется новыми обнаруженными проблемами, для которых предоставляются решения, если они известны.
3. Для обнаруженных автоматическим диагностированием проблем, для которых нет известных решений, можно просмотреть дополнительную информацию. Для этого в диалоговом окне **Отчеты о проблемах** (Problem Reporting) щелкните по ссылке **Показать подробности проблемы** (View problem details), вследствие чего внизу окна откроется дополнительная панель, содержащая подробные сведения о выявленных проблемах (рис. 9.2).

   Если вы хотите заняться поиском причин этих проблем самостоятельно, щелкните по предоставленным ссылам, чтобы извлечь связанные данные для дальнейшего анализа. Данные будут извлечены в папку Temp профиля текущего пользователя. Прежде чем выполнять следующие действия, вам нужно будет сделать копии этих данных.

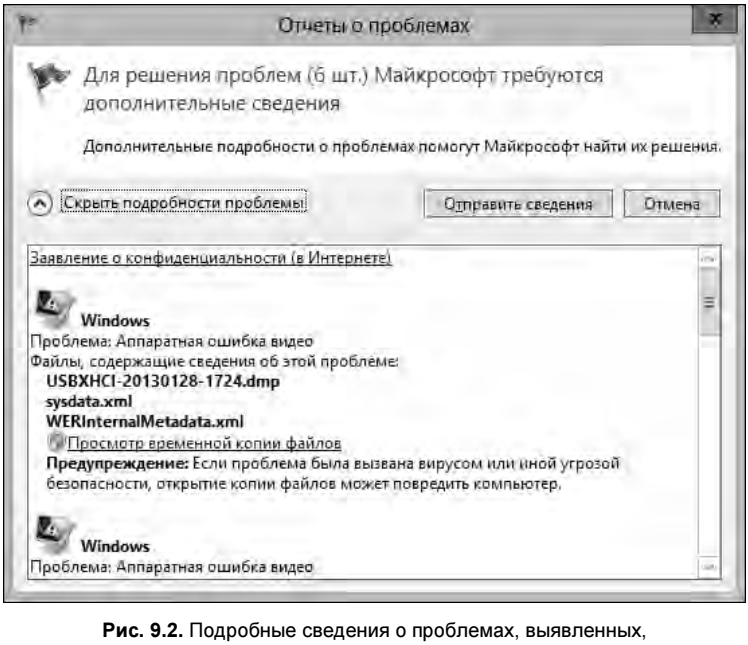


Рис. 9.2. Подробные сведения о проблемах, выявленных, но не решенных автоматическим диагностированием

4. В окне **Отчеты о проблемах** нажмите кнопку **Отправить сведения** (Send information), чтобы отправить эту информацию персоналу Microsoft. Чтобы закрыть окно отчета о проблемах без отправки сведений в Microsoft, нажмите кнопку **Отмена**. В первом случае диагностические данные о проблемах извлекаются в папку Temp профиля текущего пользователя, отправляются в Microsoft, а затем удаляются из папки. Объем извлеченных и отправляемых данных может быть довольно значительным.

В Центре поддержки обнаруженные проблемы, для которых имеются известные решения, можно решить следующим образом:

1. Для каждой проблемы имеется кнопка или ссылка решения. Для проблем из раздела **Безопасность** решения можно обычно найти в Интернете или просканировать компьютер, используя защитное программное обеспечение. А для проблем из раздела **Обслуживание** обычно следует щелкнуть по ссылке **Показать решение проблемы** (View problem response), чтобы открыть страницу с дополнительной информацией о проблеме.
2. При просмотре страницы **Дополнительная информация** (More Information) нужно иметь в виду следующее: для проблем, причиной которых является драйвер или программное обеспечение, предоставляется ссылка для загрузки последней версии драйвера или обновления программы. Для проблем, причиной которых является неправильная настройка, предоставляется описание проблемы и пошаговое руководство изменения настроек для решения проблемы.
3. После решения проблемы установкой нового драйвера или обновления программы сообщение можно заархивировать, в случае если оно понадобится в будущем. Для этого нужно установить флажок **Заархивировать данное сообщение** (Archive this message), после чего нажать кнопку **OK**, чтобы закрыть окно дополнительных сведений.

В Центре поддержки можно также просмотреть журнал проблем с аппаратным и программным обеспечением компьютера, чтобы получить представление о стабильности работы системы и определить, какие устройства или программы вызывают проблемы. Для этого нужно открыть окно монитора стабильности системы, выполнив следующие действия:

1. В Центре поддержки разверните раздел **Обслуживание**, щелкнув по его заголовку.
2. Внизу списка текущих проблем находятся область **Поиск решений для указанных в отчетах проблем** и набор связанных ссылок. Щелкните в этом наборе по ссылке **Показать журнал стабильности работы** (View reliability history).
3. Откроется окно **Монитор стабильности системы** (Reliability Monitor) (рис. 9.3), содержащее графическое представление истории работы системы за определенный период прошедшего времени. Журнал работы системы имеет два представления — по дням и по неделям. По умолчанию используется представление по дням. Для просмотра журнала по неделям щелкните на опции **Недели** (Weeks) слева от текста **Просмотр по:** (View by:). Стабильность компьютера представлена на графике значениями от 1 (плохая) до 10 (отличная).
4. На графике события, которые могли бы повлиять на стабильность, показаны с сопутствующей информацией и/или значком предупреждения. Щелчок по этому значку отображает подробности события в списке **Сведения о стабильности** (Reliability details). Как показано на рис. 9.3, для событий в списке предоставлены их источник, сводная информация, дата события и действие. Столбец события содержит ссылку. Если Windows смогла решить проблему автоматически, ссылка будет типа **Показать решение**, щелчок по которой отображает информацию о том, как ОС решила эту проблему. В других случаях ссылка будет **Показать технические подробности** (View technical details), щелчок по которой открывает окно **Сведения о проблеме** (Problem Details) с дополнительной информацией о проблеме стабильности (рис. 9.4).

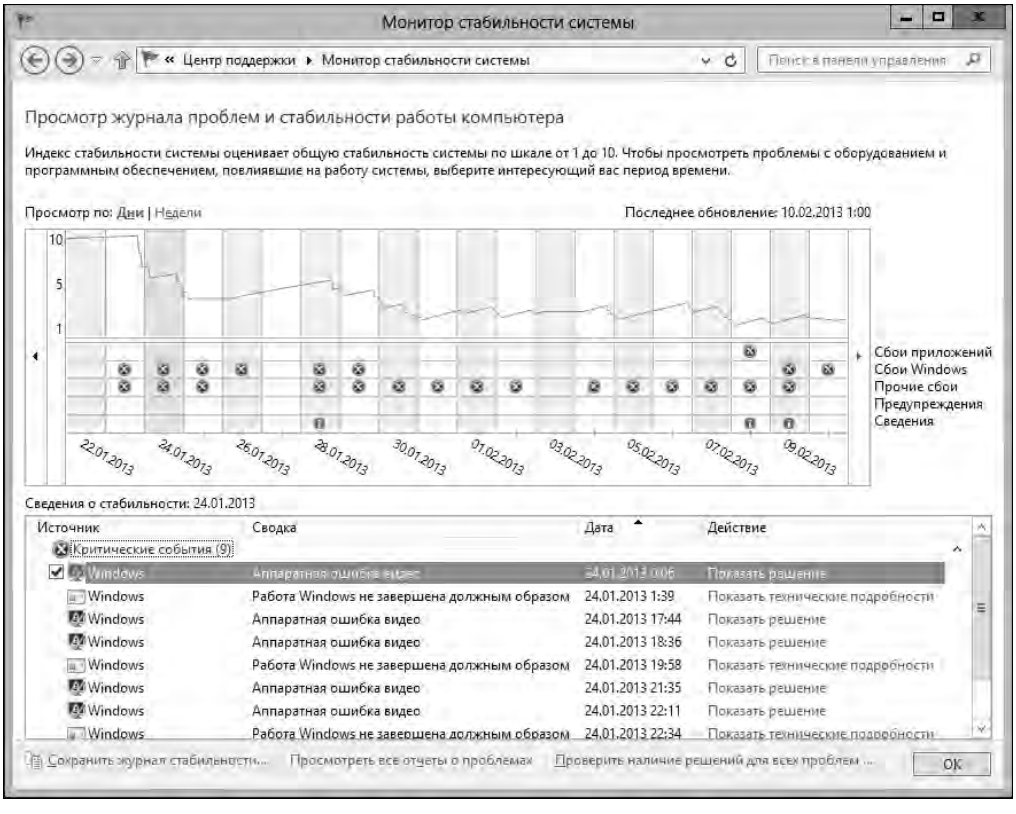


Рис. 9.3. Графический журнал проблем и стабильности системы

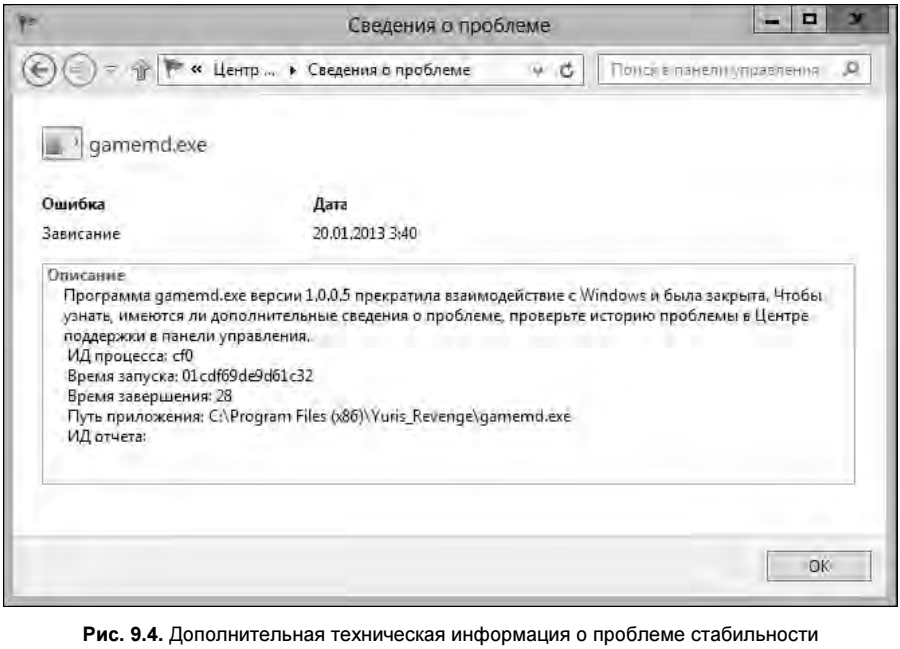


Рис. 9.4. Дополнительная техническая информация о проблеме стабильности

5. Внизу окна монитора стабильности системы доступны следующие опции.
   - **Сохранить журнал стабильности** (Save reliability history). Позволяет сохранить все содержимое журнала в случае надобности в будущем. Информация сохраняется как отчет монитора стабильности системы в формате XML. После щелчка по ссылке **Сохранить журнал стабильности** открывается диалоговое окно для навигации по файловой системе, с помощью которого файл отчета можно сохранить в нужной папке под требуемым именем. Сохраненный отчет стабильности можно просмотреть, открыв его в браузере Internet Explorer.
   - **Просмотреть все отчеты о проблемах** (View all problem reports). Щелчок по этой ссылке открывает окно **Отчеты о проблемах** (Problem Reports), содержащее отчеты обо всех зарегистрированных проблемах и их состоянии. Журнал отчетов можно очистить, нажав кнопку **Очистить все отчеты о проблемах** (Clear all problem reports).
   - **Проверить наличие решений для всех проблем** (Check for solutions to all problems). Автоматически запускает процесс обнаружения проблем. По завершению этого процесса список проблем в Центре поддержки обновляется новыми обнаруженными проблемами, для которых предоставляются решения, если таковые известны.

Настройка автоматической справки и поддержки

Операционная система Windows 8 предоставляет многочисленные средства для настройки работы системы автоматизированной справки и поддержки. На базовом уровне можно управлять типами извещений, отображаемых в Центре поддержки. Более тонкая настройка позволяет управлять диагностированием проблем и созданием отчетов.

Каждый пользователь, который входит в систему, имеет отдельный набор параметров для уведомлений. Задать типы уведомлений, отображаемые в Центре поддержки, можно следующим образом:

1. В левой панели окна Центра поддержки щелкните по ссылке **Параметры Центра поддержки** (Change Action Center settings).
2. В открывшемся одноименном окне (рис. 9.5) установите флажки для сообщений, которые требуется отображать для пользователя, и снимите флажки с ненужных сообщений.
3. По умолчанию пользовательская информация отправляется в Microsoft, как часть программы по улучшению качества программного обеспечения. Если вы не желаете участвовать в этой программе, в нижней части окна **Параметры Центра поддержки** щелкните по ссылке **Параметры программы улучшения качества программного обеспечения**[1] (Customer Experience Improvement Program settings) и в следующем окне установите переключатель **Нет, я не хочу участвовать в программе** (No, I don't want to participate in the program).
4. Нажмите кнопку **Сохранить изменения**, а затем **OK**, чтобы сохранить настройки и закрыть все окна.

В стандартной конфигурации каждый пользователь компьютера имеет отдельные настройки для отчетов о проблемах. Но администратор может задать одинаковые настройки отчетов для всех пользователей. Выполнить настройку параметров отчетов о проблемах для текущего пользователя или для всех пользователей можно следующим образом:

1. В левой панели окна Центра поддержки щелкните по ссылке **Параметры Центра поддержки**.

[1] На рис. 9.5 не видна.

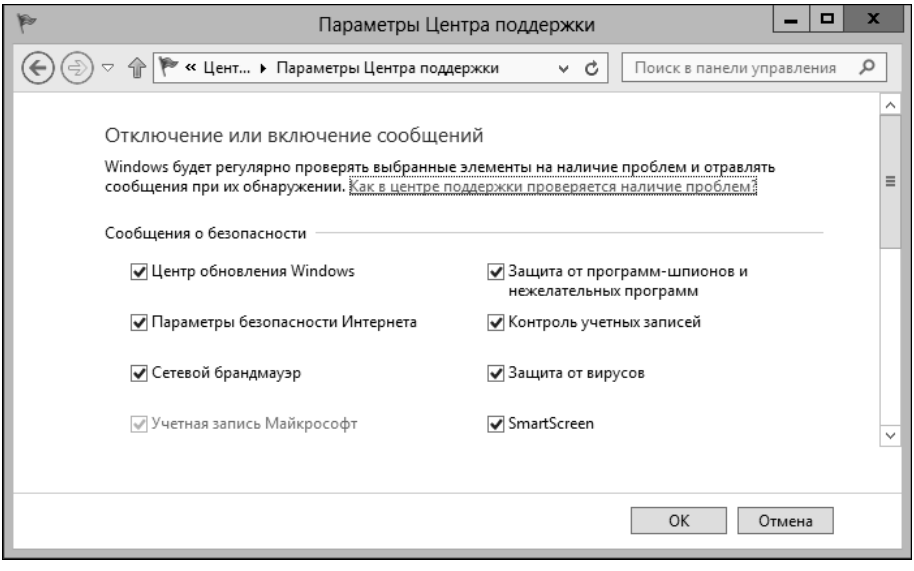


Рис. 9.5. Окно для настройки отображаемых уведомлений Центра поддержки

2. В разделе **Связанные параметры** (Related settings) открывшегося одноименного окна щелкните по ссылке **Параметры отчета о неполадках** (Problem reporting settings).
3. Следующее окно, **Параметры отчетов о проблемах**, содержит параметры настройки отчетов о проблемах для текущего пользователя. Если эти параметры доступны для редактирования, это означает, что компьютер настроен, чтобы позволить отдельным пользователям выбирать собственные параметры отчетов о неполадках. В противном случае компьютер будет настроен на использование одинаковых параметров отчетов о проблемах для всех пользователей.
4. В случае возможности индивидуальной настройки параметров отчетов о проблемах выберите опцию, которую следует применить для текущего пользователя, установив соответствующий переключатель, после чего нажмите кнопку **OK**. Доступны следующие опции:
   - **Автоматически проверять наличие решений** (Automatically check for solutions);
   - **Автоматически проверять наличие новых решений и при необходимости отправлять дополнительные данные отчета** (Automatically check for solutions and send additional report data, if needed);
   - **Каждый раз при возникновении проблемы спрашивать меня о необходимости поиска решений** (Each time a problems occurs, ask me before checking for solutions);
   - **Не проверять на наличие новых решений**(Never check for solutions).
5. В случае одинаковых параметров отчетов о проблемах для всех пользователей компьютера щелкните по ссылке **Изменить параметры отчета для всех пользователей** (Change report settings for all users). В открывшемся диалоговом окне **Отчеты о проблемах** (Problem Reporting) выберите опцию, которую следует применить для всех пользователей, установив соответствующий переключатель, после чего нажмите кнопку **OK**, чтобы сохранить настройки. Доступны следующие опции:
   - **Автоматически проверять наличие решений**;

- **Автоматически проверять наличие новых решений и при необходимости отправлять дополнительные данные отчета**;
- **Каждый раз при возникновении проблемы спрашивать меня о необходимости поиска решений**;
- **Не проверять на наличие новых решений**;
- **Разрешить каждому пользователю изменять параметры** (Allow each user to choose settings).

Функциональность отчетов о проблемах можно настроить, чтобы исключить из них определенные программы. Для этого нужно выполнить следующую процедуру:

1. В левой панели окна Центра поддержки щелкните по ссылке **Параметры Центра поддержки**.
2. В разделе **Связанные параметры** (Related settings) открывшегося окна **Параметры Центра поддержки** щелкните по ссылке **Параметры отчета о неполадках**. Внизу следующего окна, **Параметры отчетов о проблемах**, щелкните по ссылке **Выбрать программы, исключаемые из отчета** (Select programs to exclude from reporting).
3. Следующее окно, **Дополнительные параметры отчетов о проблемах** (Advanced Problem Reporting Settings), содержит список (возможно, пустой) программ, исключенных из отчетов о проблемах. Здесь можно выполнить следующее.
   - Добавить новые программы в список программ, исключенных из отчетов о проблемах. Для этого нажмите кнопку **Добавить** и с помощью открывшегося диалогового окна для навигации по файловой системе выберите исполняемый файл (с расширением exe) программы, после чего нажмите кнопку **Открыть**.
   - Удалить программы из списка программ, исключенных из отчетов о проблемах. Для этого щелкните на программе и нажмите кнопку **Удалить**.

Каждый пользователь, который входит в систему, имеет отдельный набор параметров для средства фильтрации программ Windows SmartScreen. Настройка этих параметров выполняется следующим образом:

1. В левой панели окна Центра поддержки щелкните по ссылке **Изменение параметров Windows SmartScreen** (Change Windows SmartScreen settings).
2. В открывшемся диалоговом окне **Windows SmartScreen** укажите требуемые действия для неизвестных приложений. По умолчанию Windows выводит запрос на одобрение администратором для выполнения неизвестных приложений из Интернета. Уровень проверки можно регулировать, настроив ее просто на вывод предупреждения вместо требования одобрения администратора или же вообще отключив ее.
3. Указав требуемое действие, нажмите кнопку **OK**, чтобы сохранить настройки.

Каждый пользователь, который входит в систему, имеет отдельный набор параметров для автоматического обслуживания. Настройка этих параметров выполняется следующим образом:

1. В Центре поддержки разверните раздел **Обслуживание**, щелкнув по его заголовку.
2. В области **Автоматическое обслуживание** внизу списка текущих проблем обслуживания щелкните по ссылке **Изменить параметры обслуживания** (Change maintenance settings).
3. Откроется диалоговое окно **Автоматическое обслуживание** (Automatic Maintenance) (рис. 9.6).

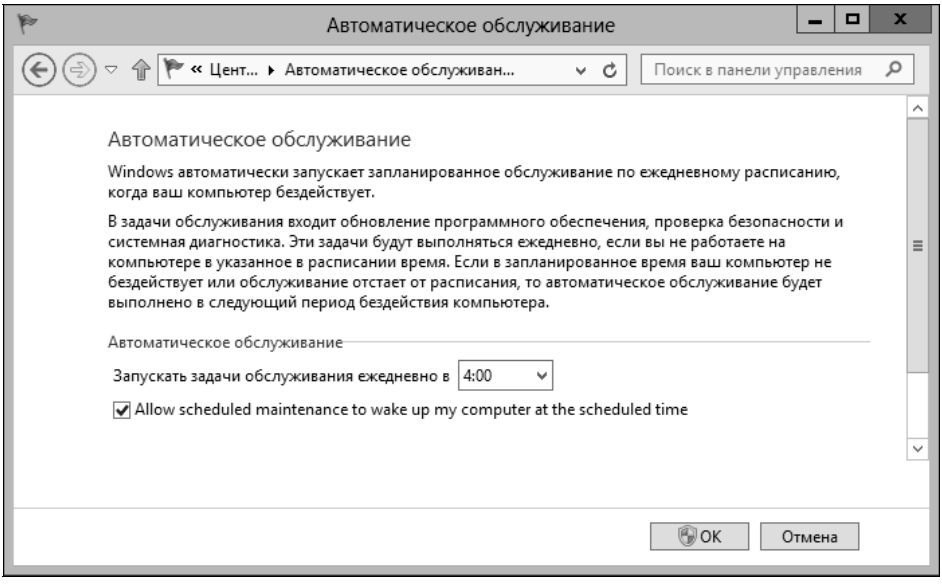


Рис. 9.6. Диалоговое окно для настройки автоматического обслуживания

4. В раскрывающемся списке **Запускать задачи обслуживания ежедневно в** (Run maintenance tasks daily at) выберите требуемое время для начала выполнения автоматического обслуживания.
5. Чтобы разрешить вывод компьютера из режима сна для выполнения обслуживания, установите флажок **Allow scheduled maintenance to wake up my computer at the scheduled time** (Разрешать задаче обслуживания пробуждать мой компьютер в запланированное время).
6. Нажмите кнопку **OK**, чтобы сохранить и применить выполненные настройки.

Функциональность автоматического обслуживания является частью инфраструктуры диагностики Windows. По умолчанию, если компьютер запитан от сети и не используется, в 3 часа утра Windows 8 запускает процесс планового технического обслуживания. При других обстоятельствах техническое обслуживание запускается при следующей работе компьютера от сети и простаивающей операционной системе. Так как техническое обслуживание выполняется только при простаивающей системе, этот процесс может исполняться в фоновом режиме на протяжении трех дней. Таким образом, Windows 8 имеет возможность завершить выполнение сложных задач технического обслуживания системы.

Статус автоматического обслуживания отображается в разделе **Обслуживание** Центра поддержки. Там же предоставляются другие опции обслуживания. Информация о состоянии обслуживания содержит последнюю дату выполнения, а также необходимость предпринятия каких-либо корректирующих действий. Если техническое облуживание выполняется в настоящее время, это отображается в состоянии. Обслуживание системы можно запустить вручную, щелкнув по ссылке **Начать обслуживание** (Start maintenance).

Автоматическое обслуживание работает, как назначенное задание. В библиотеке планировщика заданий это задание находится в узле **Microsoft\Windows\Diagnosis**; подробные сведения о выполнении этого задания можно просмотреть на его вкладке **Журнал** (History).

Каждый пользователь, который входит в систему, имеет отдельный набор параметров диагностирования. Настройка этих параметров выполняется следующим образом:

1. В Центре поддержки разверните раздел **Обслуживание**, щелкнув по его заголовку.
2. Внизу списка текущих проблем щелкните по ссылке **Устранение неполадок** (Troubleshooting), а в левой панели одноименного окна — по ссылке **Настройка** (Change settings).
3. Откроется окно **Настройка** (Change settings) (рис. 9.7), содержащее настройки средства устранения проблем. По умолчанию Windows периодически проверяет наличие распространенных проблем и выводит сообщения, если средство устранения проблем способно решить их. Например, пользователь может быть уведомлен о неиспользуемых файлах и ярлыках, которые можно удалить.

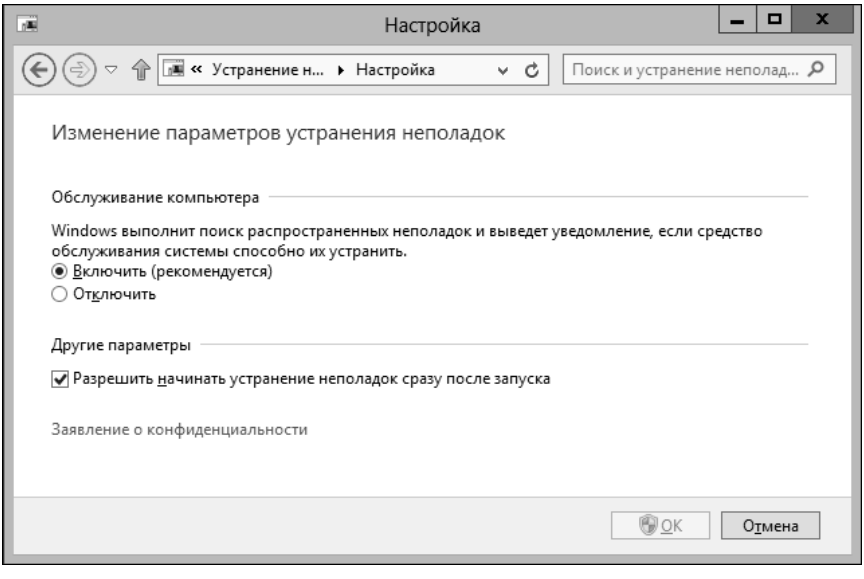


Рис. 9.7. Диалоговое окно для настройки средства устранения проблем

4. По умолчанию процесс поиска и устранения неполадок начинается сразу же после запуска средства устранения проблем. Если предполагается, что пользователь будет подтверждать запуск этого процесса, нужно снять флажок **Разрешить начинать устранение неполадок сразу после запуска** (Allow troubleshooting being immediately when started).
5. Нажмите кнопку **OK**, чтобы сохранить и применить настройки.

Средства устранения неполадок помогают автоматически определять и решать проблемы с операционной системой. Функциональность автоматизированного поиска и устранения неполадок зависит от оболочки Windows PowerShell и связанных системных служб. При условии, что оболочка Windows PowerShell установлена (а она устанавливается по умолчанию с установкой системы) и требуемые службы доступны, эта функциональность будет работать.

Стандартные средства поиска и устранения неполадок применяются для обслуживания следующих областей системы.

- **Direct Access.** Диагностика и решение проблем, не позволяющих использовать функциональность DirectAccess для подключения к компьютерам корпоративной сети.
- **Аппаратное обеспечение и устройства.** Диагностика и решение проблем, не позволяющих использовать устройства должным образом.

- **Домашняя группа.** Диагностика и решение проблем с просмотром компьютеров и общих файлов домашней группы.
- **Входящие подключения.** Диагностика и решение проблем с блокировкой входящих подключений.
- **Интернет-подключения.** Диагностика и решение проблем с подключением к Интернету и доступом к веб-сайтам.
- **Производительность Internet Explorer.** Диагностика и решение проблем, влияющих на общую производительность Internet Explorer.
- **Безопасность Internet Explorer.** Определение проблем с настройками, которые могут нарушить безопасность компьютера и пользователя при работе в Интернете.
- **Сетевой адаптер.** Диагностика и решение проблем, связанных с проводными, беспроводными и другими сетевыми адаптерами.
- **Воспроизведение аудио.** Диагностика и решение проблем, не позволяющих воспроизводить аудио.
- **Электропитание.** Диагностика и решение проблем с электропитанием компьютера.
- **Принтер.** Диагностика и решение проблем, не позволяющих использовать принтеры.
- **Совместимость программ.** Диагностика и решение проблем с выполнением на компьютере старых программ.
- **Запись аудио.** Диагностика и решение проблем, не позволяющих записывать аудио.
- **Поиск и индексирование.** Диагностика и решения проблем с функциональностями Windows для поиска и индексирования.
- **Общие папки.** Диагностика и решение проблем с доступом к общим файла и папкам на других компьютерах.
- **Обслуживание системы.** Выполнение повседневного обслуживания системы, если пользователь сам забывает делать это.
- **Обновление Windows.** Диагностика и решение проблем с использованием функциональности обновления Windows.

> ***Совет***
>
> В групповой политике администраторы могут настраивать параметры политики **Помощь при ошибке "Отказано в доступе"** (Access-Denied Accistance), чтобы помочь пользователям определить, к кому им нужно обращаться в случае проблем с доступом к файлам, и выводить специализированные сообщения об ошибке отказа в доступе. Чтобы активировать помощь при ошибке отказа в доступе, включите параметр этой политики **Включить исправление ошибки "Отказано в доступе" для всех типов файлов клиента** (Enable access-denied assistance on client for all file types). Для настройки метода работы помощи при ошибке отказа в доступе используется параметр **Настроить сообщение об ошибке "Отказано в доступе"** (Customize message for access-denied errors). Эта политика и ее параметры находятся в узле **Конфигурация компьютера\Административные шаблоны** редактора локальной групповой политики.

Доступ ко всем этим средствам поиска и устранения неполадок можно получить в окне **Устранение неполадок** (Troubleshooting) (рис. 9.8), открыть которое можно, щелкнув на одноименной ссылке под списком проблем в разделе **Обслуживание** Центра поддержки.

Как можно видеть на рис. 9.8, средства поиска и устранения неполадок организованы по следующим категориям:

- **Программы** — применяются для исправления неполадок совместимости с приложениями, предназначенными для более ранних версий Windows;

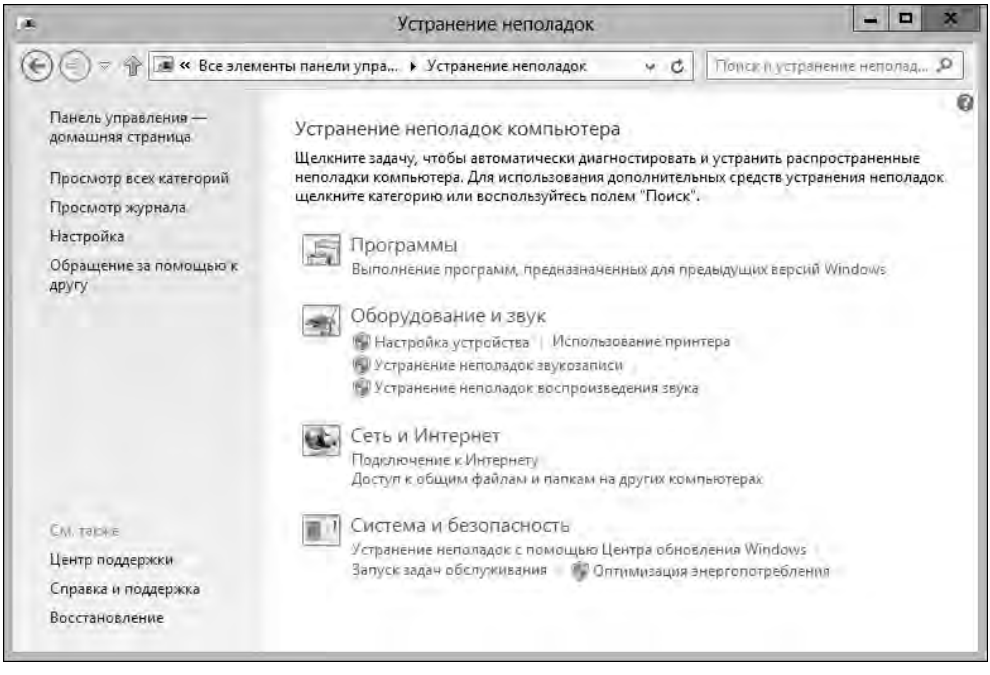


Рис. 9.8. Окно доступа к средствам поиска и устранения неполадок

- **Оборудование и звук** — предназначены для поиска и устранения проблем с аппаратными устройствами и записью и воспроизведением аудио;
- **Сеть и Интернет** — для поиска и устранения проблем с подключением к сетям и доступом к общим папкам на других компьютерах;
- **Система и безопасность** — для поиска и устранения неполадок с функциональностью обновления Windows, энергопотреблением и производительностью. Например, для удаления неиспользуемых файлов и ярлыков и выполнения других повседневных задач обслуживания щелкните по ссылке **Запуск задач обслуживания** (Run administrative tasks).

Работой автоматического обслуживания системы можно управлять посредством настройки параметров групповой политики **Диагностика** (Troubleshooting and Diagnostics), которая расположена в узле **Конфигурация компьютера\Административные шаблоны\Система** редактора локальной групповой политики. В табл. 9.1 представлены параметры для управления Центром поддержки и связанными возможностями.

Таблица 9.1. *Параметры из узла для управления Центром поддержки и связанными возможностями*

Параметр	Описание	Узел редактора групповой политики
Отключить программу по обеспечению качества программного обеспечения Windows (Turn off Windows Customer Experience Improvement Program)	Если этот параметр выключен, пользователи не участвуют в программе, а если включен — участвуют	**Конфигурация компьютера\ Административные шаблоны\ Система\Управление связью через Интернет\Параметры связи через Интернет** (Computer Configuration\Administrative Templates\System\Internet Communication Management\Internet Communication Settings)

Таблица 9.1 *(продолжение)*

Параметр	Описание	Узел редактора групповой политики
Обнаруживать сбои приложений, вызванные устаревшими COM-объектами (Detect application failures caused by deprecated COM objects)	При включенном или не заданном параметре Windows обнаруживает программы, пытающиеся создать устаревшие COM-объекты, и извещает об этом пользователей	**Конфигурация компьютера\ Административные шаблоны\ Система\Диагностика\Диагностика совместимости приложений** (Computer Configuration\Administrative Templates\System\Troubleshooting and Diagnostics\Application Compatibility Diagnostics)
Обнаруживать сбои приложений, вызванные устаревшими библиотеками DLL Windows (Detect application failures caused by deprecated Windows DLLs)	При включенном или не заданном параметре Windows обнаруживает программы, пытающиеся использовать устаревшие библиотеки DLL, и извещает об этом пользователей	**Конфигурация компьютера\ Административные шаблоны\ Система\Диагностика\Диагностика совместимости приложений** (Computer Configuration\Administrative Templates\System\Troubleshooting and Diagnostics\Application Compatibility Diagnostics)
Обнаруживать ошибки совместимости приложений и драйверов (Detect compatibility issues for application and drivers)	При включенном или не заданном параметре Windows обнаруживает сбои при установке и выполнении программ и блокировку драйверов, вызываемые проблемами совместимости, и извещает об этом пользователей	**Конфигурация компьютера\ Административные шаблоны\ Система\Диагностика\Диагностика совместимости приложений** (Computer Configuration\Administrative Templates\System\Troubleshooting and Diagnostics\Application Compatibility Diagnostics)
Уведомлять о блокированных драйверах (Notify blocked drivers)	При включенном параметре Windows уведомляет пользователей о драйверах, заблокированных в связи с проблемами совместимости	**Конфигурация компьютера\ Административные шаблоны\ Система\Диагностика\Диагностика совместимости приложений** (Computer Configuration\Administrative Templates\System\Troubleshooting and Diagnostics\Application Compatibility Diagnostics)
Устранение неполадок: разрешить пользователям запускать мастера устранения неполадок (Troubleshooting: Allow users to access and run Troubleshooting Wizards)	При включенном или не заданном параметре пользователи могут запускать средства поиска и устранения неполадок в Центре поддержки	**Конфигурация компьютера\ Административные шаблоны\Система\Диагностика\Диагностика со сценариями** (Computer Configuration\Administrative Templates\System\Troubleshooting and Diagnostics\Scripted Diagnostics)
Устранение неполадок: разрешить пользователям доступ к сведениям об устранении неполадок, расположенным на серверах корпорации Майкрософт, из компонента "Устранение неполадок" панели управления (Troubleshooting: Allow users to access online troubleshooting content on Microsoft servers from the Troubleshooting Control Panel)	При включенном или не заданном параметре, подключенные к Интернету пользователи могут получать доступ и осуществлять поиск в материалах, расположенных на серверах корпорации Microsoft. Доступ к этим материалам осуществляется нажатием кнопки **Да** в окне запроса Центра поддержки на получение наиболее новых сведений по поиску и устранению неполадок	**Конфигурация компьютера\ Административные шаблоны\ Система\Диагностика\Диагностика со сценариями** (Computer Configuration\Administrative Templates\System\Troubleshooting and Diagnostics\Scripted Diagnostics)

Таблица 9.1 *(окончание)*

Параметр	Описание	Узел редактора групповой политики
Отключение обработчика совместимости приложений (Turn off Application Compatibility Engine)	Если этот параметр включен, Windows не сверяется с базой данной совместимости перед запуском приложений	**Конфигурация компьютера\ Административные шаблоны\ Компоненты Windows\Совместимость приложений** (Computer Configuration\Administrative Templates\Windows Components\Application Compatibility)
Отключение доступа к разделу решения проблем производительности (Turn off access to the solutions to performance problems section)	При включенном параметре пользователи не имеют доступа к решениям проблем производительности. В противном случае доступ предоставляется	**Конфигурация компьютера** и **Конфигурация пользователя\ Административные шаблоны\ Система\Панель управления производительностью** (Computer Configuration и User Configuration\Administrative Templates\System\Performance Control Panel)
Отключение помощника по совместимости программ (Turn off Program Compatibility Assistant)	При включенном параметре Windows не отслеживает запущенные пользователем программы в процессе их выполнения на предмет проблем несовместимости	**Конфигурация компьютера** и **Конфигурация пользователя\ Административные шаблоны\ Компоненты Windows\Совместимость приложений** (Computer Configuration и User Configuration\Administrative Templates\Windows Components\Application Compatibility)
Настроить очередь отчетов (Configure Report Queue)	При включенном и настроенном параметре администратор может выполнять настройку очереди и уведомлений отчетов об ошибках	**Конфигурация компьютера** и **Конфигурация пользователя\ Административные шаблоны\ Компоненты Windows\Отчеты об ошибках Windows\Параметры расширенного отчета об ошибках** (Computer Configurations и User Configuration\Administrative Templates\Windows Components\Windows Error Reporting\Advanced Error Reporting Settings)
Отключить отчеты об ошибках Windows (Disable Windows Error Reporting)	Если этот параметр отключен, служба отчетов об ошибках Windows не будет отправлять информацию об ошибках в корпорацию Microsoft; в противном случае информация отправляется	**Конфигурация компьютера** и **Конфигурация пользователя\ Административные шаблоны\ Компоненты Windows\Отчеты об ошибках Windows** (Computer Configuration и User Configuration\Administrative Templates\Windows Components\Windows Error Reporting)
Удалить значок Центра поддержки (Remove the Action Center icon)	При включенном параметре значок Центра поддержки не отображается в области уведомлений панели задач, хотя пользователи могут открыть Центр поддержки из Панели управления. В противном случае значок Центра поддержки отображается	**Конфигурация пользователя\ Административные шаблоны\Меню "Пуск" и панель задач** (User Configuration\Administrative Templates\Start Menu and Taskbar)

Работа со службами поддержки

С целью поддержки средств автоматической диагностики и устранения неполадок Windows 8 предоставляет отдельные компоненты и инструменты для работы и управления функциональностями диагностики, создания отчетов о проблемах и предоставления помощи пользователям. Все эти компоненты полагаются на доступность служб поддержки, установленных с операционной системой. Подузел **Службы** узла **Службы и приложения** утилиты **Управление компьютером** содержит разнообразные службы, предназначенные для обеспечения поддержки системы.

В табл. 9.2 приведен список и краткие сведения о ключевых службах поддержки Windows 8. Возможности обнаружения и устранения неполадок в основном поддерживаются службой политики диагностики (Diagnostic Policy Service) и службой **Узел системы диагностики** (Diagnostic System Host). Еще одна связанная служба, **Узел службы диагностики** (Diagnostic Service Host), запускается только по мере надобности.

Таблица 9.2. *Службы поддержки Windows 8*

Имя службы	Описание
Служба помощника по совместимости программ (Application Experience)	Обрабатывает запросы на проверку совместимости для приложений по мере их запуска
Сведения о приложении (Application Information)	Позволяет пользователям запускать приложения с дополнительными полномочиями администратора
Управления приложениями (Application Management)	Обрабатывает запросы на установку, удаление и перечисление программ, развернутых посредством групповой политики
Фоновая интеллектуальная служба передачи (Background Intelligent Transfer Service)	Передает файлы в фоновом режиме, используя незанятую пропускную способность сети
Служба политики диагностики (Diagnostic Policy Service)	Позволяет обнаруживать проблемы, устранять неполадки и разрешать вопросы, связанные с работой компонентов Windows
Узел службы диагностики (Diagnostic Service Host)	Позволяет использовать средства диагностики, запускаемые в контексте локальной службы
Узел системы диагностики (Diagnostic System Host)	Позволяет использовать средства диагностики, запускаемые в контексте локальной службы
Поддержка элемента панели управления "Отчеты о проблемах и их решениях" (Problem Reports and Solutions Control Panel Support)	Предоставляет поддержку для создания отчетов системного уровня
Служба помощника по совместимости программ (Program Compatibility Assistant Service)	Предоставляет поддержку для помощника по совместимости программ
Вторичный вход в систему (Secondary Logon)	Позволяет запускать процессы, используя альтернативные учетные данные
Superfetch (Superfetch)	Позволяет улучшить производительность системы посредством предварительного получения данных для компонентов и приложений на основе закономерностей их использования
Служба уведомления о системных событиях (System Event Notification Service)	Отслеживает системные события и предоставляет услуги уведомления

Таблица 9.2 *(окончание)*

Имя службы	Описание
Планировщик задач (Task Scheduler)	Позволяет пользователям планировать автоматическое выполнение задач
Темы (Themes)	Позволяет использовать и управлять темами оформления рабочего стола
Служба профилей пользователей (User Profile Service)	Отвечает за загрузку и выгрузку профилей пользователя при входе и выходе из системы
Служба регистрации ошибок Windows (Windows Error Reporting Service)	Разрешает отправку об ошибках в случае зависания программ и позволяет получать решения проблем
Журнал событий Windows (Windows Event Log)	Позволяет протоколировать события
Инструментарий управления Windows (Windows Management Instrumentation)	Предоставляет информацию для управления системой
Установщик модулей Window (Windows Modules Installer)	Поддерживает установку рекомендуемых и необязательных обновлений компонентов Windows
Служба удаленного управления Windows (Windows Remote Management)	Позволяет удаленное выполнение команд оболочки Windows PowerShell и использование протокола WS-Management для удаленного управления системой
Служба времени Windows (Windows Time)	Используется для синхронизации времени системы со временем по Гринвичу
Центр обновлений Windows (Windows Update)	Позволяет выполнять обновление компонентов Windows и других программ

Как можно видеть по количеству служб поддержки, встроенная в Windows 8 автоматическая система поддержки довольно сложная. Эта система поддержки разработана для автоматического отслеживания работоспособности системы, выполнения профилактического обслуживания и уведомления о проблемах, чтобы их можно было устранить. Связанные данные о производительности и надежности можно отслеживать в Системном мониторе (Performance Monitor) и в Мониторе стабильности системы (Reliability Monitor).

Службы поддержки составляют основу расширенных функциональностей поддержки в Windows 8. Если критические службы не работают или не настроены должным образом, могут возникнуть проблемы с использованием некоторых функциональностей поддержки. Просмотреть службы поддержки, а также другие службы можно в утилите **Управление компьютером**:

1. В Панели управления щелкните по ссылке **Система и безопасность**, в следующем окне — по ссылке **Администрирование** (Administrative Tools), а в следующем — дважды щелкните по значку **Управление компьютером** (Computer Management).
2. Нажмите или щелкните правой кнопкой мыши по узлу **Управление компьютером** в дереве консоли и в контекстном меню выберите команду **Подключиться к другому компьютеру** (Connect to another computer). С помощью открывшегося окна **Выбор компьютера** выберите систему, чьи службы требуется просмотреть.
3. Разверните узел **Службы и приложения**, дважды щелкнув на нем, и выберите в нем узел **Службы** (рис. 9.9).

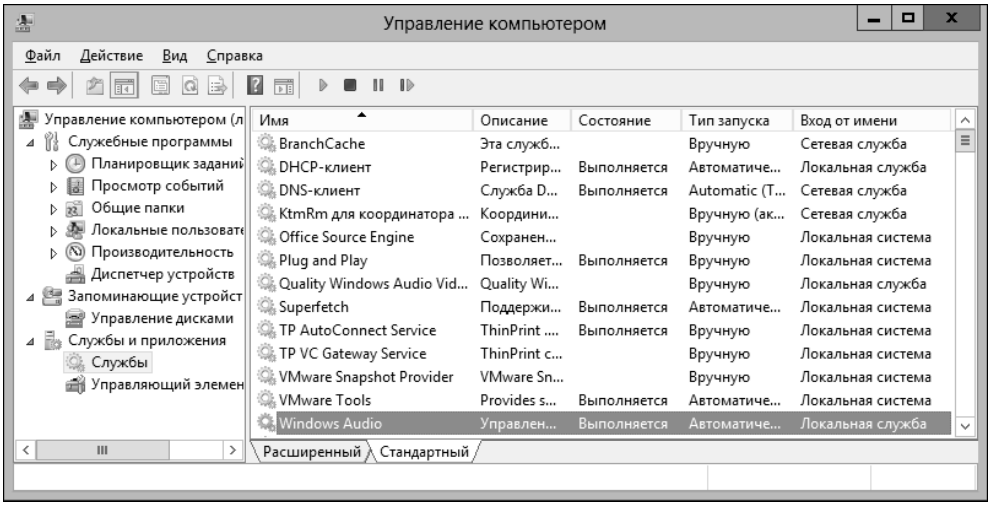


Рис. 9.9. Узел **Службы** консоли **Управление компьютером**

Этот узел содержит все службы, установленные на компьютере. По умолчанию службы в списке упорядочены по имени. Запись каждой службы имеет несколько полей, назначение которых следующее:

- **Имя** (Name) — имя службы. В списке перечислены только установленные в системе службы. Двойной щелчок по службе открывает диалоговое окно для настройки запуска и других параметров службы;
- **Описание** (Description) — краткое описание службы и ее назначение;
- **Состояние** (Status) — рабочее состояние службы: выполняется, остановлена или отключена (остановленная служба обозначается пробелом в поле состояния);
- **Тип запуска** (Startup Type) — тип запуска службы. Автоматически запускаемые службы запускаются при старте системы. Службы, запускаемые вручную, запускаются пользователями или другими службами. Отключенные службы запустить нельзя;
- **Вход от имени** (Log On As) — учетная запись, по которой служба выполняет вход в систему. По умолчанию большинство служб использует учетную запись **Локальная система** (LocalSystem).

4. Панель сведений служб имеет два представления: **Расширенный** и **Стандартный**. Переключение представлений осуществляется выбором соответствующей вкладки внизу панели сведений. В расширенном представлении предоставляются ссылки для управления службами. Для запуска остановленной службы нужно щелкнуть по ссылке **Запустить**, чтобы перезапустить работающую службу — по ссылке **Перезапустить**, чтобы остановить ее — по ссылке **Остановить**. В расширенном представлении также предоставляется подробное описание службы в левой части панели сведений.

Запуск, остановка и приостановка служб

Администратору часто приходится запускать, останавливать или приостанавливать работу служб Windows. Общая процедура для этого следующая:

1. В консоли **Управление компьютером** разверните узел **Службы и приложения** и выберите в нем узел **Службы**.

2. Щелкните правой кнопкой мыши на требуемой службе и в контекстном меню выберите необходимую опцию — **Запустить**, **Остановить** или **Приостановить**.

> ***Примечание***
>
> Также имеется опция перезапуска службы, когда служба сначала останавливается, а затем снова запускается. Для этого используется кнопка **Перезапустить**. Кроме этого, для возобновления работы приостановленной службы применяется кнопка **Возобновить** (Resume). В случае сбоя при запуске автоматически запускаемой службы пользователь обычно извещается об этом, а поле статуса этой службы остается пустым. Сбои в работе служб также можно записывать в системные журналы событий. В операционной системе Windows 8 можно настроить действия для автоматической обработки сбоев службы. Например, можно настроить Windows 8 в случае сбоя службы на попытку перезапустить ее.

Настройка запуска службы

В Windows 8 службы можно настроить для ручного или автоматического запуска, а также отключить их полностью. Настройка запуска службы выполняется следующим образом:

1. В консоли **Управление компьютером** разверните узел **Службы и приложения** и выберите в нем узел **Службы**.
2. Щелкните правой кнопкой мыши на требуемой службе, а затем в контекстном меню выберите команду **Свойства**.
3. На вкладке **Общие** окна свойств службы в раскрывающемся списке **Тип запуска** (Startup type) выберите требуемый тип запуска, а затем нажмите кнопку **OK**:
   - **Автоматически** (Automatic) — служба запускается автоматически при запуске компьютера;
   - **Автоматически (отложенный старт)** (Automatic (Delayed Start)) — служба запускается автоматически при запуске компьютера, но с задержкой, после запуска системы и всех других служб, запускаемых без задержки;
   - **Вручную** (Manual) — служба запускается вручную;
   - **Отключена** (Disabled) — отключает службу.

Настройка входа службы в систему

Службы Windows 8 можно настроить на вход в систему по системной учетной записи или по учетной записи определенного пользователя. Общая процедура для этого следующая:

1. В консоли **Управление компьютером** разверните узел **Службы и приложения** и выберите в нем узел **Службы**.
2. Щелкните правой кнопкой мыши на требуемой службе, а затем в контекстном меню выберите команду **Свойства**.
3. В окне свойств выберите вкладку **Вход в систему** (Log On). Выполните одно из следующих действий, а затем нажмите кнопку **OK**.
   - Установите переключатель **С системной учетной записью** (Local System account) для входа службы в систему с помощью системной учетной записи (вход по умолчанию для большинства служб). Если служба предоставляет пользовательский интерфейс, которым можно манипулировать, установите флажок **Разрешить взаимодействие с рабочим столом** (Allow service to interact with desktop), чтобы пользователи могли управлять интерфейсом службы.
   - Для входа службы в систему по учетной записи определенного пользователя установите переключатель **С учетной записью** (This account), а затем введите имя учетной

записи и пароль для нее в соответствующие поля. Можно также выполнить поиск требуемой учетной записи, нажав кнопку **Обзор**.

Настройка восстановления службы

При установке Windows 8 выполняется настройка критических системных служб для восстановления после сбоя. В большинстве случаев критические службы настроены для автоматического перезапуска после сбоя. Изменить эту настройку нельзя, т. к. такой возможности не предоставляется.

Настроить восстановление других служб после сбоя можно следующим образом:

1. В консоли **Управление компьютером** разверните узел **Службы и приложения** и выберите в нем узел **Службы**.
2. Щелкните правой кнопкой мыши на требуемой службе, а затем в контекстном меню выберите команду **Свойства**.
3. В открывшемся окне свойств службы выберите вкладку **Восстановление** (Recovery).
4. Здесь можно указать опции восстановления после первого, второго и последующих сбоев службы. Доступны следующие опции:
   - **Не выполнять никаких действий** (Take No Action) — операционная система не будет предпринимать попыток восстановить работу службы после этого сбоя, но, тем не менее, может пытаться выполнить восстановления после предыдущего или последующих сбоев;
   - **Перезапуск службы** (Restart The Service) — операционная система после сбоя попытается снова запустить службу;
   - **Запуск программы** (Run A Program) — в случае сбоя выполняется программа или сценарий, который может быть пакетной программой или сценарием Windows. При выборе этой опции необходимо указать полный путь к программе, которую требуется исполнить, а также задать параметры для передачи программе (если таковые требуются);
   - **Перезагрузка компьютера** (Restart The Computer) — выполняется перезагрузка компьютера. При выборе этой опции проверьте параметры загрузки и восстановления компьютера. Желательно, чтобы система могла быстро и автоматически выбрать параметры по умолчанию.

   Совет

   При настройке восстановления критических служб можно задать перезапуск службы после первых двух сбоев, а после третьего перезагрузить компьютер.

5. Выполните настройку других параметров в зависимости от ранее установленных параметров восстановления, а затем нажмите кнопку **OK**. Если для восстановления службы выбрана опция запуска программы, в разделе **Выполнение программ** следует задать необходимые параметры для выполнения этой программы. Если выбрана опция перезапуска службы, надо указать время задержки, после которой выполнять перезапуск. Обычно после остановки службы Windows 8 ожидает в течение определенного периода времени, прежде чем выполнять перезапуск службы. В большинстве случаев задержка в 1—2 минуты будет достаточной.

Отключение ненужных служб

Одной из обязанностей администратора является обеспечение безопасности компьютера и сети. В этом отношении ненужные службы представляют потенциальную угрозу безопас-

ности. Например, во многих организациях, которые автор проверял на наличие проблем безопасности, на компьютерах пользователей работали такие службы, как служба веб-публикаций, протоколы SMTP и FTP, когда пользователям эти службы были не нужны. К сожалению, эти службы допускают анонимный доступ к компьютеру и при неправильной настройке могут сделать компьютер уязвимым к атаке.

Есть два подхода к решению вопроса ненужных служб. В случае служб, которые были установлены как часть установленных функциональностей, можно удалить эту функциональность, чтобы вместе с ней удалить и ненужную службу. Ненужные службы также можно просто отключить.

Отключение служб выполняется следующим образом:

1. В консоли **Управление компьютером** разверните узел **Службы и приложения** и выберите в нем узел **Службы**.
2. Щелкните правой кнопкой мыши на требуемой службе, а затем в контекстном меню выберите команду **Свойства**.
3. На вкладке **Общие** в раскрывающемся списке **Тип запуска** выберите опцию **Отключена**.

Отключение службы не останавливает работающую службу; это просто предотвращает ее следующий запуск. До того времени угроза для безопасности компьютера продолжает существовать. Для устранения этой угрозы остановите службу, нажав кнопку **Остановить** на вкладке **Общие**, и лишь после этого нажмите кнопку **OK**, чтобы закрыть окно свойств службы.

Управление службами с помощью предпочтений

Кроме управления службами на отдельных компьютерах, посредством элементов предпочтений групповой политики службы можно настраивать на нескольких компьютерах, обрабатывающих определенный объект групповой политики. При настройке служб посредством предпочтений большинство параметров имеет значение **Без изменений** (No change), указывающее, что параметр будет изменен только в том случае, если для него будет задано другое значение. Как и при настройке служб отдельных компьютеров, посредством элементов предпочтений групповой политики можно выполнять следующее:

- запускать, останавливать и перезапускать службы;
- задавать тип запуска службы: автоматический, автоматический с задержкой или ручной, либо отключать службу;
- указывать учетную запись для выполнения службой входа в систему;
- задавать опции восстановления после сбоя службы.

Создать элемент предпочтения для управления службой можно следующим образом:

1. В редакторе управления групповыми политиками откройте для редактирования требуемый объект групповой политики. Разверните узел **Конфигурация компьютера\Настройка\Параметры панели управления**.
2. Щелкните правой кнопкой по узлу **Службы**, в контекстном меню выберите команду **Создать**, а во вложенном меню — команду **Служба**. Откроется диалогового окно **Новые свойства службы** (New Service Properties) (рис. 9.10).
3. В поле **Имя службы** введите имя настраиваемой службы. Следует иметь в виду, что имя службы не совпадает с отображаемым названием службы. Если вы не знаете имя службы, нажмите кнопку обзора (кнопка с тремя точками) справа от поля **Имя службы** и вы-

берите требуемую службу из предоставленного списка служб, установленных на компьютере. Но учтите, что некоторые службы, исполняющиеся на данном компьютере, могут быть недоступными на компьютерах пользователей и наоборот.

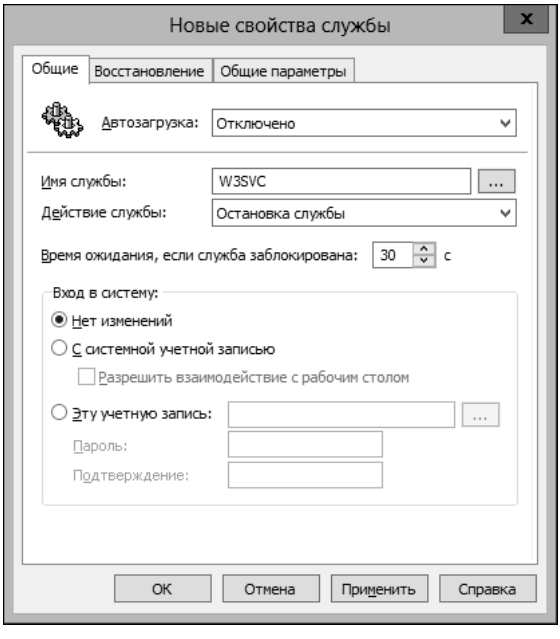


Рис. 9.10. Диалоговое окно для настройки службы посредством элемента предпочтений групповой политики

4. С помощью предоставленных опций окна свойств настройте службу, как она должна быть настроена на компьютерах пользователей. Настройки службы сохраняются только в том случае, если выбрано значение параметра, отличное от значения **Без изменений**.
5. Для управления способом применения настройки предназначены опции на вкладке **Общие параметры**. В большинстве случаев настройку службы требуется применять только один раз. В таких ситуациях нужно установить флажок **Применить один раз и не применять повторно**.
6. Нажмите кнопку **OK**, чтобы сохранить настройки. При следующем обновлении политики элемент предпочтения будет применен должным образом к объекту групповой политики, для которого он был определен.

Основы установки и обслуживания устройств

На компьютеры устанавливаются или подключаются к ним разнообразные устройства. Основными типами подключаемых к компьютерам устройств являются следующие.

- **Платы/адаптеры.** Платы расширения и адаптеры устройств вставляются в слоты расширения на системной плате внутри системного блока или, в случае ноутбуков, во внешние слоты расширения. Большинство плат и адаптеров имеют разъемы для подключения к ним других устройств.
- **Внутренние диски.** На компьютер можно устанавливать внутренние приводы разных типов дисков, таких как DVD-диски и жесткие диски. Внутренние приводы обычно

имеют два кабеля. Один, кабель данных, присоединяется к системной плате, другому приводу или к интерфейсной плате. Другой, кабель питания, подключается к соответствующему разъему блока питания компьютера.

- **Внешние приводы и устройства.** Внешние приводы и устройства подключаются к портам компьютера. Порты могут быть стандартными, например LPT1 или COM1, на плате расширения или последовательными высокоскоростными, например USB, eSATA или IEEE-1394 (FireWire). Принтеры, сканеры, флешки, смартфоны и большинство цифровых камер подключаются к компьютеру как внешние устройства.
- **Память.** Объем физической памяти компьютера расширяется с помощью дополнительных планок памяти. Память можно добавить на материнскую плату или на определенное устройство, например видеоадаптер. Наиболее распространенным видом памяти является оперативная память произвольного доступа (RAM).

В Windows 8 настройка аппаратных устройств выполняется иначе, чем в Windows XP или более ранних версиях Windows. Настройка подключенных к компьютеру устройств, которые не были обнаружены при установке или обновлении операционной системы, выполняется по-иному, чем новых устройств, устанавливаемых пользователем.

Установка подключенных устройств

Windows 8 обнаруживает подключенные устройства, которые не были автоматически установлены при инсталляции или обновлении операционной системы. Во многих случаях, если аппаратное устройство не было установлено из-за того, что Windows 8 не имеет для него драйвера, встроенные средства диагностирования аппаратного оборудования обнаружат это устройство, а затем с помощью инфраструктуры автоматического обновления получат требуемый драйвер при следующем выполнении обновления Windows при условии, что эта функциональность включена и кроме обновления операционной системы также разрешено и обновление драйверов.

Хотя обновления драйверов могут загружаться автоматически с помощью обновления Windows, они не устанавливаются автоматически. После установки или обновлении операционной системы следует проверить наличие обновлений драйверов и применить их должным образом, прежде чем пытаться установить драйверы каким-либо другим способом. Базовая процедура (подробно предмет работы с функциональностью автоматического обновления рассматривается в *главе 10*) для проверки наличия обновлений для драйверов следующая:

1. В Панели управления щелкните по ссылке категории **Система и безопасность** и в открывшемся списке элементов этой категории выберите ссылку **Центр обновления Windows** (Windows Update).
2. В левой панели окна **Центр обновлений Windows** щелкните по ссылке **Поиск обновлений** (Check for updates).

Обычно доступные обновления драйверов отображаются как рекомендуемые обновления, за исключением важных драйверов, таких как для видеоадаптера, звуковой платы или контроллера приводов дисков. Поэтому, чтобы определить наличие обновлений для драйверов устройств, следует просматривать не только важные, но и все доступные для компьютера обновления. Установка доступных обновлений драйверов устройств выполняется следующим образом:

1. В Панели управления щелкните по ссылке категории **Система и безопасность** и в открывшемся списке элементов этой категории выберите ссылку **Центр обновления Windows** (Windows Update).

2. В левой панели окна **Центр обновлений Windows** щелкните по ссылке **Поиск обновлений**. После завершения проверки Windows 8 на наличие обновлений может оказаться, что доступны как важные, так и рекомендуемые обновления (рис. 9.11). Чтобы установить важные обновления, нажмите кнопку **Установить обновления** (Install updates).
3. Так как обновления драйверов обычно считаются необязательными, следует обратить внимание на наличие необязательных обновлений. Если таковые имеются, щелкните по соответствующей ссылке и в открывшемся окне **Выбор обновлений для установки**

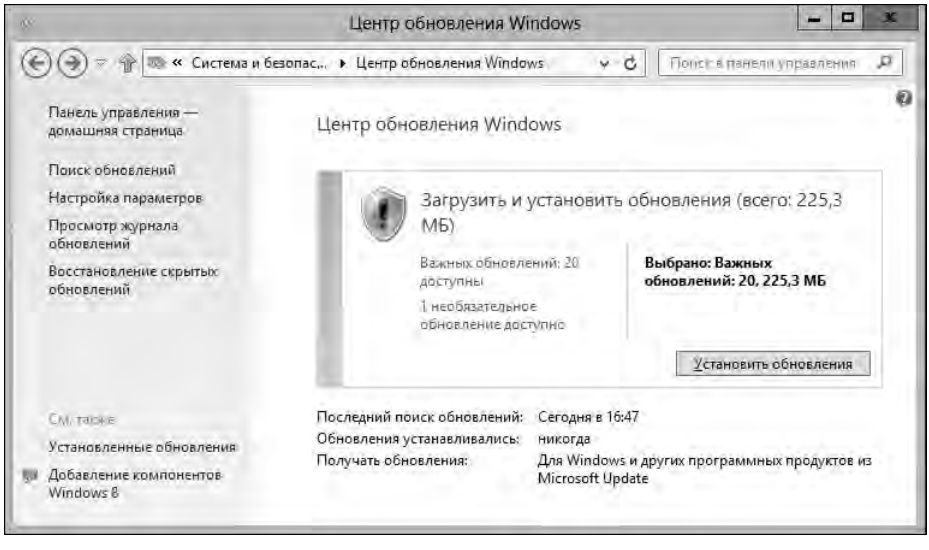


Рис. 9.11. Окно **Центр обновления Windows**

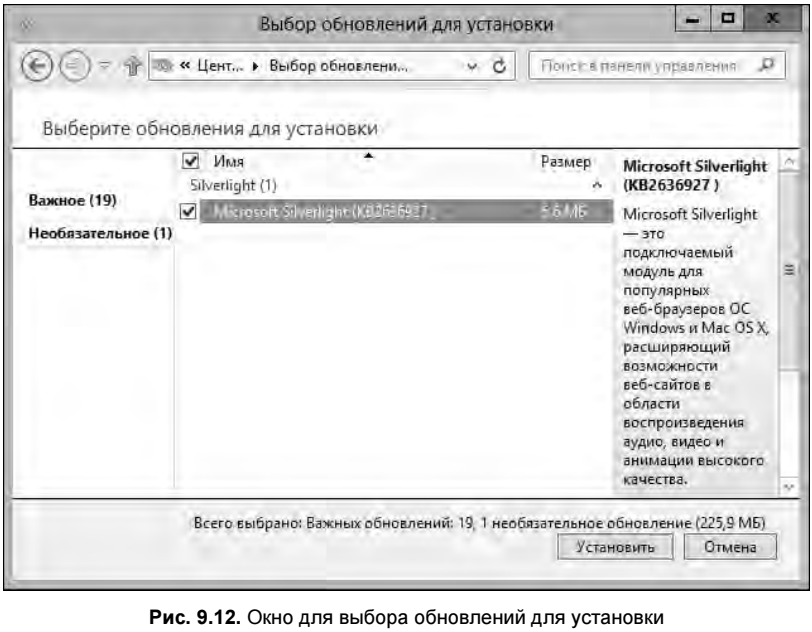


Рис. 9.12. Окно для выбора обновлений для установки

(Select updates to install) просмотрите доступные важные и необязательные обновления (рис. 9.12).

4. По умолчанию все важные обновления выбираются для установки, а необязательные — нет. Чтобы обеспечить установку необязательного обновления, нужно установить его флажок, после чего нажать кнопку **Установить**, чтобы загрузить и установить выбранные обновления.

После установки драйвера устройства Windows 8 должна в течение нескольких минут обнаружить устройство и автоматически установить его. Если ОС обнаруживает устройство, но не может автоматически установить его, можно попытаться найти приемлемое решение в Центре поддержки.

Установка внутренних, USB-, FireWire- и eSATA-устройств

Большинство новых устройств является устройствами Plug and Play (PnP). Это означает, что установку новых устройств можно с легкостью выполнить одним из следующих способов.

- Для внутренних устройств следует ознакомиться с руководством по установке, т. к. для них может быть необходимым установить драйвер перед подключением устройства. Затем нужно выключить компьютер, вставить устройство в соответствующий разъем и снова включить компьютер. Теперь Windows 8 должна автоматически обнаружить новое устройство и установить его.
- Для устройств USB, FireWire или eSATA достаточно просто вставить устройство или его кабель в соответствующий порт и предоставить Windows 8 автоматически обнаружить его.

> ***Примечание***
>
> Windows 8 ожидает, что устройства USB, FireWire и eSATA поддерживают Plug and Play. Если такое устройство не поддерживает Plug and Play, для его установки может быть необходимым использовать программное обеспечение, поставляемое с устройством.

В зависимости от устройства, Windows 8 должна автоматически обнаруживать новое устройство и затем молча установить встроенный драйвер для его поддержки. Уведомления выводятся только в случае каких-либо проблем с установкой, а так процесс незаметно выполняется в фоновом режиме.

После этого устройство должно сразу же работать без каких-либо проблем. По крайней мере такова идея, но процесс не всегда выполняется таким образом. Успех автоматического обнаружения устройства и установки драйверов для него зависит от поддержки данным устройством Plug and Play и от наличия требуемого для него драйвера.

Стандартная установка Windows 8 содержит большое количество драйверов устройств и, как правило, устройство должно установиться автоматически. Если в обновлении Windows разрешено обновление драйверов, Windows 8 автоматически проверяет наличие драйверов при подключении нового устройства или при первом обнаружении устройства. Но так как при обновлении Windows 8 автоматически не устанавливает драйверы устройств, пользователь должен самостоятельно проверить доступные обновления на наличие драйверов для установки.

> ***Примечание***
>
> Подробности по настройке обновления Windows для автоматической проверки наличия драйверов *см. в разд. "Вкладка Оборудование" главы 2*. Также для работы обновления Windows эта функциональность должна быть включена. Подробности *см. в главе 10*.

Индикацией успешной установки устройства служит возможность его использования. Кроме этого, доступность устройства можно проверить в окне **Устройства и принтеры**, которое открывается щелчком по ссылке **Просмотр устройств и принтеров** (View devices and printers) в разделе **Оборудование и звук** (Hardware and Sound) Панели управления.

Хотя Windows 8 может автоматически обнаружить новое устройство, компонент **Установка программного обеспечения драйверов** (Driver Software Installation) может испытывать проблемы с установкой устройства, и тогда установка завершается неудачно без каких-либо уведомлений об этом. Индикацией провалившейся установки устройства служит невозможность его использования. Кроме этого, в окне **Устройства и принтеры** как компьютер, так и неустановленное устройство помечаются значками предупреждения (рис. 9.13).

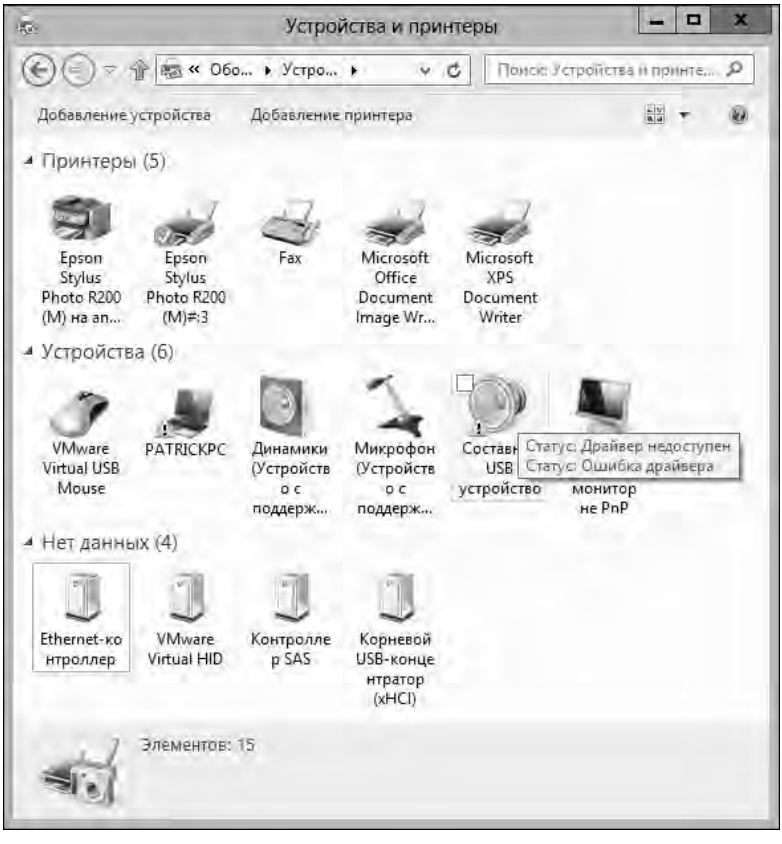


Рис. 9.13. Индикация неустановленных устройств в окне **Устройства и принтеры**

При наведении указателя мыши на устройство, помеченное значком предупреждения, выводится всплывающее сообщение о статусе устройства наподобие следующего:

```
Статус:  Драйвер недоступен
(Status: Driver is unavailable)
Статус:  Ошибка драйвера
(Status: Driver Error)
```

При щелчке на проблемном устройстве его статус также отображается в панели сведений внизу окна **Устройства и принтеры** с дополнительной информацией — **Необходимо устранение неполадок** (Needs troubleshooting).

Таким же образом можно получить сведения о состоянии устройств, которые вы пытаетесь установить. Наведение курсора на проблемное устройство выводит всплывающее сообщение о статусе ошибки, а щелчок по проблемному устройству также отображает его статус в панели сведений внизу окна **Устройства и принтеры**, с дополнительной информацией — **Необходимо устранение неполадок**. Кроме этого, сообщение о статусе ошибки может содержать дополнительные сведения наподобие следующего:

```
Статус: Установка не завершена. Подключитесь к Интернету.
(Status: Setup incomplete. Connect to the Internet.)
```

Чтобы приступить к диагностированию проблемы, щелкните на проблемном устройстве, а затем — по ссылке меню **Устранение неполадок** вверху окна устройств. Запустится мастер устранения неполадок, который будет выводить пошаговые инструкции для устранения проблемы. Наиболее вероятной причиной проблемы с установкой устройства будет то, что следовало загрузить драйвер устройства из Интернета. Если это действительно так, мастер устранения неполадок быстро определит этот факт и выведет запрос на установку драйвера (рис. 9.14).

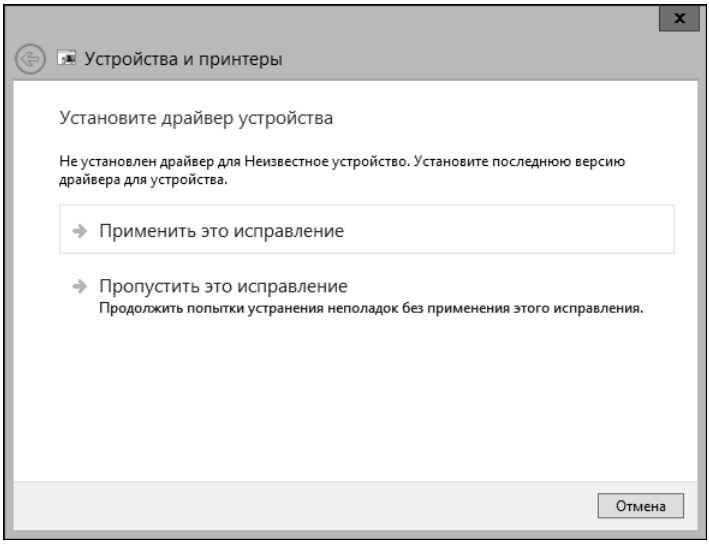


Рис. 9.14. Сообщение о возможном решении проблемы с установкой устройства

Если Windows 8 не обнаружит и, соответственно, не установит устройство, посетите вебсайт производителя устройства, чтобы загрузить последнюю версию драйвера для него. Загрузив необходимый драйвер, запустите его программу установки и следуйте выводимым инструкциям. Теперь устройство должно установиться должным образом.

> ***Примечание***
>
> Если Windows 8 не может установить устройство, это может быть вследствие наличия проблемы с самим устройством или его драйвером либо конфликта с уже установленным оборудованием. Дополнительную информацию по поиску и устранению неполадок *см. в разд. "Поиск и устранение неполадок с оборудованием" далее в этой главе*.

Успешно установив устройство, необходимо периодически выполнять техническое обслуживание как самого устройства, так и его драйвера. Новые драйверы для устройства желательно сначала протестировать в среде разработки или поддержки, чтобы проверить, может

ли новый драйвер исправить проблемы, которые испытывали пользователи. Если новый драйвер устанавливается правильно и решает проблемы пользователей, его можно более уверенно устанавливать на компьютеры в рабочей среде. Обновление драйверов следует выполнять согласно такой процедуре:

1. Прежде чем устанавливать новый драйвер, ознакомьтесь с информацией об устройстве и драйвере на каждой системе. В частности, обратите внимание на размещение, версию и имя файла текущего драйвера.
2. Создайте точку восстановления системы *(см. разд. "Создание резервной копии и восстановление состояния системы, используя средство Восстановление системы" главы 10)*.
3. Установите новый драйвер и, по усмотрению, перезагрузите компьютер. Если после перезагрузки компьютер и устройство функционируют должным образом, обновление драйвера было успешным.
4. Если же после установки обновленного драйвера наблюдаются проблемы в работе системы или устройства, выполните откат драйвера, используя средства, предоставляемые диспетчером устройств. Если откат драйвера нельзя выполнить вследствие отказа системы загружаться, восстановите систему, загрузив последнюю работоспособную конфигурацию системы, а затем осуществите восстановление системы к точке, созданной в шаге 2.

Установка устройств Bluetooth, беспроводных и сетевых устройств

К компьютеру можно подключать большой круг устройств Bluetooth и других беспроводных и сетевых устройств, включая беспроводные сетевые устройства, клавиатуры, мыши, телефоны, устройства хранения данных и медиаприставки. Часто эти устройства имеют свои установочные программы, но прежде чем запускать их, следует удостовериться, что они совместимы с Windows 8. В случае несовместимости следует проверить наличие обновленной программы установки на веб-сайте производителя устройства.

Некоторые устройства подключаются к компьютеру напрямую, а другие через сеть. Подключить устройство Bluetooth или иное беспроводное устройство непосредственно к компьютеру можно следующим образом:

1. Для большинства устройств Bluetooth и других беспроводных устройств к компьютеру необходимо подключить отдельный приемопередатчик. Некоторые устройства могут использовать один общий приемопередатчик. Например, для комплекта беспроводной клавиатуры и мыши применяется один приемопередатчик, который подключается к порту USB компьютера.
2. Приемопередатчик следует разместить таким образом, чтобы соответствующее беспроводное устройство было в радиусе его действия. Например, радиус действия приемопередатчика для беспроводной клавиатуры и мыши составляет около 2 метров, а беспроводного сетевого адаптера — около 30 метров.
3. Настройте устройство должным образом и убедитесь, что оно включено. При установке беспроводного сетевого адаптера его нужно настроить под используемую беспроводную сеть. Кроме этого, некоторые беспроводные сетевые устройства нужно перевести в режим WPS[1], чтобы система могла их обнаружить.

[1] Wireless Protected Setup — защищенная установка беспроводного подключения.

4. Система должна автоматически обнаружить и установить беспроводное устройство. Если этого не происходит, откройте окно **Устройства и принтеры** и проверьте, указано ли устройство в этом окне как доступное. Если устройство еще не указано в окне **Устройства и принтеры**, щелкните по ссылке **Добавить устройство** и следуйте инструкциям мастера добавления устройства.
5. В случае проблем с подключением устройства попробуйте, среди прочего, предпринять следующие действия для поиска и устранения неполадки.
   - Убедитесь, что устройство не выключено, его батарея (если имеется) не разряжена и устройство не находится в режиме сна. Некоторые беспроводные устройства оснащены кнопкой, которую требуется нажать, чтобы установить подключение. Другие, такие, как устройства Bluetooth, могут иметь опцию в программном меню, которую нужно выбрать, чтобы устройство было доступно. Кроме этого, приемопередатчик устройства может иметь кнопку, которую следует нажать, чтобы выполнить сканирование для обнаружения совместимых беспроводных устройств.
   - Если возможность Bluetooth или другого типа беспроводной связи встроена в компьютер, проверьте, что приемопередатчик включен. На многих ноутбуках такие приемопередатчики оснащены выключателем, что позволяет включать их только тогда, когда нужно, в целях экономии заряда батарей.
   - При подозрении, что устройство находится вне радиуса действия своего приемопередатчика, попробуйте расположить его ближе к нему. Если между устройством и компьютером находится стена, попытайтесь разместить их в одной комнате.
   - Если же проблема вызвана местоположением устройства, можно попробовать решить ее перемещением в другое место кабелей и устройств, которые могут создавать электромагнитные помехи, включая кабели питания других устройств, большие динамики и настольные лампы. Если проблему устранить не удается, проверьте, что устройство не расположено вблизи кондиционера, микроволновой печи и т. п.

Подключить проводное или беспроводное сетевое устройство к компьютеру по сети можно следующим образом:

1. Подключите устройство к сети и включите его. Далее настройте параметры устройства для данной сети. Например, может потребоваться настроить параметры протокола TCP/IP, чтобы получать IP-адрес посредством службы DHCP или же использовать статический IP-адрес.
2. Дайте системе достаточное время, до 90 секунд, для обнаружения устройства. Система должна автоматически обнаружить и установить устройство. Если этого не происходит, откройте окно **Устройства и принтеры** и проверьте, указано ли устройство в этом окне как доступное. Если устройство еще не указано в окне **Устройства и принтеры**, щелкните по ссылке **Добавить устройство** и следуйте инструкциям мастера добавления устройства.
3. В случае проблем с подключением устройства попробуйте, среди прочего, предпринять следующие шаги для поиска и устранения неполадки.
   - Проверьте, что устройство не блокируется брандмауэром. Может потребоваться открыть в брандмауэре порт, чтобы разрешить доступ устройства к компьютеру.
   - Проверьте, что устройство настроено и подключено к той же сети, что и компьютер. Если сеть состоит из нескольких подсетей, устройство следует подключить к тому же сегменту сети, что и компьютер. Определить сегмент сети можно по IP-адресу компьютера.

- Проверьте, что устройство настроено на оповещение своего присутствия в сети. Большинство сетевых устройств делают это автоматически.
- Убедитесь, что для сетевого устройства задан правильный IP-адрес, а также другие сетевые параметры. При использовании в сети службы динамического назначения адресов (DHCP) IP-адреса присваиваются устройствам автоматически при их подключении к сети.

Примечание

Не все устройства, которые обнаруживаются системой, можно подключить к компьютеру. Чтобы узнать, можно ли подключить устройство к компьютеру, ознакомьтесь с информацией об устройстве в сопровождающей его документации или на веб-сайте производителя устройства.

Практический совет

Функциональность сетевого обнаружения позволяет компьютеру обнаруживать другие компьютеры и устройства в сети и наоборот. По умолчанию эта функциональность заблокирована брандмауэром Windows, но ее можно включить следующим образом:

1. В Панели управления щелкните по ссылке **Сеть и Интернет**.
2. В следующем окне щелкните по ссылке **Центр управления сетями и общим доступом** (Network and Sharing Center).
3. В левой панели этого окна щелкните по ссылке **Изменить дополнительные параметры общего доступа** (Change advanced sharing settings).
4. В разделе **Сетевое обнаружение** (Network discovery) доменной сети (и других сетей по мере необходимости) установите переключатель **Включить сетевое обнаружение** (Turn on network discovery), а затем нажмите кнопку **Сохранить изменения** (Save changes).

Установка локальных и сетевых принтеров

Подключать к компьютеру принтеры можно разными способами. Какой из этих способов использовать, зависит от конкретного принтера. Некоторые принтеры подключаются непосредственно к компьютеру и называются *локальными принтерами*. Другие принтеры подключаются по сети и называются *сетевыми принтерами*. В число сетевых принтеров входят все принтеры в сети, такие как принтеры, подключенные посредством Bluetooth или другим беспроводным способом, а также принтеры, подключенные к другому компьютеру и являющиеся общим сетевым ресурсом.

Первоначальная конфигурация большинства принтеров выполняется посредством поставляемого вместе с ними установочного программного обеспечения. В случае локального принтера программа установщика выполняется один раз, настраивает принтер и создает на компьютере подключение к нему. А в случае сетевого принтера программа установщика выполняется на сервере принтера, чтобы подготовить принтер к использованию, а затем на каждом компьютере создается сетевое подключение к этому принтеру.

Установка локального принтера

Принтер USB подключается непосредственно к USB-порту компьютера, и Windows автоматически обнаруживает и устанавливает его. Установку принтера с последовательным или параллельным интерфейсом может потребоваться выполнять вручную. Ручная установка принтера осуществляется следующим образом:

1. Включите принтер и проверьте, отображается ли он в окне **Устройства и принтеры** как доступный. Если принтер не отображается, выполните его установку, следуя дальнейшим шагам этой процедуры.

2. В меню окна **Устройства и принтеры** выберите опцию **Добавить принтер**. Запустится мастер добавления принтера, который попытается обнаружить и установить принтер. Если мастер обнаружит требуемый принтер, выберите его в списке обнаруженных принтеров и следуйте дальнейшим инструкциям мастера. Пропустите остальные шаги этой процедуры. Если же мастер не обнаружит требуемый принтер, щелкните по ссылке **Нужный принтер отсутствует в списке** (The printer that I want isn't listed).
3. В следующем окне установите переключатель **Установите локальный или сетевой принтер с параметрами, заданными вручную** (Add a local printer of network printer with manual settings), а затем нажмите кнопку **Далее**.
4. В следующем окне установите переключатель **Использовать существующий пор**т (Use an existing port), выберите в связанном выпадающем списке порт подключения принтера и нажмите кнопку **Далее**.
5. Далее выполните одно из следующих действий.
   - Выберите производителя и модель принтера и нажмите кнопку **Далее**.
   - Если принтер отсутствует в списке, но у вас есть установочный носитель, нажмите кнопку **Установить с диска** (Have disk), а затем укажите папку, в которой находится драйвер принтера. Подробную информацию см. в руководстве по установке принтера.
   - Если у вас нет установочного носителя, нажмите кнопку **Центр обновления Windows** и подождите, пока Windows проверит наличие требуемых драйверов.
6. Выполните остальные шаги мастера установки и нажмите кнопку **Готово**. Проверить работоспособность установленного принтера можно, распечатав пробную страницу.

Локальными принтерами можно управлять посредством предпочтений групповой политики. Но этот подход рекомендуется применять только в тех ситуациях, когда можно точно указать целевые компьютеры, чтобы настройка выполнялась лишь на компьютерах, которые действительно имеют локальные принтеры.

Создать элемент предпочтения для создания, обновления, замены или удаления локальных принтеров можно следующим образом:

1. В редакторе управления групповыми политиками откройте для редактирования требуемый объект групповой политики. Для настройки параметров компьютера разверните узел **Конфигурация компьютера\Настройка\Параметры панели управления** и выберите узел **Принтеры**. Для настройки параметров пользователя разверните узел **Конфигурация пользователя\Настройка\Параметры панели управления** и выберите в нем узел **Принтеры**.
2. Щелкните правой кнопкой мыши по узлу **Принтеры**, в контекстном меню выберите команду **Создать**, а во вложенном меню — команду **Локальный принтер**. Откроется диалоговое окно **Новые свойства локального принтера**.
3. В раскрывающемся списке **Действие** этого окна выберите требуемое действие — **Создать**, **Обновить**, **Заменить** или **Удалить**.
4. В поле **Имя** введите имя принтера. Для создаваемого принтера укажите имя, которое позволит однозначно определить этот принтер. При обновлении, замене или удалении принтера нужно указать имя соответствующего локального принтера.
5. В раскрывающемся списке **Порт** выберите порт подключения локального принтера.
6. В поле **Путь к принтеру** (Printer path) введите путь в формате UNC к общему принтеру такого же самого типа, как и устанавливаемый локальный принтер. Этот элемент будет использован в качестве источника драйвера для устанавливаемого принтера.

7. Для управления способом применения настройки предназначены опции на вкладке **Общие параметры**. Так как мы принудительно используем элемент управления, обычно желательно применять параметры при каждом обновлении групповой политики. В таком случае нужно снять флажок **Применить один раз и не применять повторно**.
8. Нажмите кнопку **OK**. При следующем обновлении политики элемент предпочтения будет применен должным образом к объекту групповой политики, для которого он был определен.

Создать элемент предпочтения для управления общим локальным принтером можно следующим образом:

1. В редакторе управления групповыми политиками откройте для редактирования требуемый объект групповой политики. Разверните узел **Конфигурация пользователя\Настройка\Параметры панели управления** и выберите в нем узел **Принтеры**.
2. Щелкните правой кнопкой мыши по узлу **Принтеры**, в контекстном меню выберите команду **Создать**, а во вложенном меню — команду **Общий принтер** (Shared printer). Откроется диалоговое окно **Новые свойства общего принтера**.
3. В раскрывающемся списке **Действие** этого окна выберите требуемое действие — **Создать**, **Обновить**, **Заменить** или **Удалить**. Если создается элемент предпочтения удаления, можно указать для удаления все подключения общих принтеров, отметив действие **Удалить** и установив флажок **Удалить все подключения общих принтеров** (Delete all shared printer connections).
4. В поле **Путь к общему ресурсу** (Share path) введите путь в формате UNC к общему принтеру. По усмотрению, можно указать локальный порт, на который следует отображать общее подключение. Если выбрано действие **Удалить**, общий принтер, связанный с этим локальным портом, будет удален. Альтернативно, для действия удаления можно выбрать удаление сопоставления всех локальных портов, установив соответствующий флажок.
5. По усмотрению, можно задать использование принтера в качестве принтера по умолчанию. Если создаваемое, обновляемое или заменяемое подключение к общему принтеру должно быть доступным при каждом входе пользователя в систему, нужно установить флажок **Повторное подключение** (Reconnect).
6. Для управления способом применения настройки служат опции на вкладке **Общие параметры**. Так как мы принудительно используем элемент управления, обычно параметры желательно применять при каждом обновлении групповой политики. В таком случае нужно снять флажок **Применить один раз и не применять повторно**.
7. Нажмите кнопку **OK**. При следующем обновлении политики элемент предпочтения будет применен должным образом к объекту групповой политики, для которого он был определен.

Установка Bluetooth-, сетевого или беспроводного принтера

Если принтер подключается посредством Bluetooth или другого беспроводного подключения, компьютер и принтер можно подготовить, как любое подобное устройство. В частности, применяется подход, описанный в *разд. "Установка устройств Bluetooth, беспроводных и сетевых устройств" ранее в этой главе*, с тем исключением, что подключение к принтеру осуществляется таким же образом, как к сетевому принтеру.

Проверьте, что принтер включен и находится в режиме обнаружения. Для этого может потребоваться вручную включить приемопередатчик принтера Bluetooth или другого типа беспроводного подключения. В случае проводного подключения встроенные возможности

динамического выделения IP-адреса могут быть недоступными, и настройку параметров TCP/IP принтера придется выполнять вручную.

Проверьте, отображается ли принтер в окне **Устройства и принтеры** как доступный. Если принтер еще не отображается в этом окне, подключить его можно следующим образом:

1. В меню окна **Устройства и принтеры** выберите опцию **Добавление принтера**. Запустится мастер добавления принтера, который попытается обнаружить и установить принтер. Если мастер найдет требуемый принтер, выберите его в списке обнаруженных принтеров и следуйте дальнейшим инструкциям мастера. Пропустите остальные шаги этой процедуры. Если же мастер не обнаружит требуемый принтер, щелкните по ссылке **Нужный принтер отсутствует в списке**.
2. В мастере добавления принтера установите переключатель **Добавить принтер Bluetooth, беспроводный принтер или принтер с возможностью обнаружения в сети** (Add Bluetooth, wireless or network discoverable printer).
3. Выберите в списке доступных принтеров требуемый принтер и нажмите кнопку **Далее**.
4. Если потребуется, установите драйвер принтера.
5. Выполните остальные шаги мастера установки и нажмите кнопку **Готово**. Проверить работоспособность установленного принтера можно, распечатав пробную страницу.
6. В случае проблем с подключением к принтеру, попробуйте, среди прочего, выполнить следующие действия для поиска и устранения неполадки.
   - Проверьте, что принтер не блокируется брандмауэром. Может потребоваться открыть в брандмауэре порт, чтобы разрешить доступ принтера к компьютеру.
   - Проверьте, что принтер настроен и подключен к той же сети, что и компьютер. Если сеть состоит из нескольких подсетей, принтер следует пытаться подключить к тому же сегменту сети, что и компьютер. Определить сегмент сети можно по IP-адресу компьютера.
   - Проверьте, что принтер настроен на оповещение своего присутствия в сети. Большинство сетевых принтеров делает это автоматически.
   - Убедитесь, что для сетевого принтера задан правильный IP-адрес, а также другие сетевые параметры. При использовании в сети службы динамического назначения адресов (DHCP) IP-адреса присваиваются принтерам автоматически при их подключении к сети.

Сетевыми принтерами можно управлять посредством предпочтений групповой политики. Создать, обновить, заменить или удалить подключение к сетевому принтеру можно следующим образом:

1. В редакторе управления групповыми политиками откройте для редактирования требуемый объект групповой политики. Для настройки предпочтений компьютера разверните узел **Конфигурация компьютера\Настройка\Параметры панели управления** и выберите узел **Принтеры**. Для настройки предпочтений пользователя разверните узел **Конфигурация пользователя\Настройка\Параметры панели управления** и выберите в нем узел **Принтеры**.
2. Щелкните правой кнопкой мыши по узлу **Принтеры**, в контекстном меню выберите команду **Создать**, а во вложенном меню — команду **TCP/IP-принтер**. Откроется диалоговое окно **Новые свойства TCP/IP-принтера**.
3. В раскрывающемся списке **Действие** этого окна выберите требуемое действие — **Создать**, **Обновить**, **Заменить** или **Удалить**.

4. Далее выполните одно из следующих действий:
   - если к принтеру требуется подключаться по его IP-адресу, введите IP-адрес принтера в поле **IP-адрес**;
   - если к принтеру требуется подключаться по его DNS-имени, установите флажок **Использовать DNS-имя** и введите в поле **DNS-имя** полное доменное имя принтера.
5. В поле **Локальное имя** введите локальное имя принтера. Если создается подключение к принтеру, на компьютерах пользователей принтер будет отображаться под этим именем. При обновлении, замене или удалении подключения к принтеру нужно указать имя соответствующего принтера.
6. В поле **Путь к принтеру** (Printer path) введите путь в формате UNC к общему принтеру такого же типа, как и настраиваемый сетевой принтер. Этот элемент будет использован в качестве источника драйвера для устанавливаемого принтера.
7. По усмотрению, можно задать использование принтера в качестве принтера по умолчанию.
8. На вкладке **Параметры порта** (Порт settings) укажите протокол, номер порта и другие параметры принтера.
9. Для управления способом применения настройки предназначены опции на вкладке **Общие параметры**. Так как мы принудительно используем элемент управления, обычно параметры желательно применять при каждом обновлении групповой политики. В таком случае нужно снять флажок **Применить один раз и не применять повторно.**
10. Нажмите кнопку **OK**. При следующем обновлении политики элемент предпочтения будет применен должным образом к объекту групповой политики, для которого он был определен.

Знакомство с диспетчером устройств

Утилита **Диспетчер устройств** применяется для просмотра и настройки аппаратных устройств компьютера. Так как это одна из наиболее часто применяемых для управления компьютеров утилит, следует знать, как пользоваться ею должным образом.

Открыть окно диспетчера устройств, содержащее подробный список всех аппаратных устройств системы, можно следующим способом:

1. В Панели управления щелкните по ссылке **Система и безопасность**, в следующем окне — по ссылке **Администрирование**, а далее — дважды по значку **Управление компьютером**.

   Примечание

   Для работы с удаленным компьютером нажмите или щелкните правой кнопкой мыши по узлу **Управление компьютером** в дереве консоли и в контекстном меню выберите команду **Подключиться к другому компьютеру**. В диалоговом окне **Выбор компьютера** установите переключатель **другим компьютером** и введите полное имя требуемого компьютера. Альтернативно, можно выполнить поиск необходимого компьютера, нажав кнопку **Обзор**. Задав требуемый компьютер, нажмите кнопку **OK**.

2. В консоли **Управление компьютером** разверните узел **Служебные программы** (System Tools) и выберите в нем узел **Диспетчер устройств**. В панели сведений консоли отобразится полный список установленных на компьютере аппаратных устройств

(рис. 9.15). По умолчанию этот список упорядочен в алфавитном порядке по типу устройства. Опции команды **Вид** меню консоли позволяют упорядочить устройства по подключению, а ресурсы — по типу или подключению.

3. Развернув тип устройства, можно просмотреть список конкретных экземпляров устройств этого типа и выбрать требуемое из них для работы.

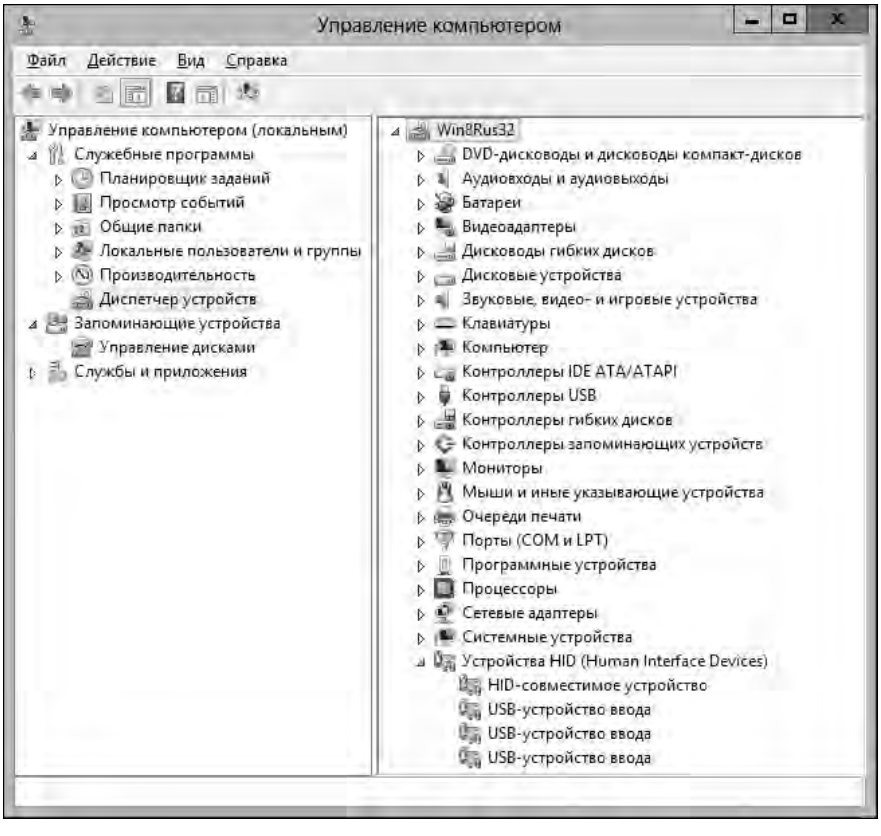


Рис. 9.15. Оснастка **Диспетчер устройств** консоли **Управление компьютером**

Для работы с любым из устройств, отображаемых в диспетчере устройств, щелкните по нему правой кнопкой мыши, чтобы открыть его контекстное меню. Опции контекстного меню зависят от типа устройства, но обычно содержат следующие:

- **Свойства** (Properties) — открывает окно свойств устройства;
- **Удалить** (Uninstall) — удаляет устройство и его драйверы;
- **Отключить** (Disable) — отключает устройство, но не удаляет его;
- **Задействовать** (Enable) — включает отключенное устройство;
- **Обновить драйверы** (Update Driver Software) — запускает мастер обновления оборудования (Hardware Update Wizard) для обновления драйвера устройства;
- **Обновить конфигурацию оборудования** (Scan For Hardware Changes) — указывает Windows 8 выполнить сканирование установленного оборудования на предмет изменения конфигурации.

Совет

Проблемные устройства в списке обозначаются предупреждающими значками. Значок желтого цвета с изображением восклицательного знака означает общую проблему с устройством. Значок красного цвета с изображением × означает, что устройство установлено неправильно. А круглый значок белого цвета с изображением стрелки вниз обозначает отключенное устройство.

Посредством опций меню **Вид** консоли **Управление компьютером** можно изменить настройки по умолчанию для отображения устройств. Доступны следующие опции.

- **Устройства по типу** (Devices by type). Список упорядочен по типу устройств, например, дисковые приводы и принтеры. Конкретные экземпляры устройств перечислены под названием типа. Этот вид применяется по умолчанию.
- **Устройства по подключению** (Devices by connection). Устройства в списке упорядочены по типу подключения, например, устройства, подключенные к шине PCI.
- **Ресурсы по типу** (Resources by type). Устройства отображаются упорядоченными по типу используемых ими ресурсов: ввод-вывод, запрос на прерывание (IRQ), память и прямой доступ к памяти (DMA).
- **Ресурсы по подключению** (Resources by connection). Отображается статус выделенных ресурсов по типу подключения устройства. С помощью этого вида можно, например, проследить ресурсы по их подключению к шине PCI, корневым портам и т. п.
- **Показать скрытые устройства** (Show Hidden Devices). К стандартным представлениям добавляются скрытые устройства, включая не-PnP-устройства, а также устройства, которые были физически отсоединены от компьютера, но чьи драйверы не были удалены.

Работа с драйверами устройств

Для каждого установленного на компьютере аппаратного устройства в системе установлен соответствующий драйвер. Задача драйвера устройства заключается в описании способа использования операционной системой уровня HAL[1] для работы с компонентом оборудования. Уровень HAL выполняет низкоуровневые задачи взаимодействия между операционной системой и компонентом оборудования. Установка аппаратного компонента посредством операционной системы сообщает ей об используемом компонентом драйвере, после чего драйвер этого устройства загружается автоматически и выполняется, как часть операционной системы.

Основы драйверов устройств

В состав Windows 8 входит обширная библиотека драйверов устройств. В базовой установке операционной системы эти драйверы содержатся в папке FileRepository в хранилище драйверов. Некоторые пакеты обновлений также содержат обновления хранилища драйверов. На 32-разрядных компьютерах хранилище 32-разрядных драйверов находится в папке *%SystemRoot%*\ System32\DriverStore. На 64-разрядных компьютерах хранилище 64-разрядных драйверов находится в папке *%SystemRoot%*\System32\DriverStore, а 32-разрядных — в папке *%SystemRoot%*\SysWOW64\DriverStore. Папка DriverStore также содержит вложенные папки, в которых хранится локализованная информация для драйверов. Для каждого установленного на системе языка имеется своя папка. Например, информация о русской локализации драйверов хранится в папке ru-RU.

[1] Hardware Abstraction Layer — уровень абстрагирования от аппаратных средств.

Каждый драйвер устройства в хранилище драйверов сертифицирован на полную совместимость с Windows 8 и подписан цифровой подписью Microsoft, чтобы предоставить операционной системе доказательство его подлинности. При установке нового PnP-устройства Windows 8 проверяет хранилище драйверов на наличие совместимого драйвера устройства. Если такой драйвер имеется, операционная система автоматически устанавливает устройство.

Каждый драйвер устройства имеет соответствующий файл с информацией по установке. Этот файл имеет расширение inf и представляет собой текстовый файл, содержащий подробную информацию по установке устройства и исходные файлы драйвера. Исходные файлы драйвера имеют расширение sys. Папка драйвера может содержать файлы pnf и dll, а также файлы манифеста связанных компонентов с расширением amx. Файл манифеста имеет формат XML, содержит сведения о цифровой подписи драйвера и может включать информацию по Plug and Play, которую устройство использует, чтобы выполнить автоматическую самонастройку.

Каждый установленный в системе драйвер имеет исходный файл (с расширением sys) в папке Drivers. При установке драйвера нового устройства драйвер записывается в соответствующую подпапку папки Drivers, а в реестре сохраняются параметры настройки. Для управления установкой драйвера и записи параметров в реестр используется inf-файл драйвера. Если драйвера еще нет в хранилище драйверов, для него в системе нет и файла inf и других связанных файлов. В таком случае inf-файл и другие связанные файлы драйвера записываются в соответствующую подпапку папки DriverStor\FileRepository при установке устройства.

Подписанные и неподписанные драйверы

Каждый драйвер устройства в хранилище драйверов снабжается цифровой подписью, которая указывает, что драйвер был всесторонне протестирован в лабораториях WHQL[1]. Драйвер с цифровой подписью Microsoft не должен вызывать сбоев или нестабильной работы системы. Наличие цифровой подписи Microsoft также удостоверяет, что целостность драйвера устройства не была нарушена. Отсутствие у драйвера устройства цифровой подписи Microsoft означает, что для него не было выполнено тестирование для одобрения его пригодности либо после исходной установки его файлы были модифицированы другой программой. Это означает, что неподписанные драйверы могут вызвать зависание программ или сбой системы с намного большей вероятностью, чем другое установленное программное обеспечение.

Чтобы предотвратить проблемы с неподписанными драйверами, Windows 8 по умолчанию выводит предупреждение при попытке установить неподписанный драйвер устройства. Windows можно также настроить, чтобы предотвратить установку определенных типов устройств. Управлять параметрами драйверов устройств на всех компьютерах организации можно с помощью групповой политики, указывая, разрешено ли устанавливать устройства и каким образом выполнять установку.

Установку устройств можно настраивать для отдельных компьютеров, используя параметры политики **Установка устройства**, которая находится в узле **Конфигурация компьютера\Административные шаблоны\Система**.

> ***Совет***
>
> Причиной невозможности установки устройства могут быть ограничения на установку, наложенные в групповой политике. В таком случае, чтобы установить устройство, нужно отменить связанные параметры групповой политики.

[1] Microsoft Windows Hardware Quality Labs — лаборатории тестирования качества оборудования Windows.

Отслеживание информации о драйверах

Каждый установленный в системе драйвер имеет связанный с ним файл драйвера. Просмотреть размещение файла драйвера устройства и связанные сведения можно следующим образом:

1. Откройте консоль **Управление компьютером** и разверните в ней узел **Служебные программы**.
2. Выберите узел **Диспетчер устройств**. Этот узел содержит список всех установленных на компьютере устройств, упорядоченный по типу устройства.
3. Щелкните правой кнопкой мыши на требуемом устройстве, а затем в контекстном меню выберите команду **Свойства**. Откроется диалоговое окно свойств устройства.
4. На вкладке **Драйвер** этого окна нажмите кнопку **Сведения**. Откроется диалоговое окно **Сведения о файлах драйверов** (Driver File Details) (рис. 9.16).

   Это окно содержит следующую информацию о драйвере:

   - **Файлы драйвера** (Driver Files) — список путей к папкам, содержащим файлы драйвера;
   - **Поставщик** (Provider) — создатель драйвера;
   - **Версия файла** (File Version) — версия файла драйвера.

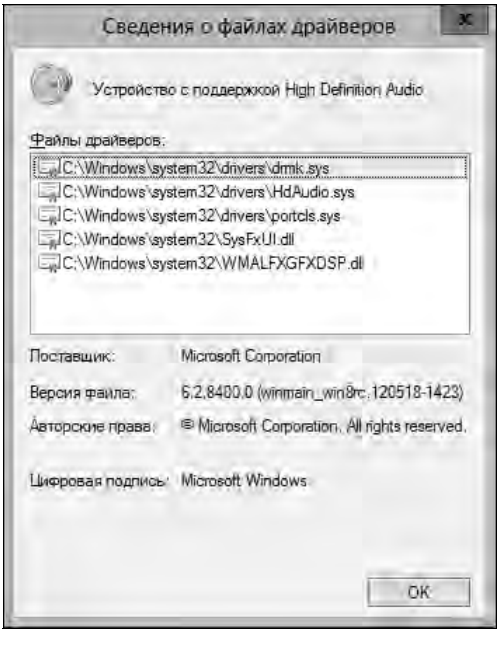


Рис. 9.16. Окно сведений о драйвере

Установка и обновление драйверов устройств

Чтобы обеспечить надежную работу устройства, важно содержать его драйверы в актуальном состоянии. Драйверы устройств устанавливаются посредством мастеров обнаружения нового оборудования (Found New Hardware), добавления оборудования (Add Hardware) и обновления драйверов (Update Driver Software).

По умолчанию эти мастера могут выполнять поиск обновленных драйверов устройств в следующих местах:

- локальный компьютер;
- установочный диск устройства;
- веб-сайт обновления Windows или сервер обновления Windows организации.

В групповой политике для управления получением информации об устройствах и поиском драйверов Windows используются следующие параметры политики.

- **Отключить доступ ко всем компонентам Центра обновления Windows** (Turn off access to all Windows Update features). Находится в узле редактора локальной групповой политики **Конфигурация компьютера\Административные шаблоны\Система\Управление связью через Интернет\Параметры связи через Интернет**.

  Включение этого параметра блокирует все функциональности Центра обновления Windows, делая их недоступными пользователям. Доступ пользователей к веб-сайту Центра обновления Windows будет запрещен.

- **Отключить поиск драйверов устройств в Центре обновления Windows** (Turn off Windows Update device driver searching). Находится в узле редактора локальной групповой политики **Конфигурация компьютера\Административные шаблоны\Система\Управление связью через Интернет\Параметры связи через Интернет**.

  По умолчанию поиск в Центре обновления Windows при установке устройств не является обязательным. При включении этого параметра поиск в Центре обновления Windows при установке устройства не будет выполняться. При выключенном параметре, если при установке нового устройства локальные драйверы отсутствуют, всегда выполняется поиск драйверов в Центре обновления Windows.

- **Задать порядок поиска в исходных расположениях драйверов устройств** (Specify search order for device driver source location). Находится в узле редактора локальной групповой политики **Конфигурация компьютера\Административные шаблоны\Система\Установка устройства**.

  Если этот параметр не включен или не задан, для каждого компьютера можно задать порядок поиска драйверов устройств в исходных расположениях. При включенном параметре можно указать, что при поиске драйвера в процессе установки устройства поиск в Центре обновления Windows следует выполнять первым, последним или вообще не выполнять.

- **Настроить время ожидания установки устройства** (Configure device installation timeout). Находится в узле редактора локальной групповой политики **Конфигурация компьютера\Административные шаблоны\Система\Установка устройства**.

  Если этот параметр отключен или не задан, Windows 8 ожидает окончания установки устройства в течение 5 минут, прежде чем принудительно завершить процесс установки. При включенном параметре можно задать период времени для установки устройства, прежде чем принудительно завершать процесс установки.

- **Запретить получение метаданных устройства из Интернета** (Prevent device metadata retrieval from the Internet). Находится в узле редактора локальной групповой политики **Конфигурация компьютера\Административные шаблоны\Система\Установка устройства**.

  Если этот параметр отключен или не задан, Windows 8 получает из Интернета метаданные для установленных устройств и использует эту информацию для содержания уст-

ройств в актуальном состоянии. При включенном параметре Windows 8 не получает из Интернета метаданные для установленных устройств.

Установка и обновление драйверов выполняется следующим образом:

1. Откройте консоль **Управление компьютером** и разверните в ней узел **Служебные программы**.
2. Выберите узел **Диспетчер устройств**. В панели сведений консоли должен отобразиться список всех установленных на компьютере устройств, упорядоченный по типу устройства.
3. Щелкните правой кнопкой мыши на требуемом устройстве, а затем в контекстном меню выберите команду **Обновить драйверы** (Update Driver Software). Запустится мастер обновления драйверов (рис. 9.17).

Рекомендации

Обновленный драйвер может расширить функциональность устройства, улучшить его производительность и разрешить конфликты устройств в системе. Но последние версии драйверов не следует устанавливать на пользовательские компьютеры, предварительно не проверив их в тестовой среде. Если драйвер работает без проблем в тестовой среде, тогда его можно с уверенностью устанавливать и на компьютеры пользователей.

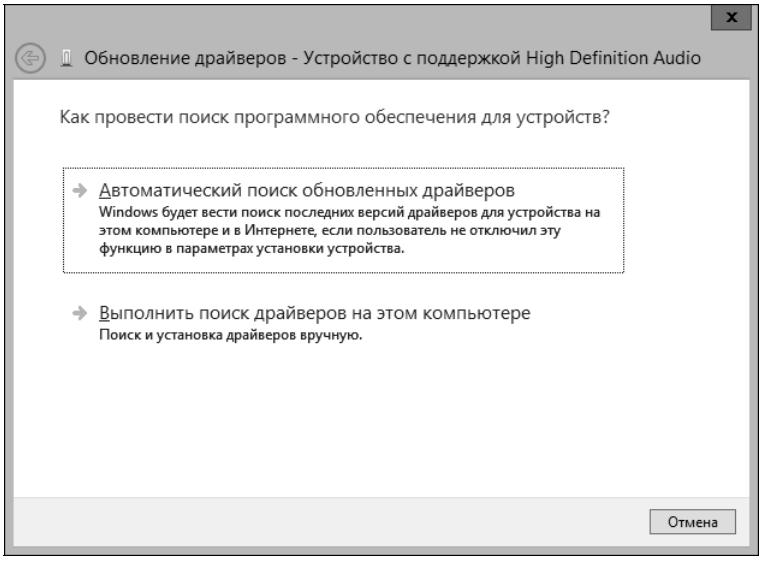


Рис. 9.17. Выбор метода поиска драйвера

4. В начальном окне мастера можно указать способ поиска обновленного драйвера — автоматически или вручную на локальном компьютере.
5. При выборе автоматического поиска Windows 8 пытается автоматически найти более новую версию драйвера и при успешном поиске устанавливает его. В противном случае оставляется старый драйвер. В любом случае, по завершению процесса нажмите кнопку **Закрыть** и пропустите последующие шаги.
6. При выборе ручного поиска возможны следующие варианты действий.
   - **Выполнить поиск драйвера на данном компьютере.** (Tap or click Browse My Computer For Driver Software to select a search location). В следующем окне нажмите

кнопку **Обзор** и с помощью открывшегося окна **Обзор папок** (Browse For Folder) укажите папку, в которой следует искать новый драйвер, после чего нажмите кнопку **OK**. Установка флажка **Включая вложенные папки** (Include subfolders) может повысить шансы найти новый драйвер. При установке этого флажка поиск выполняется во всех вложенных папках указанной папки, поэтому, указав вместо папки диск, можно выполнить поиск по всему этому диску.

- **Выбрать драйвер для установки.** В следующем окне щелкните на опции **Выбрать драйвер из списка уже установленных драйверов** (Let me pick from the list of device drivers on my computer). Откроется страница мастера со списком совместимых устройств. Выберите в этом списке устройство, соответствующее вашему устройству. Чтобы просмотреть список всех возможных устройств, сбросьте флажок **Только совместимые устройства** (Show compatible hardware). Таким образом будет предоставлен список всех производителей типа устройства, для которого выполняется поиск драйверов (рис. 9.18). Выберите в первом списке производителя устройства, а потом во втором списке модель устройства.

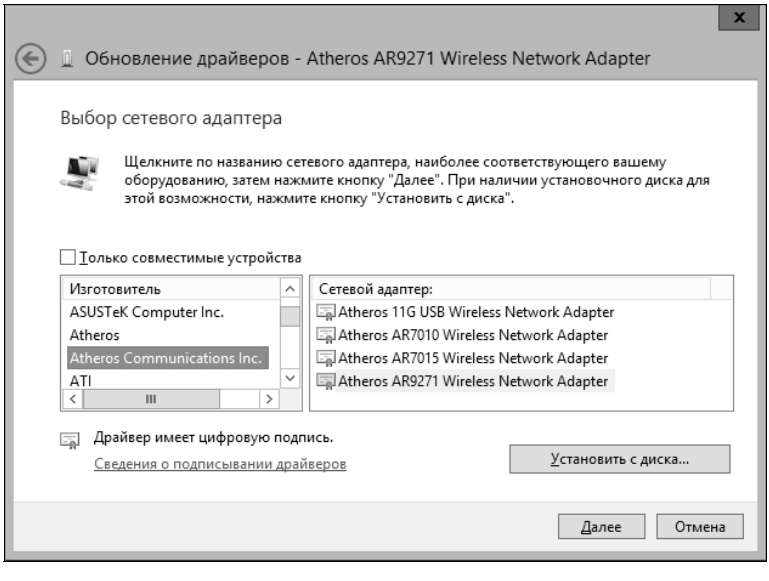


Рис. 9.18. Выбор производителя и типа устройства в процессе поиска обновленного драйвера для устройства

Примечание

Если списки не содержат производителя или правильной модели устройства и у вас есть установочный диск для него, вставьте диск в привод и нажмите кнопку **Установить с диска** (Have Disk). Далее следуйте выводимым инструкциям.

7. Выбрав посредством автоматического или ручного поиска требуемый драйвер, продолжите процесс установки, нажав кнопку **Далее**. По завершению операции установки драйвера нажмите кнопку **Закрыть**. Если мастер не может найти требуемый драйвер, необходимо раздобыть таковой и повторить процедуру установки. Следует иметь в виду, что в некоторых случаях, чтобы активировать новоустановленный драйвер, необходимо перезагрузить систему.

Включение и отключение типов устройств

С помощью предпочтений групповой политики можно управлять тем, какие аппаратные устройства следует использовать на компьютерах, на которые распространяется действие объекта групповой политики. Управление устройствами осуществляется путем включения и отключения их согласно следующим характеристикам:

- *класс устройства* — охватывает широкий диапазон подобных устройств, например, все DVD-приводы;
- *тип устройства* — обозначает конкретное устройство в классе устройств, например, устройство NEC DVD-ROM RW ND-3530A ATA.

> ***Примечание***
>
> Чтобы управлять устройствами по их типу, нужно оснастить компьютер управления устройствами, с которыми планируется работать, а затем создать на этом компьютере элементы предпочтения. *Компьютер управления* представляет собой компьютер, на котором установлены средства управления, включая средства RSAT.

Элемент предпочтения для включения или отключения устройств по классу или типу создается следующим образом:

1. В редакторе управления групповыми политиками откройте для редактирования требуемый объект групповой политики. Для настройки предпочтений компьютера разверните узел **Конфигурация компьютера\Настройка\Параметры панели управления** и выберите узел **Устройства**. Для настройки предпочтений пользователя разверните узел **Конфигурация пользователя\Настройка\Параметры панели управления** и выберите в нем узел **Устройства**.
2. Щелкните правой кнопкой мыши по узлу **Устройства**, в контекстном меню выберите команду **Создать**, а во вложенном меню — команду **Устройство**. Откроется диалоговое окно **Новые свойства устройства** (New Device Properties).
3. В списке **Действие** этого окна выберите одну из следующих опций:
   - **Использовать это устройство (включить)** (Use this device (enable)) — включение устройств по классу или типу;
   - **Не использовать это устройство (выключить)** (Do not use this device (disable)) — выключение устройства по классу или типу.
4. Нажмите кнопку обзора справа от поля **Класс устройства** (кнопка с тремя точками) и в открывшемся окне со списком устройств выполните одно из следующих действий:
   - выберите класс устройств для управления устройствами по классу;
   - разверните узел класса устройств и выберите в нем тип устройства для управления устройствами по типу устройства.
5. Для управления способом применения настройки служат опции на вкладке **Общие параметры**. Так как мы принудительно используем элемент управления, обычно параметры желательно применять при каждом обновлении групповой политики. В таком случае нужно снять флажок **Применить один раз и не применять повторно**.
6. Нажмите кнопку **OK**. При следующем обновлении политики элемент предпочтения будет применен должным образом к объекту групповой политики, для которого он был определен.

Использование групповой политики для ограничения установки устройств

Кроме подписания кода и ограничения поиска, с помощью параметров групповой политики можно разрешать или запрещать установку устройств на основе класса устройства. Устройства, одинаково установленные и настроенные, группируются в класс установки устройств. Каждому классу установки устройств присваивается идентификатор GUID. Для ограничения устройств посредством групповой политики необходимо знать идентификатор GUID для класса установки устройств, который требуется ограничить.

В узле реестра `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Class` имеется раздел для каждого класса установки устройств. Эти разделы реестра именуются согласно идентификатору GUID класса. Значение параметра `Class` раздела реестра для определенного идентификатора GUID указывает класс установки устройств, который определяется данным идентификатором GUID. Например, если выбрать раздел реестра `{4d36e965-e325-11ce-bfc1-08002be10318}`, можно увидеть, что это класс установки устройств для приводов CD-ROM.

Параметры политики для управления установкой устройств расположены в узле редактора локальной групповой политики **Конфигурация компьютера\Административные шаблоны\Система\Установка устройства\Ограничения на установку устройств** (Computer Configuration\Administrative Templates\System\Device Installation\Device Installation Restrictions) и включают, среди прочих, следующие:

- **Разрешить администраторам заменять политики ограничения установки устройств** (Allow administrators to override Device Installation Restriction policies);
- **Разрешить установку устройств, соответствующих какому-либо из этих кодов устройств** (Allow installation of devices that match any of these device IDs);
- **Разрешить установку устройств с использованием драйверов, соответствующих этим классам установки устройств** (Allow installation of devices using drivers that match these device setup classes);
- **Запретить установку устройств, не описанных другими параметрами политики** (Prevent installation of devices not described by other policy settings);
- **Запретить установку устройств с указанными кодами устройств** (Prevent installation of devices that match any of these device IDs);
- **Запретить установку съемных устройств** (Prevent installation of removable devices);
- **Время (в секундах) до принудительной перезагрузки при необходимости введения параметров политики в действие** (Time (in seconds) to force reboot when required for policy changes to take effect).

Настройка этих параметров осуществляется следующим образом:

1. В редакторе управления групповыми политиками откройте для редактирования требуемый объект групповой политики.
2. Разверните узел **Конфигурация компьютера\Административные шаблоны\Система\Установка устройства\Ограничения на установку устройств**.
3. Откройте диалоговое окно свойств требуемого параметра политики, дважды щелкнув по нему мышью.
4. Установите переключатель **Не задано**, чтобы не применять параметр, **Включить**, чтобы применить, или **Отключить**, чтобы заблокировать применение параметра (все установки в зависимости от разрешений настройки групповой политики).

5. При настройке параметра, который имеет опцию **Показать**, нажмите кнопку **Показать** и в диалоговом окне **Вывод содержания** (Show Contents) укажите код устройства, которое нужно сопоставить этой политике. В редакторе реестра идентификатором GUID для класса установки устройств является все имя раздела, включая открывающие и закрывающие круглые и фигурные скобки — `{{` и `}}`. Имя раздела реестра можно скопировать и вставить в диалоговое окно **Вывод содержания** следующим способом.
   а) Откройте редактор реестра. Это можно сделать, нажав клавишу <Windows> и выполнив команду `regedit` в поле поиска панели **Приложения**. Но этот метод работает, только если это поле имеет фокус. Тогда можно выполнить эту команду в консоли командной строки.
   б) В редакторе реестра щелкните правой кнопкой мыши на требуемом разделе и в контекстном меню выберите команду **Копировать имя раздела** (Copy Key Name).
   в) В диалоговом окне **Вывод содержания** дважды щелкните по полю **Значение**, чтобы поместить в него курсор для вставки. Щелкните правой кнопкой мыши в этом поле и в контекстном меню выберите команду **Вставить**.
   г) Во вставленном значении удалите всю часть, предшествующую части идентификатора GUID. В частности, удалить нужно `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Class\`.
   д) Чтобы добавить идентификатор GUID для другого класса установки устройств, повторите шаги *б—г*.
6. Нажмите кнопку **OK**.

Откат драйверов

Иногда может случиться, что установленный новый драйвер вызывает проблемы в работе соответствующего устройства или даже всей системы. В таком случае можно выполнить откат драйвера устройства до прежней его версии. Процедура для этого следующая:

1. В случае проблем с запуском системы загрузите компьютер в безопасном режиме *(см. разд. "Поиск и устранение неполадок запуска и завершения работы" главы 10)*.
2. Откройте консоль **Управление компьютером** и разверните в ней узел **Служебные программы**.
3. Выберите узел **Диспетчер устройств**. В панели сведений консоли должен отобразиться список всех установленных на компьютере устройств, упорядоченный по типу устройства.
4. Щелкните правой кнопкой мыши на требуемом устройстве, а затем в контекстном меню выберите команду **Свойства**. Откроется диалоговое окно свойств устройства.
5. В этом окне выберите вкладку **Драйвер** и нажмите на ней кнопку **Откатить** (Roll Back Driver). При выводе запроса подтвердить откат драйвера нажмите кнопку **Да**.
6. Нажмите кнопку **OK**, чтобы закрыть окно свойств устройства.

> ***Примечание***
>
> Если драйвер не обновлялся, то и выполнять откат будет нечего. В таком случае кнопка **Откатить** будет неактивной.

Удаление драйверов удаленных устройств

Обычно Windows 8 обнаруживает удаление устройства из системы и автоматически удаляет драйверы для этого устройства. Но иногда Windows 8 не замечает удаление устройства, и тогда его драйверы нужно удалить вручную. Процедура для ручного удаления драйверов устройства следующая:

1. Откройте консоль **Управление компьютером** и разверните в ней узел **Служебные программы**.
2. Выберите узел **Диспетчер устройств**.
3. Щелкните правой кнопкой мыши на устройстве, которое нужно удалить, а затем в контекстном меню выберите команду **Удалить**.
4. При выводе запроса подтвердить удаление устройства нажмите кнопку **OK**.

Удаление, обновление и отключение драйверов устройств

Удаление драйвера устройства обычно также удаляет и соответствующее устройство. Иногда проблему с работой устройства можно решить, полностью удалив его, перезапустив систему, а затем повторно установив драйвер устройства. Процедура для удаления и повторной установки драйвера следующая:

1. Откройте консоль **Управление компьютером** и разверните в ней узел **Служебные программы**.
2. Выберите в нем узел **Диспетчер устройств**. В панели сведений консоли должен отобразиться список всех установленных на компьютере устройств, упорядоченный по типу устройства.
3. Щелкните правой кнопкой мыши на требуемом устройстве, а затем в контекстном меню выберите команду **Удалить**.
4. При выводе запроса подтвердить удаление устройства нажмите кнопку **OK**.
5. Перезагрузите систему. Windows 8 должна обнаружить устройство и автоматически установить требуемый для него драйвер. Если по какой-либо причине автоматическая установка драйвера не происходит, выполните ее вручную, как рассматривается в *разд. "Установка и обновление драйверов устройств" ранее в этой главе.*

Если по какой-либо причине устройство требуется сделать недоступным, но чтобы система автоматически не переустанавливала его, вместо удаления устройство следует отключить. Для этого нужно в диспетчере устройств щелкнуть на требуемом устройстве правой кнопкой мыши и в контекстном меню выбрать команду **Отключить** (Disable).

Включение и отключение аппаратных устройств

Когда устройство не работает должным образом, может понадобиться удалить или отключить его. Удаление устройства заключается в удалении его драйвера, вследствие чего временно кажется, что устройство было удалено из системы. Но при следующем запуске системы Windows 8 может попытаться автоматически переустановить удаленное устройство. Обычно Windows 8 автоматически переустанавливает устройства, поддерживающие технологию Plug and Play.

Отключение устройства делает его недоступным системе и предотвращает его использование Windows 8. Так как отключенное устройство не использует системные ресурсы, можно быть уверенным, что оно не вызывает никаких конфликтов в системе.

Удалить и отключить устройство можно следующим образом:

1. Откройте консоль **Управление компьютером** и разверните в ней узел **Служебные программы**.
2. Выберите в нем узел **Диспетчер устройств**. В панели сведений консоли должен отобразиться список всех установленных на компьютере устройств, упорядоченный по типу устройства.
3. Щелкните правой кнопкой мыши на требуемом устройстве и в контекстном меню выберите **Удалить** или **Отключить**.
4. При выводе запроса подтвердить действие нажмите, в зависимости от действия, кнопку **Да** или **OK**.

Поиск и устранение неполадок с оборудованием

Встроенная в Windows 8 функциональность диагностирования оборудования может обнаруживать многие типы проблем с аппаратными устройствами. Система может уведомлять об обнаружении проблемы всплывающим сообщением, щелчок по которому открывает Центр поддержки. Центр поддержки также можно открыть из Панели управления, щелкнув по ссылке **Система и безопасность**, а затем по ссылке **Центр поддержки**.

Устройство, которое было неправильно установлено или испытывает проблемы по какой-либо другой причине, обозначается в диспетчере устройств предупреждающим значком. Двойной щелчок по проблемному устройству в списке диспетчера устройств открывает окно свойств устройства с отображением кода ошибки на вкладке **Общие** в поле **Состояние устройства**. Код ошибки может быть полезным при выяснении причины проблемы с устройством и ее устранении. В табл. 9.3 приведен список кодов ошибок устройств и рекомендуемые действия по их решению. В случае большинства корректирующих действий в этой таблице предполагается выбранная вкладка **Общие** диалогового окна свойств устройства.

Таблица 9.3. *Распространенные ошибки устройств и методы их устранения*

Сообщение об ошибке	Корректирующее действие
Это устройство настроено неправильно. (This device is not configured correctly.) (Код 1)	Раздобудьте совместимый драйвер для устройства, а затем нажмите кнопку **Обновить** на вкладке **Драйвер** окна свойств устройства, чтобы запустить мастер обновления драйверов, и следуйте выводимым инструкциям
Драйвер для данного устройства может быть поврежден, или в системе недостаточно памяти или иных ресурсов. (The driver for this device might be corrupted, or your system might be running low on memory or other resources.) (Код 3)	Нажмите кнопку **Обновить** на вкладке **Драйвер** окна свойств устройства, чтобы запустить мастер обновления драйверов, и следуйте выводимым инструкциям. Эта ошибка может выводить сообщение об ошибке нехватки памяти
Запуск этого устройства невозможен. (This device cannot start.) (Код 10)	Запустите мастер обновления драйверов, нажав кнопку **Обновить** на вкладке **Драйвер** окна свойств устройства, и следуйте выводимым инструкциям. Выберите опцию не автоматической установки драйвера, а ручную и укажите устройство, для которого нужно установить драйвер

Таблица 9.3 *(продолжение)*

Сообщение об ошибке	Корректирующее действие
Не найдены свободные ресурсы, нужные для этого устройства. (This device cannot find enough free resources that it can use.) (Код 12)	Конфликт выделения ресурсов этому устройству и другому устройству, или же неправильная настройка микропрограммного обеспечения. Проверьте микропрограммное обеспечение, а также наличие конфликтов ресурсов на вкладке **Ресурсы** окна свойств устройства
Это устройство не может работать правильно, пока компьютер не будет перезагружен. (This device cannot work properly until you restart your computer.) (Код 14)	Обычно драйвер установлен правильно, но чтобы его задействовать, нужно перезапустить компьютер
Не удается установить все ресурсы, используемые этим устройством. (Windows cannot identify all the resources this device uses.) (Код 16)	Проверьте возможность установки подписанного драйвера для устройства. Если подписанный драйвер уже установлен, возможно, нужно выполнить настройку выделения ресурсов для устройства. Проверьте наличие конфликтов ресурсов на вкладке **Ресурсы** окна свойств устройства
Нужно заново установить драйверы этого устройства. (Reinstall the drivers for this device.) (Код 18)	После обновления может потребоваться войти в систему по учетной записи администратора, чтобы завершить установку устройства. Если это не требуется, переустановите драйвер, нажав кнопку **Обновить** на вкладке **Драйвер** окна свойств устройства
Возможно, поврежден реестр. (Your registry might be corrupted.) (Код 19)	Удалите и повторно установите устройство. Это должно исправить неверные или конфликтующие настройки реестра
Устройство будет удалено. (Windows is removing this device.) (Код 21)	Система удалит устройство по причине возможного повреждения реестра. Если устройство продолжает выводить это сообщение, перезапустите компьютер
Устройство отключено. (This device is disabled.) (Код 22)	Устройство было отключено в диспетчере устройств. Включите его, нажав кнопку **Включить** на вкладке **Драйвер** окна свойств устройства
Устройство отсутствует, работает неправильно, или для него установлены не все драйверы. (This device is not present, is not working properly, or does not have all its drivers installed.) (Код 24)	Это сообщение может быть признаком неполадки драйвера или устройства. Ошибка также может возникать с унаследованными устройствами. Обновите драйвер
Для устройства не установлены драйверы. (The drivers for this device are not installed.) (Код 28)	Раздобудьте совместимый драйвер для устройства, а затем запустите мастер обновления драйверов, нажав кнопку **Обновить** на вкладке **Драйвер** окна свойств устройства, и следуйте выводимым инструкциям
Устройство отключено, т. к. управляющее встроенное ПО устройства не получило затребованные ресурсы от системы. (This device is disabled because the firmware of the device did not give it the required resources.) (Код 29)	Проверьте в документации на устройство, как выделять ему ресурсы. Может понадобиться обновить микропрограммное обеспечение устройства или включить его в микропрограммном обеспечении системной платы

Таблица 9.3 *(продолжение)*

Сообщение об ошибке	Корректирующее действие
Это устройство работает неправильно, т. к. Windows не удается загрузить для него нужные драйверы. (This device is not working properly because Windows cannot load the drivers required for this device.) (Код 31)	Драйвер устройства может быть несовместим с Windows 8. Раздобудьте совместимый драйвер для устройства, а затем запустите мастер обновления драйверов, нажав кнопку **Обновить** на вкладке **Драйвер** окна свойств устройства, и следуйте выводимым инструкциям
Драйвер для этого устройства не требуется и был отключен. (A driver for this device was not required and has been disabled.) (Код 32)	Зависимая служба для этого устройства была отключена. Проверьте журналы событий, чтобы определить, какие службы нужно включить и запустить
Невозможно определить, какие ресурсы требуются для данного устройства. (Windows cannot determine which resources are required for this device.) (Код 33)	Это сообщение может быть признаком неполадки драйвера или устройства. Ошибка также может возникать с унаследованными устройствами. Обновите драйвер и/или проверьте в документации на устройство, как настраивать выделение ресурсов для него
Не удается определить параметры настройки для этого устройства. (Windows cannot determine the settings for this device.) (Код 34)	Унаследованное устройство, для которого настройку нужно выполнять вручную. Проверьте установку перемычек или настройку параметров микропрограммного обеспечения, а затем настройте выделение ресурсов устройству на вкладке **Ресурсы** окна свойств устройства
Аппаратные средства защиты программного обеспечения не содержат достаточной информации для правильной настройки и использования этого устройства. (Your computer's system firmware does not include enough information to properly configure and use this device.) (Код 35)	Эта ошибка происходит на многопроцессорных системах. Обновите микропрограммное обеспечение; проверьте установленное в микропрограммном обеспечении значение многопроцессорной спецификации (MPS) — 1.1 или 1.4. Обычно нужно установить значение MPS 1.4
Устройство запрашивает прерывание PCI, а в параметрах настройки указаны прерывания ISA (или наоборот). (This device is requesting a PCI interrupt but is configured for an ISA interrupt (or vice versa).) (Код 36)	Прерывания унаследованных устройств не могут быть разделяемыми. Эта ошибка может происходить, если устройство установлено в слот PCI, который в настройках микропрограммного обеспечения зарезервирован для унаследованного устройства. Исправьте настройку параметров в микропрограммном обеспечении
Не удалось инициализировать драйвер этого устройства. (Windows cannot initialize the device driver for this hardware.) (Код 37)	Запустите мастер обновления драйверов, нажав кнопку **Обновить** на вкладке **Драйвер** окна свойств устройства, и следуйте выводимым инструкциям
Системе Windows не удается загрузить драйвер этого устройства, т. к. его предыдущий экземпляр все еще находится в памяти. (Windows cannot load the device driver for this hardware because a previous instance of the device driver is still in memory.) (Код 38)	Конфликт, вызываемый находящимся в памяти предыдущим экземпляром драйвера. Перезагрузите компьютер

Таблица 9.3 *(продолжение)*

Сообщение об ошибке	Корректирующее действие
Не удалось загрузить драйвер этого устройства. Возможно, драйвер поврежден или отсутствует. (Windows cannot load the device driver for this hardware. The driver might be corrupted or missing.) (Код 39)	Проверьте, что устройство установлено правильно, подключено и на него подается питание. Если с этим все в порядке, обновите драйвер или переустановите текущий драйвер
Windows не удается получить доступ к этому оборудованию, т. к. информация о разделе службы в реестре отсутствует или неправильна. (Windows cannot access this hardware because its service key information in the registry is missing or recorded incorrectly.) (Код 40)	Раздел реестра для драйвера устройства может быть недействительным. Переустановите драйвер
Драйвер этого устройства успешно загружен, но само устройство не обнаружено. (Windows successfully loaded the device driver for this hardware but cannot find the hardware device.) (Код 41)	Если устройство было удалено, удалите драйвер, переустановите устройство, а затем в панели инструментов консоли управления компьютеров нажмите кнопку **Обновить конфигурацию оборудования** (Scan for hardware changes), чтобы переустановить драйвер. Если устройство не было отключено или не поддерживает Plug and Play, заполучите новый драйвер для устройства или обновление для него. Для установки устройств, не поддерживающих Plug and Play, воспользуйтесь мастером добавления оборудования. Для этого в меню диспетчера устройств нажмите опцию **Действие** и выберите опцию **Установить старое устройство** (Add legacy hardware)
Windows не удается загрузить драйвер этого устройства, т. к. такое же устройство уже работает в системе. (Windows cannot load the device driver for this hardware because there is a duplicate device already running in the system.) (Код 42)	Система обнаружила дубликат устройства. Эта ошибка происходит, когда драйвер устройства ошибочно создает два устройства с одинаковым именем или когда устройство с серийным номером обнаруживается в новом месте, прежде чем оно было удалено из старого. Перезапустите компьютер, чтоб устранить проблему
Система Windows остановила это устройство, т. к. оно сообщило о возникновении неполадок. (Windows has stopped this device because it has reported problems.) (Код 43)	Устройство было остановлено операционной системой. Может потребоваться удалить, а затем снова установить его. Устройство может испытывать проблемы с возможностью процессора NX. В таком случае следует рассмотреть установку нового драйвера
Приложение или служба выполнили завершение работы этого устройства. (An application or service has shut down this hardware device.) (Код 44)	Драйвер был остановлен приложением или службой. Перезагрузите компьютер. Также устройство может испытывать проблемы с возможностью процессора NX. В таком случае следует рассмотреть установку нового драйвера
Сейчас это устройство не подключено к компьютеру. (Currently, this hardware device is not connected to the computer.) (Код 45)	При запуске диспетчера устройств, когда переменная среды `DEVMGR_SHOW_NONPRESENT_DEVICES` имеет значение `1`, все ранее подключенные устройства, которые отсутствуют в данный момент, отображаются в списке устройств и имеют этот код ошибки. Чтобы устранить это сообщение, подключите устройство к компьютеру или запустите диспетчер устройств, присвоив этой переменной среды значение `0`

Таблица 9.3 *(окончание)*

Сообщение об ошибке	Корректирующее действие
Windows не удалось получить доступ к этому устройству, поскольку операционная система находится в процессе завершения работы. (Windows cannot gain access to this hardware device because the operating system is in the process of shutting down.) (Код 46)	Устройство недоступно, т. к. выполняется завершение работы компьютера. Устройство будет доступно после перезагрузки компьютера
Windows не может использовать это устройство, поскольку оно было подготовлено для "безопасного извлечения", но так и не было извлечено из компьютера. (Windows cannot use this hardware device because it has been prepared for safe removal, but it has not been removed from the computer.) (Код 47)	Эта ошибка происходит при попытке использовать устройство, подготовленное для безопасного извлечения. Чтобы использовать устройство, отсоедините, а затем снова подсоедините его, или же перезапустите компьютер
Запуск программного обеспечения для этого устройства был заблокирован, поскольку известно, что оно не может нормально работать под управлением Windows. Обратитесь к изготовителю для получения нового драйвера. (The software for this device has been blocked from starting because it is known to have problems with Windows. Contact the hardware vendor for a new driver.) (Код 48)	Драйвер этого устройства не совместим с Windows, и система не позволила его загрузить. Заполучите у поставщика устройства новый или обновленный драйвер и установите его
Windows не удалось запустить новые устройства, поскольку системный куст реестра слишком велик (превышен допустимый размер реестра). (Windows cannot start new hardware devices because the system hive is too large (exceeds the Registry Size Limit).) (Код 49)	Превышен максимальный размер раздела реестра, и для работы новых устройств необходимо уменьшить размер раздела. Эту ошибку могут вызывать устройства, которые больше не подключены к компьютеру, но все еще записаны в реестре системы. Попытайтесь удалить устройства, которые больше не используются

ГЛАВА 10

Выполнение задач обслуживания и поддержки

До сих пор мы рассматривали методы поддержки, поиска и устранения неисправностей, которые можно использовать для управления Windows 8. В этой главе мы обсудим методы для улучшения предоставления технической поддержки, независимо от местонахождения компьютеров, и методы восстановления. Начнем с рассмотрения автоматических обновлений, а затем взглянем, как удаленный помощник способен помочь в диагностировании проблем на удаленном компьютере пользователя. В этом отношении следует напомнить о средстве записи действий по воспроизведению неполадок (psr.exe). Как рассматривалось в *главе 7*, это средство можно использовать для записи сведений, связанных с испытываемой пользователем проблемой, не требуя доступа к его компьютеру.

Управление автоматическими обновлениями

В Windows 8 стандартная функциональность автоматического обновления называется Центром обновления Windows (Windows Update). Но он используется для обновления не только операционной системы, но и программ, поставляемых с ней, а также драйверов аппаратных устройств. В последующих разделах мы рассмотрим работу Центра обновления Windows и его использование для содержания системы в работоспособном состоянии.

Обзор Центра обновлений Windows

Центр обновления Windows является клиентским компонентом, который периодически подключается к указанному серверу и проверяет наличие обновлений. Эту утилиту можно настроить таким образом, что при существовании обновлений она либо загружает и устанавливает их автоматически, либо просто извещает пользователей или администраторов об этом. Серверным компонентом, к которому подключается Центр обновления Windows, является веб-сайт Windows Update корпорации Microsoft (**http://windowsupdate.microsoft.com/**) или указанный сервер служб Windows Update Services, содержащийся организацией.

Центр обновления Windows поддерживает загрузку и установку следующих обновлений и компонентов:

- *критические обновления* — обновления, которые считаются критическими для стабильности и обеспечения безопасности компьютера;
- *обновления безопасности* — обновления, специально предназначенные для повышения безопасности системы;

- *наборы исправлений* — протестированные накопительные наборы обновлений, включающие исправления, обновления безопасности, критические обновления и общие обновления, собранные вместе для облегчения установки;
- *пакеты обновлений* — всесторонние обновления операционной системы и ее компонентов, которые обычно включают критические обновления, обновления безопасности и наборы исправлений;
- *необязательные обновления* — обновления, не представляющие особой важности, но которые могут быть полезными, включая обновления драйверов аппаратных устройств.

Примечание

По умолчанию Центр обновления Windows получает обновления драйверов с веб-сайта Windows Update. Центр обновления Windows можно также настроить на поиск обновлений драйверов на сервере служб Windows Server Update Services, или сначала выполнять поиск на этом сервере и при отсутствии обновлений на нем осуществлять поиск на веб-сайте Windows Update. Для этого нужно включить параметр **Указать поисковый сервер для поиска обновлений для драйверов устройств** (Specify the search server for device driver updates) в узле **Конфигурация компьютера\Административные шаблоны\Система\Установка устройства** редактора объекта локальной политики и выбрать соответствующую опцию **Искать на управляемом сервере** (Search managed server) или **Искать на управляемом сервере, затем на веб-сайте Центра обновления Windows** (Search managed server, then WU).

Ключевой частью расширенной функциональности является возможность Центра обновления Windows сортировать обновления по приоритету, чтобы их можно было применять в порядке важности. Таким образом, наиболее важные обновления можно загрузить и установить перед менее важными. Также можно настроить порядок проверки на наличие обновлений и способ их установки. По умолчанию проверка на наличие новых обновлений выполняется каждые 22 часа. Этот период можно изменить с помощью групповой политики. Также, по умолчанию, загруженные обновления устанавливаются в 3:00 по местному времени. Эти параметры можно изменить, чтобы извещать пользователя о загрузке и/или установке обновлений или выполнять установку в другое время.

Операционная система Windows 8 сокращает количество перезапусков, требуемых после установки обновлений, разрешая установку новой версии файла, даже если старая версия в данный момент используется приложением или компонентом системы. Для этого Windows 8 помечает используемый файл, как требуемый обновления, а затем автоматически заменяет его новой версией при следующем запуске приложения. А для некоторых приложений и компонентов, где этот подход неприемлем, Windows 8 может сохранить их данные, закрыть приложение, обновить файл, а затем перезапустить приложение. В результате процесс обновления является менее неудобным для пользователей.

Практический совет

Для передачи файлов при автоматическом обновлении используется служба BITS[1]. Эта служба передает файлы в фоновом режиме и возобновляет прерванные передачи. Версия службы BITS 4.0, которая входит в состав Windows 8, улучшает механизм передачи посредством более эффективного использования пропускной способности канала, что означает более быструю передачу меньшего объема данных. Посредством групповой политики службы BITS можно настроить загрузку обновлений только в определенные периоды времени и ограничить объем используемой для этого пропускной способности канала. Эти и другие параметры можно настроить посредством параметра политики **Ограничить максимальную пропускную способность сети, используемую службой BITS для фоновой передачи, с помощью расписания работы** (Set up a work schedule to limit the maximum network bandwidth used for BITS background transfers). Этот

[1] Background Intelligent Transfer Service — фоновая интеллектуальная служба передачи.

параметр находится в узле **Конфигурация компьютера\Административные шаблоны\Сеть\ Фоновая интеллектуальная служба передачи (BITS)** редактора объекта групповой политики. Кроме этого, использование BITS 4.0 позволяет Windows 8 получать обновления от доверенных одноранговых узлов по локальной сети, а также с сервера обновлений или непосредственно от Microsoft. Компьютеры локальной сети могут автоматически обнаруживать, когда одноранговый узел сети имеет копию обновления, и загружать обновление непосредственно с этого узла. Это означает, что необходимое обновление можно передавать по глобальной сети лишь один раз, а не десятки или даже сотни раз.

Автоматическое обновление можно использовать несколькими разными способами. Компьютеры можно настроить, применяя следующие опции.

- **Устанавливать обновления автоматически** (Install updates automatically). Операционная система получает все обновления через установленный интервал времени (по умолчанию, каждые 22 часа), после чего устанавливает их в заданное время (по умолчанию, в 3:00). Эта настройка отличается от Windows XP, т. к. от пользователей не требуется одобрение обновлений перед их установкой. Вместо этого обновления загружаются автоматически, а затем устанавливаются согласно определенному расписанию — раз в день в определенное время или раз в неделю в определенный день и время.
- **Загружать обновления, но решение об установке принимается мной** (Download updates but let me choose whether to install them). Операционная система загружает все доступные обновления и уведомляет пользователя о наличии готовых к установке обновлений. Пользователь может принять или отклонить каждое обновление. Принятые обновления устанавливаются. Непринятые обновления не устанавливаются, но остаются в системе и могут быть установлены позже.
- **Искать обновления, но решение о загрузке и установке принимается мной** (Check for updates but let me choose whether to download and install them). Операционная система уведомляет пользователя о наличии обновлений, но не загружает их, ожидая решения пользователя. Одобренные и загруженные обновления также требуют решения пользователя по их установке. Принятые обновления устанавливаются. Непринятые обновления не устанавливаются, но остаются в системе и могут быть установлены позже.
- **Не проверять наличие обновлений** (Never check for updates). Система не проверяет наличие обновлений, не загружает и не устанавливает их, но пользователи могут выполнять проверку самостоятельно и загружать требуемые обновления с веб-сайта Windows Update.

Когда обновление Windows настроено на автоматическую загрузку и установку обновлений, пользователи извещаются об этих процессах в минимальном объеме. Получить дополнительную информацию о состоянии обновлений можно, щелкнув на соответствующем значке в области уведомлений панели задач.

Восстановление полезных данных и компонентов с помощью Центра обновления Windows

Центр обновления Windows также применяется для выполнения следующих задач:

- восстановления удаленных полезных данных;
- переустановки поврежденных компонентов.

Двоичные файлы, необходимые для установки функциональностей Windows, называются *полезными данными* (payloads). На серверах под управлением Windows Server 2012 можно удалить не только необязательную функциональность, но также и полезные данные этой функциональности, используя для этого параметр `-Remove` командлета `Unistall-WindowsFeature`.

А с помощью командлета `Install-WindowsFeature` функциональность и ее полезные данные можно восстановить. По умолчанию восстановление полезных данных выполняется через веб-сайт Windows Update. Но можно указать и альтернативные источники файлов, включив и настроив параметр **Указать параметры для установки необязательных компонентов и восстановления компонентов** (Specify settings for optional component installation and component repair), который находится в узле **Конфигурация компьютера\Административные шаблоны\Система** редактора объекта групповой политики. Посредством этого параметра можно также указать никогда не загружать полезные данные с веб-сайта Windows Update.

В качестве альтернативных источников можно указать общие папки или файлы Windows Imaging (wim). Пути к альтернативным источникам разделяются точкой с запятой. В случае файлов wim, следует указать в формате UNC путь к общей папке, содержащей файл wim, и индекс требуемого образа в этом файле, используя для этого следующий синтаксис:

`wim:\\`*`ServerName`*`\`*`ShareName`*`\`*`ImageFileName`*`.wim:`*`Index`*

Здесь параметр *`ServerName`* обозначает имя сервера, *`ShareName`* — имя общей папки, *`ImageFileName`*`.wim` — имя файла wim, а *`Index`* — индекс требуемого образа в файле. Например:

```
wim:\\CorpServer62\Images\install.wim:2
```

Если операционная система обнаруживает повреждение системного компонента, требуемое для восстановления этого компонента содержимое можно загрузить с веб-сайта Windows Update. По умолчанию обновление компонентов выполняется через службы Windows Server Update Services (WSUS), если таковые доступны. Путь к альтернативному источнику файлов можно указать, включив и настроив параметр групповой политики **Указать параметры для установки необязательных компонентов и восстановления компонентов**. Можно также указать получение обновлений непосредственно с веб-сайта Windows Update, а не через службы WSUS.

Настройка автоматического обновления

Операционная система Windows 8 разделяет обновления на следующие четыре общие категории:

- **Важные обновления** — содержат критические обновления, обновления безопасности, наборы исправлений и пакеты обновлений для операционной системы и программ, поставляемых вместе с операционной системой;
- **Рекомендуемые обновления** — в состав входят обновления для драйверов, поставляемых с операционной системой, и рекомендуемые необязательные обновления;
- **Обновления продуктов Майкрософт** — содержат обновления для других установленных на компьютере продуктов Microsoft, а также новое необязательное программное обеспечение Microsoft;
- **Драйверы для указывающих устройств и принтеров** — содержит обновления драйверов, обеспечивающих возможности рендеринга на стороне клиента.

> ***Примечание***
>
> По умолчанию обновление Windows содержит обновления списков веб-совместимости, предоставляемых Microsoft. Содержащиеся в таких списках веб-сайты автоматически отображаются в Internet Explorer в режиме совместимости. Этой возможностью можно управлять посредством параметров групповой политики **Просмотр в режиме совместимости** (Compatibility View), которая находится в узле редактора групповой политики **Конфигурация компьютера\Компоненты Windows\Internet Explorer**.

Практический совет

В стандартной версии Windows 8, если Центр обновления Windows не находит драйверов для указывающих устройств и принтеров на локальном компьютере или на веб-сайте Windows Update, он продолжает поиск этих драйверов. Если система не находит требуемого драйвера для устройства, она пытается создать подключение, используя любой доступный драйвер, который поддерживает данное оборудование. Но в корпоративных версиях Windows 8 такое поведение необходимо указать явно, включив параметр **Расширить подключения указания и печати для поиска обновлений Windows** (Extend point and print connection to search Windows Updates). Этот параметр находится в узле **Конфигурация компьютера\Административные шаблоны\ Принтеры** редактора локальной групповой политики.

По умолчанию Windows 8 настроена для автоматической установки важных обновлений. Настроить автоматические обновления для отдельных компьютеров можно следующим образом:

1. В Панели управления щелкните на ссылке категории **Система и безопасность**. В открывшемся одноименном окне в разделе **Центр обновления Windows** щелкните на ссылке **Включение или отключение автоматического обновления** (Turn automatic updating on or off).
2. В списке **Важные обновления** (Important updates) следующего окна (рис. 10.1) выберите требуемую опцию для выполнения важных обновлений.

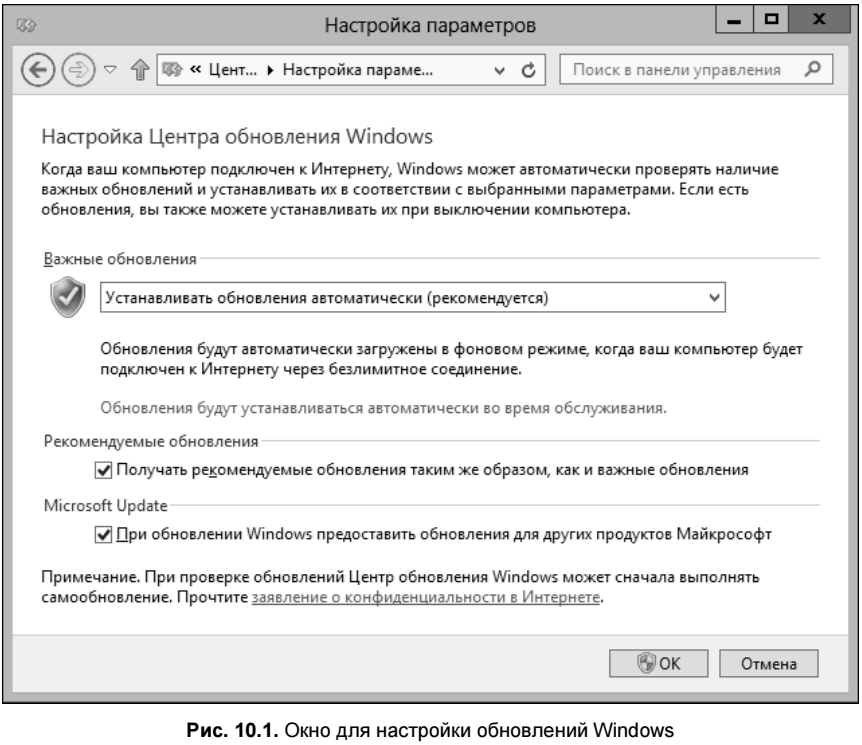


Рис. 10.1. Окно для настройки обновлений Windows

3. Если при выбранной автоматической загрузке обновлений также требуется устанавливать драйверы и необязательные обновления, установите флажок **Получать рекомендуемые обновления таким же образом, как и важные обновления** (Give me recommended updates the same way I receive important updates).
4. Нажмите кнопку **OK**, чтобы закрыть окно и сохранить заданные настройки.

С помощью модуля расширения Microsoft Update функциональность Центра обновления Windows можно расширить для получения обновлений для других установленных на компьютере продуктов Microsoft, а также для получения необязательного программного обеспечения корпорации Microsoft. Модуль расширения Microsoft Update может быть установленным автоматически в процессе установки некоторых загруженных продуктов Microsoft.

Определить, установлен ли на компьютере модуль Microsoft Update, можно следующим образом:

1. В Панели управления щелкните на ссылке категории **Система и безопасность** и в открывшемся списке элементов этой категории выберите ссылку **Центр обновления Windows** (Windows Update).
2. Если компьютер обладает функциональностью Microsoft Update, внизу страницы будет следующее сообщение:

```
Получать обновления: Для Windows и других программных продуктов
из Microsoft Update
(You receive updates: For Windows and other products from Microsoft
Update)
```

Модуль Microsoft Update можно установить следующим образом:

1. В Панели управления щелкните на ссылке категории **Система и безопасность** и в открывшемся списке элементов этой категории выберите ссылку **Центр обновления Windows**.
2. Внизу окна Центра обновления Windows щелкните на ссылке **Дополнительные сведения**, следующей за надписью **Получайте обновления и для других продуктов Майкрософт**. В браузере по умолчанию откроется страница Центра обновления Windows вебсайта Microsoft.
3. Ознакомившись с информацией о Центре обновления Microsoft, установите флажок **Я принимаю условия использования Центра обновления Майкрософт** (I agree to the terms of use) и нажмите кнопку **Установить**.
4. После установки расширения Microsoft Update при включенном автоматическом обновлении система будет загружать и устанавливать обновления для продуктов Microsoft в процессе автоматического обновления. Теперь загрузку и установку обновлений для продуктов Microsoft можно включать и отключать, устанавливая или снимая флажок **При обновлении Windows предоставить обновления для других продуктов Майкрософт** (Give me updates for Microsoft products) в окне настройки параметров обновления Windows. Открыть это окно можно, щелкнув в левой панели окна Центра обновления Windows по ссылке **Настройка параметров**.

По умолчанию обновления Windows устанавливаются автоматически в процессе автоматического обслуживания Windows, которое запускается в 3:00, но если в это время компьютер находится в спящем режиме, он из этого режима не выводится. Если во время запуска запланированного автоматического обслуживания компьютер используется, обслуживание будет запущено позже, когда компьютер будет простаивать. Если автоматическое обслуживание отстает от графика, оно запускается на выполнение в любое время при простаивающем компьютере.

Настроить выполнение автоматического обновления можно следующим образом:

1. В Панели управления щелкните на ссылке категории **Система и безопасность**. В открывшемся одноименном окне в разделе **Центр обновления Windows** щелкните на ссылке **Включение или отключение автоматического обновления**.

2. В следующем окне, **Настройка параметров**, щелкните на ссылке **Обновления будут устанавливаться автоматически во время обслуживания** (Updates will be automatically installed during the maintenance window). В открывшемся окне **Автоматическое обслуживание** (рис. 10.2) в раскрывающемся списке выберите требуемое время для запуска автоматического обслуживания.

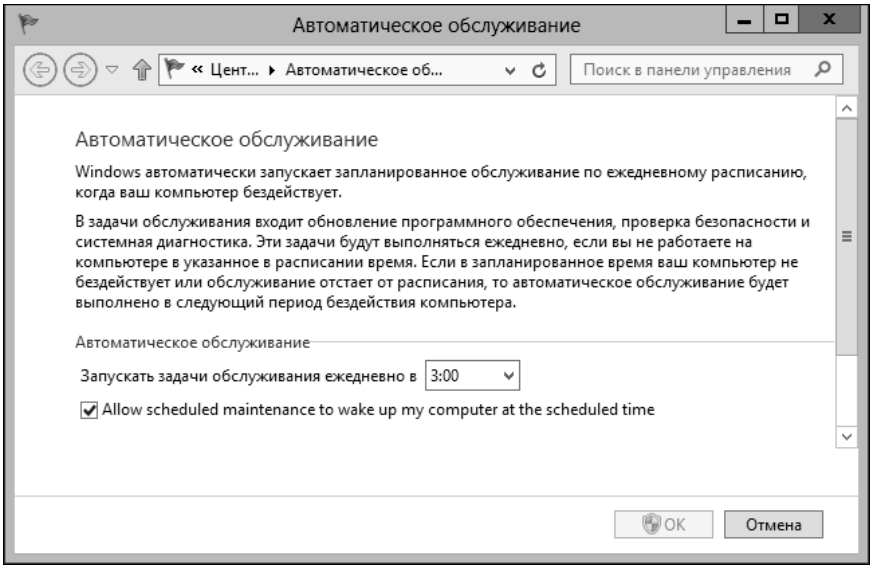


Рис. 10.2. Диалоговое окно для настройки запуска автоматического обслуживания системы, включая установку обновлений Windows

3. В этом же окне можно указать выводить компьютер из режима сна для запуска автоматического обслуживания, установив соответствующий флажок (**Allow scheduled maintenance to wake up my computer at the scheduled time**).
4. Завершив установку параметров запуска автоматического обслуживания, нажмите кнопку **OK**, чтобы сохранить их и закрыть диалоговое окно.

В домене службы Active Directory автоматические обновления можно централизованно настраивать и управлять ими посредством параметров политики **Центр обновления Windows**, которая находится в узле **Конфигурация компьютера\Политики\Административные шаблоны\Компоненты Windows** редактора управления групповыми политиками. Основные параметры политики и их краткое описание перечислены в табл. 10.1.

> ***Совет***
>
> Посредством параметров политики **Планировщик заданий обслуживания** (Maintenance scheduler), которая находится в узле **Конфигурация компьютера\Политики\Административные шаблоны\Компоненты Windows** редактора управления групповыми политиками, можно управлять расписанием запуска автоматического обслуживания. Граница активации — это ежедневное запланированное время начала автоматического обслуживания. Для виртуальных машин к значению этого параметра добавляется произвольная задержка вплоть до 30 минут. Значение задержки также можно настраивать.

Таблица 10.1. *Параметры политики для управления автоматическими обновлениями*

Параметр политики	Функция
Разрешить немедленную установку автоматических обновлений (Allow automatic updates immediate installation)	Включение этого параметра разрешает немедленную установку автоматических обновлений, которые не прерывают выполнение служб Windows и не требуют перезагрузки компьютера. Такие обновления устанавливаются сразу же после их загрузки
Разрешать пользователям, не являющимся администраторами, получать уведомления об обновлениях (Allow non-administrators to receive update notifications)	При включенном параметре любой вошедший в систему пользователь может получать уведомления об обновлениях согласно настройке автоматического обновления. При отключенном параметре уведомления об обновлениях получают только администраторы
Частота поиска автоматических обновлений (Automatic updates detection frequency)	Включив этот параметр, можно настроить интервал для проверки на наличие обновлений. По умолчанию этот интервал составляет 22 часа. Если установить новый интервал, к нему добавляется до 20% указанного значения. Иными словами, если задать значение интервала в 10 часов, действительная длина интервала будет составлять, в зависимости от компьютера, от 8 до 10 часов
Настройка автоматического обновления (Configure automatic updates)	Включив этот параметр, можно настраивать работу автоматического обновления, используя опции, подобные описанным ранее в этом разделе. Как часть запланированного обслуживания, можно также выполнять установку (включив соответствующую возможность). Для этого нужно включить и настроить параметры политики **Планировщик заданий обслуживания** (Maintenance Scheduler) в узле **Конфигурация компьютера\Политики\Административные шаблоны\Компоненты Windows** редактора управления групповыми политиками
Задержка перезагрузки при запланированных установках (Delay restart for scheduled installations)	По умолчанию, если после автоматического обновления требуется перезагрузка, она выполняется с задержкой в 15 минут. Включив этот параметр, можно задать другое значение времени задержки
Разрешить клиенту присоединение к целевой группе (Enable client-side targeting)	При включенном параметре и указанном узле размещения службы обновления Microsoft в интрасети администратор может задать целевую группу для текущего объекта групповой политики. Эта функциональность позволяет администраторам управлять установкой обновлений на определенные группы компьютеров. Перед выполнением развертывания обновления оно должно быть разрешено для определенной целевой группы. Этот параметр применим только при использовании службы обновления Microsoft в корпоративной сети
Разрешить управлению электропитанием Центра обновления Windows выводить систему из спящего режима для установки обновлений (Enabling Windows Update power management to automatically wake up the system to install scheduled updates)	Когда этот параметр включен и компьютер настроен для автоматической установки запланированных обновлений, Центр обновлений Windows использует возможности управления электропитанием компьютера для вывода компьютера из спящего режима в запланированное для обновления время с целью установки обновлений. При питании от батарей пробуждение (и установка обновлений) не выполняется
Не выполнять автоматическую перезагрузку при автоматической установке обновлений, если в системе работают пользователи (No auto-restart with logged on users for scheduled automatic updates installations)	При включенном параметре компьютер не будет автоматически перезагружаться после установки обновлений, требующих перезагрузки, если в системе в это время работают пользователи. Вместо этого пользователи уведомляются о необходимости выполнить перезагрузку. Применение обновлений происходит после перезагрузки компьютера

Таблица 10.1 *(окончание)*

Параметр политики	Функция
Повторный запрос для перезагрузки при запланированных установках (Re-prompt for restart with scheduled installations)	Когда этот параметр включен и компьютер настроен для автоматической установки запланированных обновлений, если предыдущая перезагрузка была отложена, пользователи уведомляются повторно о необходимости выполнить перезагрузку после установленного периода времени. Если этот параметр отключен или не задан, интервал для повторных уведомлений будет 10 минут
Запретить использование любых средств Центра обновления Windows (Remove access to use all Windows Update features)	Включение этого параметра запрещает доступ ко всем функциональностям Центра обновления Windows. Доступ пользователей к Центру обновления Windows блокируется, а автоматические обновления полностью отключаются (Этот параметр находится в политике **Центр обновления Windows** в узле **Конфигурация пользователя\Политики\Административные шаблоны\Компоненты Windows** редактора управления групповыми политиками.)
Перенос запланированных автоматических установок обновлений (Reschedule automatic updates scheduled installations)	При включенном параметре можно задать период времени для ожидания после загрузки системы, прежде чем выполнять пропущенную запланированную установку обновлений
Указать размещение службы обновления Майкрософт в интрасети (Specify intranet Microsoft Update service location)	Включив этот параметр, можно указать полное доменное имя сервера обновлений Microsoft и связанного сервера статистики, поддерживаемых организацией. Обе службы могут выполняться одним сервером
Включить рекомендуемые обновления через автоматическое обновление (Turn on recommended updates via automatic updates**)**	Включение этого параметра разрешает установку рекомендуемых обновлений, включая обновления для драйверов и другие необязательные обновления, вместе с важными обновлениями

Проверка наличия обновлений

На главной странице Центра обновления Windows предоставлены сведения о времени последней проверки (выполненной системой или пользователем) на наличие обновлений, времени последней установки обновлений и текущей конфигурации автоматических обновлений. Проверить использование Центра обновления Windows или выполнить ручную проверку на наличие обновлений можно следующим образом:

1. В Панели управления щелкните на ссылке категории **Система и безопасность**. В следующем окне щелкните на ссылке **Центр обновления Windows**. Открывшееся одноименное окно содержит сведения о времени последней проверки (выполненной системой или пользователем) на наличие обновлений, времени последней установки обновлений и текущей конфигурации автоматических обновлений.
2. Чтобы проверить наличие обновлений вручную, нажмите кнопку **Поиск обновлений** (Check for updates).
3. Чтобы установить необязательные обновления, которые могут быть доступными для установки, щелкните на ссылке, указывающей количество доступных необязательных обновлений.

4. В следующем окне, **Выбор обновлений для установки** (Select updates to install), установите флажки для необязательных обновлений, которые хотите установить, и нажмите кнопку **Установить**.

Просмотр журнала обновлений и установленных обновлений

Диспетчер загрузок Центра обновления Windows отслеживает как успешные, так и неудачные обновления, записывая их в журнал обновлений. Доступ к этому журналу можно получить следующим образом:

1. В Панели управления щелкните на ссылке категории **Система и безопасность**, а в следующем окне — на ссылке **Центр обновления Windows**.
2. В левой панели окна Центра обновления щелкните на ссылке **Просмотр журнала обновлений** (View update history). Откроется окно **Просмотр журнала обновлений**.

В журнале обновлений успешно загруженные и установленные обновления будут помечены **Успешно** в столбце **Состояние**. Обновления, помеченные **Неуспешно**, были загружены, но по какой-либо причине не были установлены. Состояние обновлений также может быть помечено как **Ожидается перезапуск** (Pending restart) или **Отменено**. Установка некоторых обновлений может быть завершена только в процессе загрузки операционной системы, и такие обновления помечаются **Ожидается перезапуск**. После перезапуска компьютера и установки такого обновления его состояния будет помечено соответственно результатам установки. Загрузка обновлений может быть отменена по разным причинам. Например, пользователю может срочно понадобиться выполнить какую-то задачу. Перезапуск компьютера также может отменить загрузку обновления.

Установленное обновление можно удалить, щелкнув в окне **Просмотр журнала обновлений** по ссылке **Установленные обновления**. Затем, в открывшемся одноименном окне следует щелкнуть правой кнопкой мыши на требуемом обновлении и в контекстном меню выбрать команду **Удалить**.

Удаление автоматических обновлений для исправления проблемы

Иногда после установки автоматических обновлений система начинает испытывать проблемы. В таком случае подозреваемое обновление можно удалить, как любую другую установленную программу. Процедура для этого следующая:

1. В Панели управления щелкните на ссылке категории **Система и безопасность**, а в следующем окне — на ссылке **Центр обновления Windows**.
2. В окне Центра обновления Windows щелкните на ссылке **Просмотр журнала обновлений** и далее — на ссылке **Установленные обновления**.
3. Выберите требуемое обновление и в строке меню над списком обновлений нажмите кнопку **Удалить**.

Скрытие доступных обновлений

Со временем может накопиться несколько обновлений, установка которых была преднамеренно отклонена, но которые продолжают отображаться в списке обновлений, доступных

для установки. Эти обновления можно скрыть в списке доступных обновлений следующим образом:

1. В Панели управления щелкните на ссылке категории **Система и безопасность**, а в следующем окне — на ссылке **Центр обновления Windows**.
2. В окне Центра обновлений щелкните на ссылке уведомления о доступных обновлениях.
3. Затем, в открывшемся окне **Выбор обновлений для установки** щелкните правой кнопкой мыши на требуемом обновлении и в контекстном меню выберите команду **Скрыть обновление** (Hide update).

Восстановление скрытых обновлений

Если по каким-либо причинам потребуется установить отклоненные и скрытые обновления, восстановить их отображение в списке доступных обновлений можно таким образом:

1. В Панели управления щелкните на ссылке категории **Система и безопасность**, а в следующем окне — на ссылке **Центр обновления Windows**.
2. В левой панели окна Центра обновления Windows щелкните на ссылке **Восстановление скрытых обновлений** (Restore hidden updates).
3. В открывшемся одноименном окне установите флажок требуемого обновления и нажмите кнопку **Восстановить** (Restore).
4. Обновление опять будет отображаться в списке доступных для установки обновлений и может быть установлено обычным образом.

Использование удаленного помощника для решения проблем

Удаленный помощник позволяет персоналу технической поддержки просматривать рабочий стол удаленного пользователя и управлять его компьютером для поиска и удаления неполадок или для предоставления пошагового руководства пользователю при выполнении сложных задач. Но чтобы использовать эту возможность, ее нужно предварительно настроить. Локальная настройка удаленного помощника рассматривается в *главе 7*, а посредством групповой политики — в *главе 5*.

Основные сведения об удаленном помощнике

Функциональность удаленного помощника доступна в Windows XP и более поздних версиях Windows. Только пользователи компьютеров с такими операционными системами могут создавать и отвечать на приглашения удаленного помощника. Для простоты и легкости работы с удаленным помощником в организации следует обеспечить следующее:

1. Всегда используйте учетную запись, которая является членом локальной группы удаленных помощников (Offer remote assistance helpers).
2. Создайте исключения брандмауэра Windows для исполняемых файлов msra.exe и raserver.exe и откройте TCP-порт 135 для DCOM. Обычно эти настройки выполняются по умолчанию посредством групповой политики.
3. Проверьте, что удаленный компьютер настроен на разрешение подключения удаленного помощника.

Теперь к удаленному компьютеру можно подключиться по его имени или IP-адресу.

Дополнительная информация

Операционная система Windows может определить, когда брандмауэр Windows блокирует подключения удаленного помощника. В таком случае на компьютере пользователя, приглашающего удаленного помощника, в окне удаленного помощника выводится сообщение о том, что его компьютер не настроен на отправление приглашений. В этом же окне пользователю предоставляется возможность исправить эту проблему, нажав кнопку **Исправить**. Эта кнопка запускает средство диагностики сетей Windows, которое исследует сетевые настройки компьютера, выводит окно с сообщением о причине проблемы — **Удаленный помощник не включен** — и ее рекомендуемым решением, а также предоставляет пользователю возможность реализовать рекомендуемое решение от имени администратора. Если пользователь обладает полномочиями администратора, он может выбрать эту опцию, чтобы включить удаленный помощник, а затем закрыть средство диагностики.

В корпоративной сети предоставление удаленной помощи осуществляется следующим образом:

1. Откройте окно **Удаленный помощник Windows** (Windows Remote Assistance). Это можно сделать, например, нажав клавишу <Windows> и выполнив команду `msra.exe` в поле поиска панели **Приложения**.
2. В окне удаленного помощника щелкните на ссылке **Помочь тому, кто вас пригласил** (Help someone who has invited you).
3. На следующей странице окна удаленного помощника щелкните на ссылке **Вариант расширенного подключения для службы поддержки** (Advanced connection option for help desk).
4. На следующей странице удаленного помощника введите имя или IP-адрес требуемого компьютера в соответствующее поле, а затем нажмите кнопку **Далее**, чтобы выполнить подключение к этому компьютеру.

Пользователи могут инициировать сеанс удаленной помощи, отправив приглашение персоналу технической поддержки. Персонал технической поддержки может сам инициировать сеанс удаленной помощи, предлагая ее пользователям. После установления сеанса помощник может обмениваться сообщениями с пользователем, просматривать его рабочий стол и управлять его компьютером (последнее при условии получения разрешения пользователя на это).

Существует несколько способов создания приглашения удаленному помощнику.

- **Пригласить по электронной почте** (Use email to send an invitation). Эти приглашения отправляются в виде сообщений электронной почты по указанному адресу. Сообщение содержит вложение, которое используется для инициирования сеанса удаленной помощи. Полезно настроить стандартный адрес электронной почты, например, **RemotAssist@*your_company_name*.com**, чтобы позволить пользователям с легкостью отправлять приглашения персоналу технической поддержки по электронной почте. Если этот адрес настроить в сервере Microsoft Exchange Server в виде списка рассылки, который доставляет приглашения членам команды технической поддержи, или в виде отдельного почтового ящика для определенных членов команды технической поддержки, персонал команды поддержки сможет обрабатывать приглашения более эффективно, а у пользователей будет стандартный способ для запроса помощи.
- **Отправка приглашения в файле.** Файловые приглашения сохраняются в файлах типа MsRcIncident. Двойной щелчок по такому файлу активирует сеанс удаленного помощника. Файловые приглашения можно применять, когда используется электронная почта с веб-интерфейсом и приглашение необходимо вставлять отдельно. Для файловых приглашений будет полезным создать общую папку, которая автоматически подключается для пользователей в виде сетевого диска, и сделать ее доступной для персонала техниче-

ской поддержки. Этой папке следует присвоить имя, которое позволяет с легкостью определить ее назначения общего приемника запросов удаленной помощи, например, **Запросы службы поддержки** или **Приглашения помощника**.

- **Использование Easy Connect.** При этом подходе приглашение удаленному помощнику отправляется по Интернету с помощью протокола PNRP[1]. Средство Easy Connect автоматически создает пароль, который позволяет удаленному помощнику подключаться к компьютеру. Контактная информация пользователя сохраняется для быстрого доступа в будущем, без использования пароля. (Этот метод работает только в том случае, если компьютеры как пользователя, запрашивающего помощь, так и пользователя, предоставляющего его, работают под управлением Windows 8 или более поздней версии Windows.)

В отличие от предыдущий версий Windows, на компьютерах под Windows 8, чтобы повысить безопасность, для приглашения требуется создать пароль. Пароль предоставляет дополнительный уровень безопасности в параметрах удаленного помощника, обеспечивая возможность просмотра рабочего стола и управление компьютером пользователя только санкционированными помощниками, которым пользователь предоставил пароль для сеанса удаленной помощи. Администратору следует установить официальные правила, требующие использования паролей для приглашений. Чтобы упорядочить процесс приглашения удаленного помощника, полезно определить пароли, используемые с приглашениями. Желательно назначать разные пароли для различных групп организации и регулярно менять эти пароли.

Для работы удаленного помощника требуется наличие установленного сетевого подключения между компьютерами пользователя и помощника. Для обеспечения удаленному помощнику связи используются протоколы UPnP, SSDP, PNRP и Teredo. Так как большинство брандмауэров по умолчанию не разрешает эти протоколы, брандмауэр между компьютерами может препятствовать установлению сеанса удаленного помощника. В таком случае в брандмауэре необходимо создать исключение для исходящих сообщений из компьютера помощника на компьютер пользователя, нуждающегося в помощи. Это исключение можно настроить следующим образом:

1. В Панели управления щелкните на ссылке категории **Система и безопасность**. В разделе Брандмауэр Windows щелкните на ссылке **Разрешение взаимодействовать с приложением через брандмауэр Windows** (Allow an app through Windows Firewall).
2. В открывшемся окне **Разрешенные программы** (Allowed Apps) прокрутите список **Разрешенные программы и компоненты** (Allowed apps and features) вниз до тех пор, пока не будет видна запись **Удаленный помощник** (Remote Assistance), и проверьте, что для этой записи установлен флажок для соответствующей сети — **Домен**, **Частная** или **Публичная**.
3. Установите и снимите эти флажки, чтобы указать типы сетей, в которых разрешено использование удаленного помощника. Нажмите кнопку **OK**, чтобы закрыть окно и сохранить заданные настройки.

Удаленный помощник может работать через брандмауэры NAT. При предоставлении поддержки посредством удаленного помощника можно использовать встроенные инструменты диагностирования, которые можно запускать простым щелчком мыши. Чтобы упростить процесс поиска и устранения неполадок и разрешить передачу вопросов поддержки по инстанции, к удаленному компьютеру могут одновременно подключаться два разных техни-

[1] Peer Name Resolution Protocol — протокол разрешения одноранговых имен.

ческих специалиста. Наконец, благодаря возможности автоматического переподключения после перезапуска, после перезагрузки удаленного компьютера восстанавливать сеанс удаленного помощника не нужно, т. к. он восстанавливается автоматически после загрузки удаленного компьютера.

Создание приглашений удаленному помощнику

Приглашение удаленному помощнику для отправки по электронной почте создается следующим образом:

1. В разделе **Система и безопасность** Панели управления щелкните по ссылке **Поиск и устранение проблем** (Find and fix problems). В левой панели открывшегося окна **Устранение неполадок** (Troubleshooting) щелкните по ссылке **Обращение за помощью к другу** (Get help from a friend).
2. В следующем окне, **Удаленный помощник**, щелкните по ссылке **Попросите вам помочь** (Invite someone to help you) и в открывшемся диалоговом окне — по ссылке **Пригласить по электронной почте** (Use email to send an invitation).
3. Запустится программа электронной почты по умолчанию со стандартным сообщением запроса о помощи. Введите адрес электронной почты человека, которого вы хотите попросить помочь вам, и отправьте сообщение. После отправления сообщения отроется окно удаленного помощника, содержащее пароль для подключения к компьютеру. Этот пароль нужно сообщить лицу, которому вы отправили приглашение о помощи.

Приглашение удаленному помощнику, которое сохраняется в файле, создается следующим образом:

1. В разделе **Система и безопасность** Панели управления щелкните по ссылке **Поиск и устранение проблем**. В левой панели открывшегося окна **Устранение неполадок** щелкните по ссылке **Обращение за помощью к другу**.
2. В следующем окне, **Удаленный помощник**, щелкните по ссылке **Попросите вам помочь** и в открывшемся диалоговом окне **Удаленный помощник Windows** — по ссылке **Сохранить приглашение как файл** (Save this invitation as a file).
3. В открывшемся окне для навигации по файловой системе укажите папку для сохранения приглашения и имя файла приглашения (по умолчанию используется имя файла "Приглашение") и нажмите кнопку **Сохранить**. (Если сохранить файл приглашения в сетевой папке, администратор или другой член команды поддержки может с легкостью получить доступ к этому приглашению.)
4. Окно сохранения файла закроется и откроется окно удаленного помощника с паролем. Передайте сохраненный файл приглашения и пароль лицу, у которого запрашивается помощь. Пароль нужен для того, чтобы помощник мог подключиться к компьютеру, и действителен только для данного сеанса удаленного помощника.

Приглашение удаленному помощнику методом Easy Connect создается следующим образом:

1. В разделе **Система и безопасность** Панели управления щелкните по ссылке **Поиск и устранение проблем**. В левой панели открывшегося окна **Устранение неполадок** щелкните по ссылке **Обращение за помощью к другу**.
2. В следующем окне, **Удаленный помощник**, щелкните по ссылке **Попросите вам помочь** и в открывшемся диалоговом окне **Удаленный помощник Windows** — по ссылке **Использовать Easy Connect** (Use Easy Connect).

3. После настройки подключения Easy Connect откроется окно удаленного помощника, содержащее автоматически сгенерированный пароль. Этот пароль необходимо сообщить помощнику, чтобы он мог подключиться к компьютеру, и действителен только для данного сеанса удаленного помощника.

По умолчанию приглашения удаленному помощнику действительны в течение 6 часов и позволяют удаленному помощнику управлять удаленным компьютером. Эти настройки можно изменить в диалоговом окне **Свойства системы** *(см. разд. "Настройка удаленного помощника" главы 7)*. После отправления приглашения по электронной почте или сохранения файла приглашения открывается диалоговое окно удаленного помощника. Диалоговое окно помощника пользователя, получающего помощь, предоставляет следующие опции управления.

- **Приостановить/Продолжить** (Pause/Continue). Приостанавливает сеанс удаленной помощи, временно запрещая просмотр рабочего стола пользователя, получающего помощь, пользователем, предоставляющим ее. Чтобы возобновить сеанс удаленной помощи, получающий помощь пользователь должен нажать кнопку **Продолжить**.
- **Прекратить удаленное управление** (Stop sharing). Завершает сеанс удаленной помощи, завершая просмотр рабочего стола и управление компьютером удаленным помощником.
- **Параметры** (Settings). Позволяет настраивать параметры сеанса удаленной связи. Доступные параметры зависят от компьютера, которому предоставляется помощь. Общие параметры включают возможность нажатия клавиши <Esc> для прекращения совместного управления удаленным компьютером, сохранение журнала сеанса удаленной помощи и настройка пропускной способности канала связи посредством соответствующего вертикального ползунка для управления качеством отображения удаленного рабочего стола на экране помощника.

> ***Примечание***
>
> По умолчанию журнал сеанса удаленной помощи сохраняется в папке *%ПрофильПользователя%*\Документы\Remote Assistance Logs как компьютера пользователя, получающего помощь, так и компьютера пользователя, предоставляющего ее.

- **Разговор** (Chat). Открывает окно для обмена сообщениями между пользователем и помощником.

Предложение удаленной помощи или ответ на приглашение удаленного помощника

Если вы знаете, что пользователь испытывает проблемы со своим компьютером, ему можно предложить удаленную помощь, не ожидая, пока он ее запросит одним из выше рассмотренных способов. Процедура для предложения помощи удаленному помощнику следующая:

1. Запустите мастер удаленного помощника Windows. Один из способов сделать это — ввести команду `msra` в поле поиска панели **Приложения** и нажать клавишу <Enter>.
2. В окне удаленного помощника щелкните по ссылке **Помочь тому, кто вас пригласил**.
3. На следующей странице окна удаленного помощника щелкните по ссылке **Вариант расширенного подключения для службы поддержки**.
4. На следующей странице удаленного помощника введите имя или IP-адрес требуемого компьютера в соответствующее поле, а затем нажмите кнопку **Далее**, чтобы выполнить подключение к этому компьютеру.

Если пользователь прислал вам приглашение по электронной почте, на это приглашение можно ответить, выполнив двойной щелчок по файлу приглашения, вложенному в сообщение электронной почты. Также можно ответить на приглашение, сохраненное в файле. Процедура для этого следующая:

1. Запустите мастер удаленного помощника Windows. Один из способов сделать это — ввести команду `msra` в поле поиска панели **Приложения** и нажать клавишу <Enter>.
2. В окне удаленного помощника щелкните по ссылке **Помочь тому, кто вас пригласил**.
3. На следующей странице мастера щелкните по ссылке **Использовать файл приглашения** (Use an invitation file), в открывшемся окне навигации по файловой системе компьютера укажите требуемый файл приглашения и нажмите кнопку **Открыть**.
4. В окне запроса пароля введите предоставленный вам пользователем пароль для этого приглашения и нажмите кнопку **OK**.
5. После того как пользователь удаленного компьютера разрешит подключение, будет установлен сеанс удаленной помощи с удаленным компьютером.

Если удаленный пользователь хочет получить помощь посредством метода Easy Connect и предоставил вам пароль, на это приглашение можно ответить следующим образом:

1. Запустите мастер удаленного помощника Windows. Один из способов сделать это — ввести команду `msra` в поле поиска панели **Приложения** и нажать клавишу <Enter>.
2. В окне удаленного помощника щелкните по ссылке **Помочь тому, кто вас пригласил**.
3. На следующей странице мастера щелкните по ссылке **Использовать Easy Connect** (Use Easy Connect). В окне запроса пароля введите предоставленный вам пользователем пароль для этого приглашения и нажмите кнопку **OK**.
4. После того как удаленный пользователь разрешит подключение, между вашими компьютерами будет установлен сеанс удаленной помощи.

При использовании любого из только что рассмотренных методов ответа на приглашение удаленного помощника, после установления сеанса удаленной помощи на компьютере помощника откроется окно удаленного помощника, в котором отобразится рабочий стол удаленного компьютера.

На рис. 10.3 показана верхняя часть этого окна, содержащая опции меню для управления сеансом.

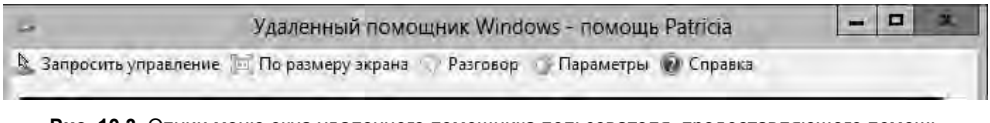


Рис. 10.3. Опции меню окна удаленного помощника пользователя, предоставляющего помощь

Диалоговое окно помощника пользователя, предоставляющего помощь, содержит следующие пункты меню управления.

- **Запросить управление/Прекратить удаленное управление** (Request control/Stop sharing). Запрашивает или прекращает удаленное управление компьютером пользователя. При запросе управления на компьютере удаленного пользователя выводится диалоговое окно с запросом на его согласие предоставления управления.
- **Истинный размер/По размеру экрана** (Fit to screen/Actual size). Настраивает отображение рабочего стола пользователя в окне удаленного помощника или полностью, или по размеру окна.

- **Разговор** (Chat). Открывает окно для обмена сообщениями между пользователем и помощником.
- **Параметры** (Settings). Позволяет настраивать параметры сеанса удаленной помощи. По умолчанию журнал сеанса удаленной помощи сохраняется на компьютере пользователя, предоставляющего помощь, в папке *%ПрофильПользователя%*\Документы\Remote Assistance Logs.

Помощник может завершить сеанс удаленной помощи, закрыв окно удаленного помощника.

Когда предоставляющий помощь пользователь запрашивает управление компьютером удаленного пользователя, на экране этого пользователя выводится диалоговое окно с запросом подтвердить предоставление управления. Получающий помощь пользователь должен нажать в этом окне кнопку **Да**, чтобы разрешить удаленному помощнику управлять его компьютером. Но перед тем как запрашивать управление компьютером удаленного пользователя может быть желательным, чтобы он в своем окне настроил параметры для разрешения удаленному помощнику отвечать на запросы контроля учетных записей. Это разрешение необходимо для того, чтобы предоставляющий помощь пользователь мог выполнять на компьютере пользователя, получающего помощь, задачи, требующие полномочий администратора.

Обнаружение и устранение ошибок Windows 8

На любом компьютере могут быть установлены десятки, а в некоторых случаях сотни, разных служб и компонентов. Содержание всех этих компонентов в надлежащем рабочем состоянии — задача не из легких. Хорошим помощником в обнаружении причин распространенных проблем с работой программных компонентов компьютера и их устранении будут встроенные средства диагностирования, которые обсуждались ранее в этой книге. Как рассматривается в *главе 9*, зарегистрированные проблемы отслеживаются в консоли **Отчеты о проблемах и их решениях** (Problem Reports And Solutions). Подобно встроенным средствам диагностирования это средство пытается предоставить решения проблем, там где это возможно. Но не все проблемы поддаются автоматическому обнаружению и решению. В таких случаях для диагностирования проблем можно использовать сообщения об ошибках, выдаваемые компонентами Windows, приложениями, службами и аппаратными устройствами.

Использование журналов событий для отслеживания и диагностирования ошибок

Операционная система Windows 8 сохраняет сообщения об ошибках, генерируемые процессами, службами, приложениями и аппаратными устройствами, в файлах журналов. При этом используются два общих типа файлов журналов.

- **Журналы событий Windows.** Журналы, в которые операционная система записывает общие системные события, связанные с приложениями, безопасностью, установкой и системными компонентами.
- **Журналы событий приложений и служб.** Журналы, используемые отдельными приложениями и службами для записи своих событий.

Записи в файле журнала заносятся в соответствии с предупредительным уровнем действия. Записываться могут как ошибки, так и общие информационные события. Записи событий классифицируются по следующим уровням:

- **Сведения** (Information) — информационное событие, которое обычно связано с успешным действием;

- **Аудит успеха** (Audit Success) — событие, связанное с успешным выполнением действия;
- **Аудит** — отказ (Audit Failure) — событие, связанное с неудачным выполнением действия;
- **Предупреждение** (Warning) — предупреждение, подробности которого часто полезны для предотвращения будущих проблем с системой;
- **Ошибка** (Error) — ошибка, например, сбой запуска службы.

Кроме уровня, даты и времени, общее и подробное представления события предоставляют следующую информацию:

- **Источник** (Source) — приложение, служба или компонент, который сделали запись о событии;
- **Код события** (Event ID) — идентификатор конкретного события;
- **Категория задачи** (Task Category) — категория события, которая иногда применяется для более подробного описания связанного действия;
- **Пользователь** (User) — учетная запись пользователя, работающего в системе, когда произошло событие. Если событие было вызвано системным процессом или службой, в качестве имени пользователя обычно указывается имя специальной сущности, вызвавшей событие, например, `NETWORK SERVICE`, `LOCAL SERVICE` или `система`;
- **Компьютер** (Computer) — имя компьютера, на котором произошло событие;
- **Подробности** (Details) — в записях сведений предоставляет текстовое описание события и связанные данные или сообщение об ошибке.

Просмотр и управление журналами событий

Журналы событий находятся в узле **Просмотр событий** консоли **Управление компьютером**. Чтобы открыть эту консоль, в Панели управления щелкните по ссылке **Система и безопасность**, далее по ссылке **Администрирование**, а в открывшемся одноименном окне — по значку **Управление компьютером**. Другой способ открыть консоль **Управление компьютером** — это нажать клавишу <Windows> и выполнить в поле поиска панели **Приложения** команду `compmgmt.msc`. (Это поле становится видимым при вводе первой буквы команды.)

Доступ к журналам событий можно получить следующим образом:

1. Откройте консоль **Управление компьютером**. По умолчанию консоль подключена к локальному компьютеру. Для работы с журналами удаленных компьютеров щелкните правой кнопкой мыши по корневому узлу **Управление компьютером** в дереве консоли (левая панель) и в контекстном меню выберите команду **Подключиться к другому компьютеру**. В открывшемся диалоговом окне **Выбор компьютера** установите переключатель **другой компьютер** и введите имя требуемого компьютера в соответствующее поле, после чего нажмите кнопку **OK**.
2. Разверните узел **Просмотр событий** (Event Viewer), а в нем узел **Журналы Windows** (Windows Logs) и/или узел **Журналы приложений и служб** (Applications and Services).
3. Выберите для просмотра требуемый журнал (рис. 10.4).

Дополнительная информация

Нажатие комбинации клавиш <Windows>+<X> открывает в левом нижнем углу экрана контекстное меню со списком наиболее часто используемых инструментов, включая **Управление ком-**

пьютером и **Просмотр событий**. Открыв консоль **Просмотр событий**, можно подключить для просмотра другие компьютеры, щелкнув правой кнопкой мыши по корневому узлу дерева консоли в левой панели и выбрав в контекстном меню команду **Подключиться к другому компьютеру**.

Основными типами событий, на которые следует обратить внимание, являются ошибки и предупреждения. Просмотреть подробное описание таких событий можно в окне свойств события, которое открывается двойным щелчком по требуемому событию. Обратите внимание на источник ошибки и попытайтесь исправить проблему, используя рассматриваемые в этой книге методы. Чтобы получить дополнительную информацию об ошибке и возможных способах ее исправления (если существует такая необходимость), щелкните внизу панели описания события по ссылке **Веб-справка журнала событий** (Event log online) или выполните поиск в базе знаний Microsoft по коду события или по части описания ошибки.

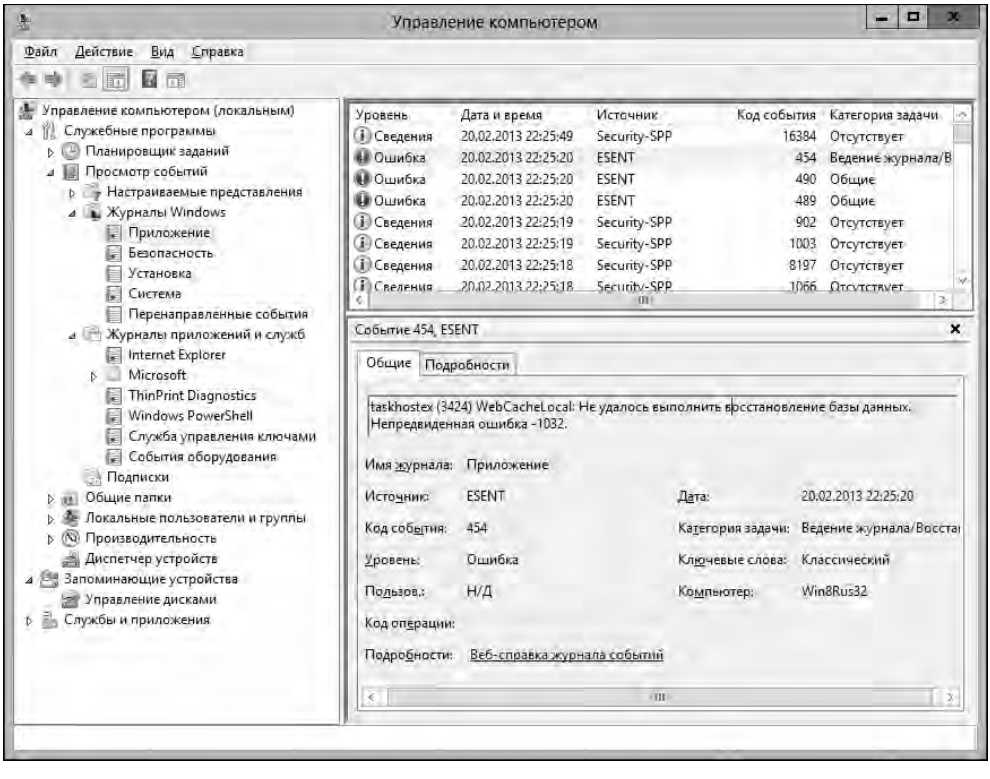


Рис. 10.4. Просмотр журнала событий в оснастке **Просмотр событий** консоли **Управление компьютером**

Планирование задач обслуживания

В процессе администрирования настольных и портативных компьютеров часто требуется выполнять периодические регламентные задачи обслуживания. Для планирования автоматического выполнения таких повторяющихся или одноразовых задач обслуживания можно использовать средство **Планировщик заданий**. Автоматическое выполнение задач осуществляется исполнением сценариев командной строки, сценариев сервера, сценариев Windows или приложений, которые выполняют необходимые команды. В отличие от предыдущих версий Windows, Windows 8 содержит обширную библиотеку предварительно

настроенных заданий. Эти задания выполняют широкий круг операций, от удаления устройств Bluetooth до дефрагментации дисков и сканирований защитником Windows.

Основы планирования заданий

Операционная система Windows 8 содержит несколько инструментов для планирования заданий, включая такие, как **Планировщик заданий**, инструмент командной строки Schtasks и несколько командлетов консоли Windows PowerShell. Эти инструменты можно использовать для планирования заданий как на локальных, так и на удаленных системах. Планировщик заданий содержит несколько мастеров для планирования заданий, которые оснащены интерфейсом типа "указать и щелкнуть" (point-and-click interface) для создания задач. Средство Schtasks представляет собой аналог планировщика заданий, используемый в консоли командной строки. Командлеты консоли Windows PowerShell включают такие, как New-ScheduledTask, New-ScheduledTask Action, Set-ScheduledTask, Start-ScheduledTask и StopScheduledTask.

Все эти инструменты планирования для мониторинга системных часов и исполнения заданий в определенное время полагаются на службу **Планировщик заданий**. Эта служба по умолчанию выполняется по учетной записи **Локальная система**. Но эта учетная запись не обладает достаточными полномочиями для выполнения задач администрирования. Данную проблему можно решить, настроив каждое задание для выполнения определенным пользователем, указав при создании задания имя пользователя и пароль. Но при этом следует обеспечить, чтобы используемая учетная запись обладала достаточными полномочиями и правами доступа для выполнения планируемого задания.

> ***Примечание***
>
> В этом разделе акцент делается на средстве **Планировщик заданий**. Это основной инструмент, используемый для планирования заданий в системах под управлением Windows 8. Дополнительную информацию об инструменте командной строки Schtasks можно получить, выполнив команду `schtasks /?`, а еще более подробную — в *главе 8* книги "Windows Command-Line Administrator's Pocket Consultant, Second Edition"[1].

В Windows 8 существуют два основных типа планируемых заданий.

- **Стандартные задания.** Задания этого типа используются для автоматизации повседневных задач и обслуживания компьютерной системы. Пользователь может видеть эти задания и модифицировать их в случае необходимости.
- **Скрытые задания.** Задания этого типа используются для автоматизации специальных системных задач. Эти задания по умолчанию скрыты от пользователей и в большинстве случаев их не следует изменять. Некоторые скрытые задания создаются и управляются посредством связанной программы, например Защитником Windows.

Операционная система Windows 8 допускает намного более утонченное создание и управление заданиями, чем любая предшествующая версия Windows. Любое задание можно настроить, чтобы:

- выполнять только тогда, когда пользователь вошел в систему, или выполнять независимо от того, выполнил ли пользователь вход в систему или нет;
- выполнять с полномочиями стандартного пользователя или с наивысшими требуемыми полномочиями (включая полномочия администратора).

---

[1] William R. Stanek. Windows Command-Line Administrator's Pocket Consultant, Second Edition. — Microsoft Press, 2008.

Созданные обычным образом задания в Windows 8 несовместимы с более ранними версиями Windows, и поэтому их нельзя копировать на такие компьютеры. Но при создании задания можно указать для него совместимость с более ранними версиями Windows, позволяя, таким образом, использовать эти задания на таких системах.

Задания могут иметь разные связанные с ними свойства, включая следующие.

- **Триггеры.** Триггеры задают условия начала и завершения выполнения задания. Выполнение задания можно начинать по расписанию, а также при входе пользователя в систему, запуске компьютера или при простаивании компьютера. Также задания можно начинать выполнять на основе событий, подключения или отключения пользователя от сеанса сервера терминалов либо при блокировании/разблокировании компьютера пользователем. Возможно, наиболее эффективными являются задания, запускаемые на выполнение посредством событийных триггеров, т. к. они предоставляют возможность автоматизировать обработку ошибок и предупреждений.
- **Действия.** Действия определяют операцию, которую должно выполнять запущенное на выполнение задание. Это позволяет заданию запускать программы, отправлять сообщения электронной почты или выводить сообщения.
- **Условия.** Условия помогают уточнить обстоятельства, при которых активированное задание запускается или останавливается. Например, условия можно использовать, чтобы вывести компьютер из режима сна для выполнения задания и запускать компьютер только в случае наличия определенного сетевого подключения. С помощью условия можно запускать, останавливать и перезапускать задание на основе длительности простоя компьютера. Например, задание можно запускать на исполнение только после 10 минут простоя компьютера, останавливать выполнение задания, когда компьютер начинает использоваться, а затем возобновлять выполнение задания, когда компьютер снова начинает простаивать. Посредством условий также можно указать, что задание должно запускаться на выполнение, только если компьютер работает от сети, и прекращать выполнение задания, когда компьютер переходит на питание от батарей.

Просмотр и управление заданиями на локальных и удаленных системах

Текущие задания системы можно просмотреть в узле **Планировщик заданий** консоли **Управление компьютером**. Задания упорядочены и сгруппированы посредством знакомой системы папок, где базовые папки называются в соответствии с функциональностями, инструментами и областями настроек системы, которые они представляют. Базовая папка содержит одно или несколько связанных заданий.

Просматривать и управлять запланированными заданиями компьютера можно таким образом:

1. Откройте консоль **Управление компьютером**. По умолчанию консоль подключена к локальному компьютеру. Для работы с заданиями удаленных компьютеров щелкните правой кнопкой мыши по корневому узлу **Управление компьютером** в дереве консоли (левая панель) и в контекстном меню выберите команду **Подключиться к другому компьютеру**. В открывшемся диалоговом окне **Выбор компьютера** установите переключатель **другой компьютер** и введите имя требуемого компьютера в соответствующее поле, после чего нажмите кнопку **OK**.
2. Разверните узел **Планировщик заданий**, затем подузел **Библиотека планировщика заданий**, а в нем другие необходимые подузлы.

3. При выборе в дереве консоли папки заданий, в ней по умолчанию выбирается первое задание. Если папка содержит несколько заданий, выберите в ней требуемое задание.
4. Свойства выбранного задания можно просматривать на вкладках панели сведений (рис. 10.5).

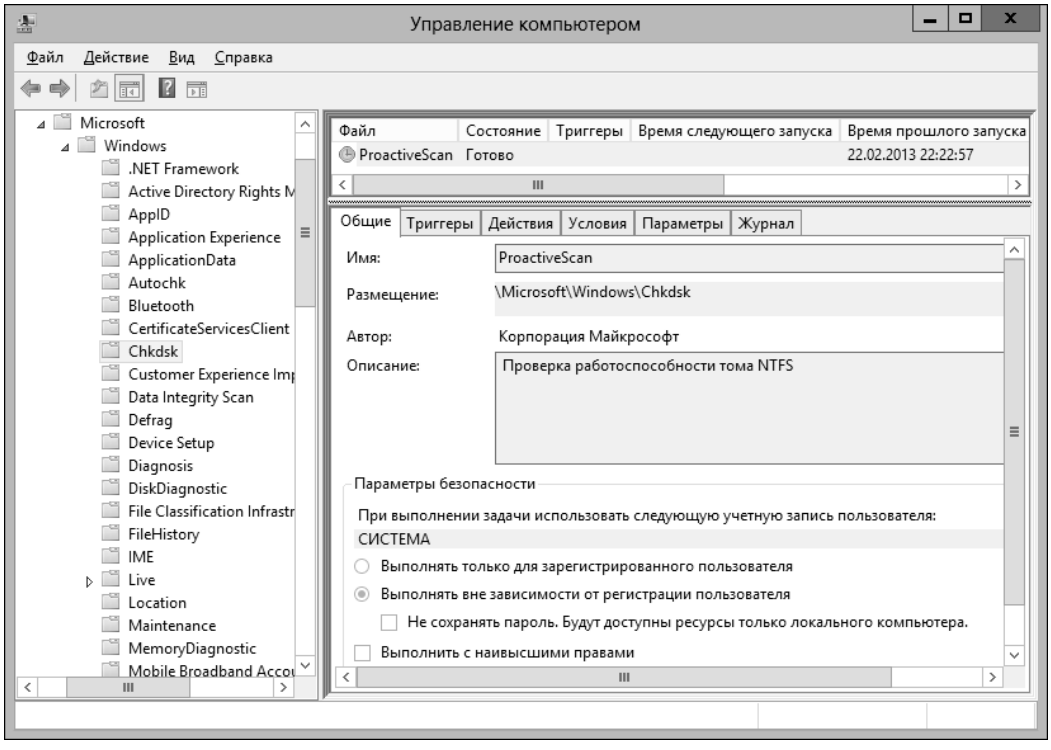


Рис. 10.5. Просмотр и управление запланированными заданиями

Для работы с заданием щелкните по нему правой кнопкой мыши в основной панели и в контекстном меню выберите одну из следующих команд:

- **Удалить** (Delete) — полностью удалить задание;
- **Отключить** (Disable) — временно отключить задание;
- **Свойства** (Properties) — просмотреть и/или редактировать свойства задания. После внесения требуемых изменений в свойства задания нажмите кнопку **OK**, чтобы применить их;
- **Экспортировать** (Export) — экспортировать задание в файл, который можно импортировать на другой компьютер. После экспортирования задания подключите к консоли **Управление компьютером** другой компьютер, как было рассмотрено ранее в этом разделе, щелкните правой кнопкой мыши по узлу **Библиотека планировщика заданий** и в контекстном меню выберите команду **Импортировать задачу** (Import task). В открывшемся окне навигации по файловой системе укажите местонахождение экспортированного файла и сам файл и нажмите кнопку **Открыть**;
- **Выполнить** (Run) — запустить задачу на выполнение;
- **Завершить** (End) — если задача выполняется, остановить ее выполнение.

Примечание

Хотя созданные пользователями задания можно без особых проблем изменять и/или удалять, с большинством заданий, созданных операционной системой, этого делать нельзя. Чтобы отобразить системные задания, разверните меню **Вид** и установите флажок **Отобразить скрытые задачи** (Show hidden tasks). Обратите внимание, что при экспортировании заданий указать операционную систему, с которой это задание можно использовать, можно с помощью параметра **Настроить для** (Configure for) на вкладке **Общие** окна свойств задания. Операционные системы Windows 8 и Windows Server 2012 имеют такую же архитектуру заданий, как и Windows 7 и Windows Server 2008 R2, но архитектура заданий более ранних версий Windows другая.

Просмотреть запланированные задания, исполняющиеся на компьютере в настоящее время, можно таким образом:

1. Откройте консоль **Управление компьютером**. По умолчанию консоль подключена к локальному компьютеру. Для работы с заданиями удаленных компьютеров щелкните правой кнопкой мыши по корневому узлу **Управление компьютером** в дереве консоли (левая панель) и в контекстном меню выберите команду **Подключиться к другому компьютеру**. В открывшемся диалоговом окне **Выбор компьютера** установите переключатель **другой компьютер** и введите имя требуемого компьютера в соответствующее поле, после чего нажмите кнопку **OK**.
2. Щелкните правой кнопкой мыши по узлу **Планировщик заданий** и в контекстном меню выберите команду **Отображать все выполняемые задачи** (Display all running tasks).

Создание планируемых заданий

Планируемое задание можно создать следующим способом:

1. Откройте консоль **Управление компьютером**. По умолчанию консоль подключена к локальному компьютеру. Чтобы создать задания на удаленном компьютере, щелкните правой кнопкой мыши по корневому узлу **Управление компьютером** в дереве консоли (левая панель) и в контекстном меню выберите команду **Подключиться к другому компьютеру**. В открывшемся диалоговом окне **Выбор компьютера** установите переключатель **другой компьютер** и введите имя требуемого компьютера в соответствующее поле, после чего нажмите кнопку **OK**.
2. Выберите, а затем щелкните правой кнопкой мыши по узлу **Планировщик заданий** и в контекстном меню выберите команду **Создать задачу** (Create Task). Запустится мастер создания задачи.
3. На вкладке **Общие** окна мастера введите имя задания и установите параметры безопасности для его выполнения.
   - Если задание должно выполняться по иной учетной записи, чем учетная запись текущего пользователя, нажмите кнопку **Изменить** (Change User or Group). В открывшемся диалоговом окне **Выбор: "Пользователь" или "Группа"** (Select User or Group) выберите пользователя или группу, с чьей учетной записью нужно выполнять задание, а затем предоставьте необходимые учетные данные.
   - Установите другие требуемые параметры, используя предоставленные для этого опции. По умолчанию задания исполняются, только если пользователь выполнил вход в систему. Чтобы выполнять задачу независимо от того, работает пользователь в системе или нет, установите переключатель **Выполнять вне зависимости от регистрации пользователя** (Run whether user is logged on or not). Также можно задать выполнение задания с наивысшими полномочиями и/или настроить его для определенных версий Windows.

4. На вкладке **Триггеры** создайте и настройте триггеры, используя доступные опции. Чтобы создать триггер, нажмите кнопку **Создать**, в открывшемся окне **Создание триггера** задайте необходимые параметры триггера, после чего нажмите кнопку **OK**.
5. На вкладке **Действия** создайте и настройте требуемые действия, используя предоставленные опции. Чтобы создать действие, нажмите кнопку **Создать**, в открывшемся окне **Создание действия** задайте необходимые параметры действия, после чего нажмите кнопку **OK**.
6. На вкладке **Условия** укажите условия для запуска и остановки выполнения задания.
7. На вкладке **Параметры** укажите требуемые дополнительные параметры для задания.
8. Выполнив все требуемые настройки, нажмите кнопку **OK**, чтобы создать задание.

Диагностирование планируемых заданий

В процессе настройки заданий можно столкнуться с несколькими типами проблем. Например, некоторые задания не будут запускаться, когда им положено, а другие, наоборот, не будут останавливаться. Чтобы определить статус задания, выберите требуемое задание в **Планировщике заданий** и просмотрите требуемые сведения, такие как состояние, время прошлого запуска, результат последнего запуска и т. п. Состояние **Поставлено в очередь** (Queued) означает, что задание ожидает выполнения в запланированное время. Состояние **Готово** означает, что задание готово к следующему выполнению. Если задание должно выполняться автоматически, но в его столбце времени последнего запуска указано **Никогда** (Never), следует проверить свойства задания, чтобы определить, почему оно не выполняется. Если при последнем выполнении задания произошла ошибка, необходимо исправить указанную проблему, чтобы задание могло исполняться должным образом.

Чтобы проверить свойства задания, выберите его в **Планировщике заданий**. Вкладка **Журнал** (History) содержит подробную информацию о задании, от его создания до последнего исполнения. Используйте это информацию в диагностировании проблемы с заданием.

Задание, чье состояние указывается как **Работает**, может в действительности не выполняться, а быть зависшим. Узнать, действительно ли задание зависло, можно, проверив столбец **Время прошлого запуска** (Last Run Time), в котором указано время запуска задания. Если задание исполняется свыше одного дня, это обычно означает проблему. Возможно, что сценарий ожидает ввод, задание столкнулось с проблемой чтения или записи файлов, или же задание, может, просто "пошло вразнос" и его нужно остановить. Чтобы остановить задание, щелкните на нем правой кнопкой мыши в **Планировщике заданий** и в контекстном меню выберите команду **Завершить**.

Создание резервной копии и восстановление системы

Операционная система Windows 8 содержит инструмент **История файлов** (File History) для создания резервной копии и восстановления личных файлов. Открыть эту консоль можно, щелкнув в разделе **Система и безопасность** Панели управления по ссылке **Сохранение резервных копий файлов с помощью истории файлов** (Save backup copies of your files with File History). Предыдущие версии файлов и папок можно также создавать для общих сетевых папок файловых серверов. Для создания резервной копии и восстановления данных компьютера также применяются такие инструменты, как **Восстановление запуска** (Startup Repair), **Загрузчик возобновления Windows** (Windows Resume Loader) и **Восстановление**

системы (System Restore). Эти инструменты рассматриваются в последующих разделах этой главы.

Создание резервной копии и восстановление файлов и папок с помощью средства *Предыдущие версии*

Файловые серверы под управлением Windows Server 2012 обладают функциональностью **Предыдущие версии**. Предыдущие версии файлов получаются из теневых копий для сетевых папок. Хотя функциональность предыдущих версий не является заменой полноценному резервному копированию системы, ее можно использовать для автоматического создания резервных копий изменяемых файлов и папок на отслеживаемых дисках. Если отслеживаемый файл или папка были случайно удалены или повреждены, их можно восстановить к предыдущей версии.

Окно свойств сетевой папки (которое можно открыть, щелкнув по ней в Проводнике Windows правой кнопкой мыши и выбрав в контекстном меню команду **Свойства**) имеет вкладку **Предыдущие версии** (Previous Versions). Эта вкладка содержит список доступных предыдущих версий файлов или папок (если таковые имеются). С предыдущими версиями можно выполнять следующие действия:

- открывать (нажав кнопку **Открыть**);
- копировать (нажав кнопку **Копировать**);
- восстанавливать файл или папку выбранной предыдущей версией (нажав кнопку **Восстановить**).

Предыдущие версии файлов могут отсутствовать на компьютере по нескольким причинам, включая следующие.

- Файл может быть *автономным*. Автономные файлы представляют собой копии сетевых файлов. Клиентские компьютеры не создают предыдущих версий автономных файлов. Но предыдущие версии могут присутствовать на сервере, где хранится исходный файл.
- Файл может быть *системным*. Функциональность **Предыдущие версии** не создает копий системных файлов.
- Папка, в которой файл был сохранен, была удалена. В таком случае нужно открыть окно свойств папки, которая содержала удаленную папку. Восстановите удаленную папку с вкладки **Предыдущие версии** папки, в которой она находилась, а затем откройте окно свойств восстановленной папки, чтобы восстановить находящийся в ней требуемый файл.
- Со времени создания или сохранения файла не было создано теневой копии.

Восстановление после сбоя запуска

Когда компьютер под управлением Windows 8 не выходит из режима сна или гибернации, диспетчер загрузки Windows инициализирует операционную систему, запуская загрузчик Windows, который в свою очередь запускает операционную систему, используя информацию из хранилища BCD. В случае сбоя запуска Windows 8, при следующей попытке запуска компьютера выводится экран восстановления. На этом экране можно выбрать опцию **Перезагрузить компьютер** (Restart my PC), чтобы выключить и снова включить компьютер, или опцию **Дополнительные параметры восстановления** (See advanced repair options) для вывода дополнительных опций, с помощью которых можно попытаться восстановить компьютер.

Среди прочих доступны следующие дополнительные параметры восстановления:

- **Продолжить** (Continue) — выйти из меню восстановления и продолжить загрузку операционной системы;
- **Использовать другую ОС** (Use another operating system) — выйти из меню восстановления и выбрать операционную систему для загрузки;
- **Выключить компьютер** (Turn off your PC) — выйти из меню восстановления и выключить компьютер;
- **Диагностика** (Troubleshoot) — выводит меню диагностики.

Меню диагностики содержит следующие опции.

- **Восстановить** (Refresh your PC). Эта возможность, которая впервые применена в Windows 8, переустанавливает операционную систему из ее образа, сохраненного на жестком диске, при этом личные файлы, учетные записи и персональные настройки пользователей сохраняются. Но если приложения рабочего стола и их настройки также сохраняются после восстановления, все ранее установленные настольные программы будут утеряны.
- **Вернуть в исходное состояние** (Reset your PC). Эта возможность, которая впервые применена в Windows 8, тоже переустанавливает операционную систему из образа, хранящегося на жестком диске, но сбрасывает ее конфигурацию к исходному, "фабричному", состоянию. Все личные файлы, учетные записи и персональные настройки пользователей теряются, как приложения рабочего стола, настольные приложения и их настройки.
- **Дополнительные параметры** (Advanced options). Открывает меню дополнительных параметров.

Меню дополнительных параметров содержит следующие пять опций.

- **Восстановление системы** (System Restore). Восстановление системы с использованием ранее созданной точки восстановления. Этот процесс рассматривается более подробно в *разд. "Создание резервной копии и восстановление состояния системы, используя средство Восстановление системы" далее в этой главе*.
- **Восстановление образа системы** (System Image Recovery). Восстановление системы, используя ее образ. Этот процесс подобен процессу возвращения компьютера в исходное состояние с той разницей, что можно выбирать образ для восстановления и файл образа может находиться на удаленном компьютере. Все личные файлы, учетные записи и персональные настройки пользователей теряются, как и приложения рабочего стола, настольные приложения и их настройки (за исключением тех, которые содержатся в восстанавливаемом образе).
- **Автоматическое восстановление** (Automatic Repair). Запускает инструмент **Автоматическое восстановление**, который может исправить проблемы, не позволяющие запуск операционной системы, включая поврежденные записи в хранилище BCD, системные файлы и диспетчеры загрузки. Обычно этот инструмент запускается автоматически самой операционной системой, если она обнаруживает исправимую проблему.
- **Командная строка** (Command prompt). Предоставляет доступ к консоли командной строки, где можно использовать команды и инструменты среды восстановления.
- **Параметры загрузки** (Startup Settings). Разрешает изменить параметры загрузки операционной системы. Эта опция позволяет, среди прочего, перезагрузить компьютер, чтобы можно было отключить принудительную проверку подписи драйверов, запустить защитное программное обеспечение на ранних этапах загрузки или выполнить автоматическую перезагрузку при сбое системы. Также можно включить режим низкого разрешения экрана, режим отладки, ведение журнала загрузки и безопасный режим.

Восстановление после сбоя возобновления

При переходе компьютера под управлением Windows 8 в режим сна или гибернации создается снимок текущего состояния системы. В случае перехода в режим сна этот снимок сохраняется в оперативной памяти компьютера, откуда он считывается при выводе компьютера из режима сна. А в случае режима гибернации снимок состояния сохраняется на жестком диске, и при переводе системы в штатный режим ее состояние восстанавливается из этого снимка. Обе эти операции выполняются загрузчиком возобновления Windows.

Проблемы с возобновлением штатной работы компьютера могут возникать по разным причинами, включая ошибки при создании снимка состояния системы, физические ошибки памяти и физические ошибки диска. В случае проблем с возобновлением штатной работы системы из режима сна загрузчик возобновления Windows загружает операционную систему, как при обычной загрузке, без данных, сохраненных в снимке состояния при переходе в спящий режим. В случае проблем с возобновлением штатной работы системы из режима гибернации загрузчик возобновления Windows загружает операционную систему, как при обычной загрузке, без данных, сохраненных в снимке состояния при переходе в режим гибернации.

Как можно видеть, в любом случае все данные, которые не были сохранены перед переходом компьютера в режим сна или гибернации, теряются. Но большинство современных приложений могут автоматически сохранять свое рабочее состояние при переходе компьютера в состояние сна. В результате при перезапуске приложений, исполняющихся при переходе в режим сна, может быть возможным восстановить данные этих приложений.

После неудачного возобновления средство **Автоматическое восстановление** может исследовать недавние изменения в конфигурации, которые повлияли на состояние сна или гибернации, и аннулировать их. Например, если действующий план электропитания был отредактирован, чтобы компьютер переходил в режим гибернации после определенного периода сна, средство **Автоматическое восстановление** может отменить это изменение.

Восстановление возможности запуска системы

Для правильного запуска компьютерам под управлением Windows 8 требуется доступ к определенным системным файлам. Если компьютер не может запуститься вследствие повреждения или отсутствия какого-либо системного файла, это можно исправить с помощью средства **Автоматическое восстановление**. Но иногда исправления поврежденного или восстановление отсутствующего файла не решает все проблемы с запуском компьютера. В таком случае необходимо продолжать диагностирование, чтобы определить более глубокую причину проблемы.

Причиной большинства других проблем запуска являются изменения в системе, например неправильная установка устройства. Также возможно неправильное выполнение конфигурации системы или редактирование реестра, вследствие чего в системе возник конфликт ресурсов. Проблемы запуска системы часто можно решить, используя для диагностирования проблемы или восстановления системы безопасный режим загрузки. Завершив работу в безопасном режиме, обязательно перезапустите компьютер в штатном режиме. Тогда можно будет использовать компьютер обычным образом.

При запуске в безопасном режиме Windows 8 загружает только основные файлы, службы и драйверы. В частности, в число загружаемых драйверов входят драйверы для мыши, монитора, клавиатуры, приводов дисков и базового видео. Драйвер монитора задает базовые параметры и режимы для монитора компьютера, а видеодрайвер устанавливает базовые параметры видеоадаптера компьютера. Для сетевого оборудования драйверы не загружаются и

не запускаются сетевые службы, если только не была выполнена загрузка в безопасном режиме с загрузкой сетевых драйверов. Ограниченный объем конфигурационной информации, загружаемой в безопасном режиме, может способствовать диагностированию проблем.

Загрузка системы в безопасном режиме выполняется следующим образом:

1. В случае проблем с обычной загрузкой операционной системы при запуске компьютера выводится экран **Восстановление**. На этом экране выберите опцию **Дополнительные параметры восстановления**, а на следующем экране — опцию **Диагностирование**.
2. На экране **Диагностирование** выберите опцию **Дополнительные параметры** (Advanced options), а на следующем экране — опцию **Параметры загрузки**.
3. На экране **Параметры загрузки** (Startup Settings) нажмите кнопку **Перезагрузить**.
4. С помощью стрелок вверх и вниз выберите требуемый тип безопасного режима, а затем нажмите клавишу <Enter>. Выбор типа безопасного режима зависит от типа проблемы. Доступны следующие основные опции.
   - **Устранение неполадок компьютера** (Repair Your Computer). Загружает инструмент **Восстановление запуска** (Startup Repair). Эту опцию следует выбирать в том случае, когда нужно исправить проблемы с запуском Windows, включая поврежденные записи в хранилище BCD, системные файлы и диспетчеры загрузки. Обычно этот инструмент запускается автоматически самой операционной системой, если она обнаруживает исправимую проблему запуска.
   - **Безопасный режим** (Safe Mode). В процессе инициализации системы загружаются только основные файлы, службы и драйверы. В частности, в число загружаемых драйверов входят драйверы для мыши, монитора, клавиатуры, приводов дисков и базового видео. Сетевые драйверы не загружаются и сетевые службы не запускаются.
   - **Безопасный режим с загрузкой сетевых драйверов** (Safe Mode with Networking). Загружаются основные файлы, драйверы и службы, а также драйверы и службы, необходимые для обеспечения сетевых возможностей.
   - **Безопасный режим с поддержкой командной строки** (Safe Mode with Command Prompt). Загружаются основные файлы, службы и драйверы, но вместо графического интерфейса Windows 8 запускается консоль командной строки. Сетевые драйверы не загружаются и сетевые службы не запускаются.

     Совет

     В **Безопасном режиме с поддержкой командной строки** можно запустить оболочку Проводника Windows. Для этого нужно открыть диспетчер задач, нажав комбинацию клавиш <Ctrl>+<Shift>+<Esc>. Затем в окне диспетчера задач в меню **Файл** выбрать опцию **Запустить новую задачу** (Run new task). В поле **Открыть** открывшегося диалогового окна **Создание задачи** (Create new task) следует ввести команду `explorer.exe` и нажать кнопку **OK**.

   - **Ведение журнала загрузки** (Enable boot logging). Позволяет записывать все события запуска в журнал загрузки.
   - **Включение видео режима с низким разрешением** (Enable low-resolution video). Позволяет запустить систему с разрешением экрана 640×480 пикселов, что может быть полезным, если текущее разрешение видеоадаптера не поддерживается используемым монитором.
   - **Отключить автоматическую перезагрузку при отказе системы** (Disable automatic restart after failure). Предотвращает перезапуск Windows после сбоя. В противном случае после сбоя Windows будет автоматически перезапускаться. Причиной постоянных перезапусков системы может быть проблема с настройкой параметров микропрограммного обеспечения *(см. главу 4)*.

- **Отключение обязательной проверки подписи драйверов** (Disable driver signature enforcement). Компьютер запускается в безопасном режиме с отключенной функциональностью проверки подписи драйверов. Если причиной проблемы загрузки является недействительная или отсутствующая подпись драйвера, таким образом можно временно решить эту проблему, чтобы можно было запустить компьютер и решить ее полностью, заполучив новый драйвер с правильной подписью или изменив параметры проверки подписи драйверов.
- **Отключение раннего запуска антивредоносного драйвера** (Disable early launch anti-malware protection). Компьютер запускается в безопасном режиме без запуска драйвера антивредоносного программного обеспечения для защиты компьютера на этапе загрузки. Если драйвер загрузки антивредоносного программного обеспечения компьютера создает проблему запуска, следует проверить наличие обновления на веб-сайте разработчика этого программного обеспечения, которое может разрешить проблему загрузки системы, или же настроить его без защиты загрузки.
- **Обычная загрузка Windows** (Start Windows Normally). Компьютер запускается с обычными параметрами загрузки.

5. Если проблема не проявляется при работе в безопасном режиме, параметры по умолчанию и основные драйверы устройств можно устранить, как ее возможные причины. Если проблема с запуском системы вызывается обновленным драйвером или драйвером нового устройства, систему можно загрузить в безопасном режиме, чтобы удалить устройство, отменить обновление или же установить другую версию драйвера.
6. Если проблема не решается таким образом и подозрение падает на аппаратное или программное обеспечение или настройки параметров, загрузите компьютер в безопасном режиме, а затем воспользуйтесь средством восстановления системы, чтобы отменить предыдущие изменения. Сведения о восстановлении системы *см. в разд. "Создание резервной копии и восстановление состояния системы, используя средство Восстановление системы" далее в этой главе*.
7. Если восстановление системы не дает желаемого результата, попробуйте изменить параметры загрузки, как рассматривается в *разд. "Управление конфигурацией, запуском и загрузкой системы" главы 2*.

Создание резервной копии и восстановление состояния системы, используя средство *Восстановление системы*

В *разд. "Вкладка Защита системы" главы 2* было представлено средство **Восстановление системы**, а также рассмотрена настройка этой функциональности. Для восстановления системы, которая испытывает проблемы после обновления, установки программного или аппаратного обеспечения или других изменений, можно использовать *точки восстановления*. В следующих разделах мы рассмотрим ручное создание точек восстановления и их применение для восстановления состояния системы. В большинстве случаев операции восстановления из контрольных точек являются обратимыми.

Принципы точек восстановления

Функциональность восстановления системы отслеживает изменения в операционной системе и создает точки восстановления через регулярные интервалы в течение дня и перед внесением изменений. Точка восстановления представляет собой снимок состояния конфигурации компьютерной системы. Этот снимок сохраняется на диске и может быть впоследст-

вии использован для восстановления состояния системы к моменту времени, когда он был сделан. Важно отметить, что функциональность восстановления системы не затрагивает личные данные. Иными словами, состояние системы можно восстановить к определенной точке в прошлом, но при этом данные приложений пользователя, кэшированные файлы или документы остаются в том же состоянии. Также никакие данные не записываются в папку **Документы**.

Функциональность восстановления системы отслеживает и сохраняет конфигурационную информацию отдельно для каждого жесткого диска компьютера, для чего на каждом из отслеживаемых дисков для этой функциональности зарезервировано определенное дисковое пространство. Эту возможность можно также включать и отключать для каждого отдельного диска. Если для диска включено восстановление системы, в случае проблем его состояние можно восстановить. Если же для определенного диска защита системы не включена, изменения в конфигурации системы для этого диска не отслеживаются, вследствие чего в случае проблем восстановление системной конфигурации для этого диска будет невозможным. На большинстве систем восстановление системы следует включать для системного диска, на котором находятся файлы ОС, и для тех дисков, на которых находятся важные приложения.

Точки восстановления создаются трех типов: контрольные точки, по дате и по событию. Точки восстановления, создаваемые операционной системой по регулярным запланированным интервалам, называются *системными контрольными точками*. Обычные системные контрольные точки создаются приблизительно через каждые 24 часа. Если в то время, когда запланировано создание системной контрольной точки, компьютер выключен, контрольная точка создается при следующем включении компьютера.

> ***Примечание***
>
> Хотя предыдущие версии Windows создавали начальную контрольную точку после установки операционной системы, Windows 8 обычно этого не делает. Причиной этому является наличие в Windows 8 опций **Восстановить** и **Вернуть в исходное состояние** для возвращения системы к исходному состоянию. Дополнительную информацию об этих опциях *см. в разд. "Восстановление после сбоя запуска" ранее в этой главе*.

При включенной функциональности восстановления системы некоторые точки восстановления создаются автоматически, на основе событий, активируемых операционной системой при установке или изменении приложений. Эти снимки состояния для простоты можно называть *событийными точками восстановления*. Существует несколько подвидов таких точек, каждый из которых имеет свое назначение.

- **Точки восстановления до установки программы.** Эти точки восстановления создаются перед установкой программ и используются в случае необходимости для восстановления компьютера к состоянию, в котором он был до установки программы. Под восстановлением состояния компьютера имеется в виду, что удаляются все файлы и параметры реестра для затрагиваемой программы и что остальные программы и системные файлы, измененные при установке этой программы, возвращаются к их исходному состоянию. По завершению восстановления с такой точки восстановления затрагиваемая программа не будет работать, и если она понадобится какому-либо пользователю, то ее нужно будет установить снова (приняв, конечно же, должные меры, чтобы не повторилась ситуация, вынудившая прибегать к восстановлению системы после первой ее установки).

> ***Осторожно!***
>
> Не следует путать восстановление системы к состоянию до установки программы с удалением этой программы. Процесс восстановления не удаляет все файлы приложения, а просто удаляет

те файлы и параметры реестра, которые влияют на работу компьютера. Чтобы полностью удалить программу, нужно воспользоваться опцией **Удаление программы** в Панели управления.

- **Точки восстановления после автоматических обновлений.** Создаются перед применением автоматических обновлений и используются в случае необходимости для восстановления компьютера к состоянию, в котором он был до применения обновления. (Удалить автоматическое обновление можно также с помощью опции **Удаление обновления** в Панели управления.)
- **Точки восстановления после операций восстановления.** Создаются перед выполнением восстановления системы. Если, например, была использована неправильная точка восстановления или выполненное восстановление не исправило проблему, с помощью этих точек восстановления компьютер можно возвратить к состоянию, в котором он был до выполнения предыдущего восстановления.
- **Точки восстановления после установки неподписанных драйверов.** Создаются перед установкой на компьютер неподписанных или несертифицированных драйверов и используются в случае необходимости для восстановления компьютера к состоянию, в котором он был до установки проблемного драйвера. Для возвращения к предыдущему состоянию после установки подписанных или сертифицированных драйверов обычно достаточно выполнить откат установленного драйвера.
- **Точки восстановления после применения средства защиты и восстановления Майкрософт.** Создаются перед восстановлением файлов или системных данных с помощью средства защиты и восстановления Microsoft. В случае неудачного восстановления его можно отменить с помощью такой точки восстановления и возвратить компьютер к его предыдущему состоянию.

Кроме этого, точки восстановления могут создаваться пользователями вручную. Такие снимки состояния системы называются, соответственно, *ручными точками восстановления*. Администраторы должны рекомендовать своим пользователям создавать ручные точки восстановления перед тем, как выполнять операции, которые могут повлиять на нормальное функционирование системы.

Восстановление системы можно выполнять при работе компьютера в штатном режиме или в режиме безопасности. В штатном режиме перед выполнением восстановления создается точка восстановления после операции восстановления. Но при восстановлении в безопасном режиме такая точка восстановления не создается, т. к. в этом режиме изменения в системе не отслеживаются. Но в этом режиме можно выполнять восстановления к любой ранее созданной точке восстановления.

Создание ручных точек восстановления

Ручную точку восстановления можно создать таким способом:

1. В Панели управления щелкните по ссылке **Система и безопасность** и в открывшемся списке элементов этой категории выберите ссылку **Система**.
2. В левой панели окна **Система** щелкните по ссылке **Защита системы**.
3. В открывшемся диалоговом окне **Свойства системы** в разделе **Параметры защиты** на вкладке **Защита системы** выберите жесткий диск, для которого нужно создать точку восстановления, а затем нажмите кнопку **Создать**.
4. В открывшемся диалоговом окне **Защита системы** введите название для создаваемой точки восстановления. Рекомендуется указывать смысловое название, отражающее обстоятельства создания точки восстановления, например, `Перед обновлением драйвера видеоадаптера`. Нажмите кнопку **Создать**.

5. После завершения создания точки восстановления нажмите кнопку **Закрыть**, а в окне свойств системы — кнопку **OK**.

Восстановление из точек восстановления

Выполнить восстановление системы из точки восстановления при доступной операционной системе можно следующим образом:

1. В Панели управления щелкните по ссылке **Система и безопасность** и в открывшемся списке элементов этой категории выберите ссылку **Система**.
2. В левой панели окна **Система** щелкните по ссылке **Защита системы**, а в открывшемся диалоговом окне свойств системы нажмите кнопку **Восстановить**. Средство восстановления проверит наличие точек восстановления системы, что может занять несколько минут, после чего откроется окно **Восстановление системы** с установленным переключателем **Рекомендуемое восстановление** (Recommended restore). Чтобы определить, какие программы будут затронуты операцией восстановления, нажмите кнопку **Поиск затрагиваемых программ** (Scan for affected programs).
3. Если требуется выполнить восстановление из другой точки восстановления, а не той, которая рекомендуется системой, установите переключатель **Выбрать другую точку восстановления** (Choose a different restore point) и нажмите кнопку **Далее**. Следующее окно содержит список доступных точек восстановления, упорядоченных по дате и времени и с описанием и типом для каждой точки. Чтобы просмотреть другие доступные точки восстановления, отметьте флажок **Показать другие точки восстановления** (Shoe more restore points). Чтобы определить, какие программы будут затронуты восстановлением с выбранной точки восстановления, нажмите кнопку **Поиск затрагиваемых программ**.
4. Выбрав требуемую точку восстановления, нажмите кнопку **Далее**, чтобы продолжить выполнение операции восстановления.
5. В следующем окне нажмите кнопку **Готово**. Далее, в окне предупреждения о невозможности прервать операцию восстановления подтвердите свое намерение выполнить восстановление, нажав кнопку **Да**.

Выполнить восстановление системы из точки восстановления при неработающей операционной системе можно следующим образом:

1. В случае проблем с обычной загрузкой операционной системы, при запуске компьютера выводится экран **Восстановление**. На этом экране выберите опцию **Дополнительные параметры восстановления**, а в следующем экране — опцию **Диагностирование**.
2. На экране **Диагностика** выберите опцию **Дополнительные параметры**, а затем — опцию **Восстановление системы**.
3. Средство восстановления проверит наличие точек восстановления системы, после чего будет предоставлена возможность выбрать точку восстановления и выполнить восстановление в процедуре, подобной описанной в шагах 4—5 предыдущей процедуры.

В процессе восстановления работа операционной системы Windows 8 прекращается. После завершения восстановления Windows 8 перезапускается с параметрами, используемыми в момент создания выбранной точки восстановления. После перезапуска системы после восстановления снова выводится диалоговое окно **Восстановление системы**, информирующее об успешном выполнении восстановления. Закройте его, нажав кнопку **Закрыть**. Теперь система готова к работе. Если после выполнения восстановления Windows 8 не работает должным образом, можно осуществить восстановление из другой точки или отменить выполненное восстановление, повторив процедуру восстановления и выбрав для нее точку восстановления, созданную перед выполнением предыдущего восстановления.

Устранение проблем с восстановлением системы

Процесс восстановления системы не всегда завершается успешно. Если средству восстановления системы не удалось возвратить систему к требуемому состоянию, можно попытаться восстановить компьютер, повторив процедуру восстановления, но на этот раз выбрав другую точку восстановления.

Создание и использование истории файлов

Средство **История файлов** можно использовать, чтобы автоматизировать процесс создания резервных копий персональных файлов из библиотек, с рабочего стола, контактов и закладок. Для создания резервной копии и восстановления файлов учетная запись пользователя должна обладать соответствующими полномочиями.

Настройка средства резервного копирования *История файлов*

Операционная система Windows 8 может автоматически выполнять резервное копирование данных пользователя. С помощью средства **История файлов** можно периодически создавать резервную копию файлов изображений, аудио, видео, сообщений электронной почты, текстовых документов и многих других типов файлов, чтобы в случае необходимости восстановить их или же перенести и использовать их на другом компьютере. В частности, резервная копия создается для подпапок **Общие документы**, **Общие изображения** и **Общие видео** папки **Пользователи\Общие** (Users\Public), а также подпапок **Контакты**, **Рабочий стол**, **Мои документы**, **Избранное**, **Изображения**, **Моя музыка** и **Мои видео** папки профиля пользователя.

Открыть окно средства **История файлов** (рис. 10.6) можно из Панели управления, щелкнув в разделе **Система и безопасность** по ссылке **Сохранение резервных копий файлов с помощью истории файлов** (Save backup copies of your files with File History).

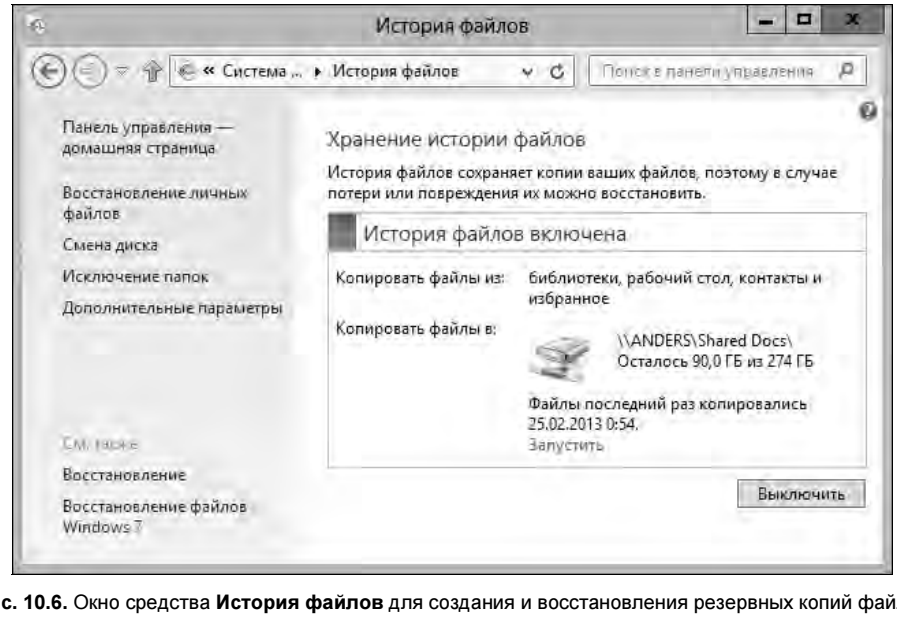


Рис. 10.6. Окно средства **История файлов** для создания и восстановления резервных копий файлов данных пользователя

При работе со средством **История файлов** нужно иметь в виду следующее:

- резервные копии файлов пользователя можно сохранять только на съемных носителях или в сетевых папках. Их нельзя сохранять на внутренних жестких дисках компьютера;
- резервные копии данных пользователя создаются автоматически при включенном средстве **История файлов**. По умолчанию резервная копия создается каждый час;
- также по умолчанию резервные копии сохраняются в течение неограниченного времени при условии, что их объем не превышает 5% объема диска, на котором они хранятся.

При хранении резервных копий данных пользователя на сетевых дисках для них создается папка, название которой имеет формат *Имя_пользователя@Домен_или_компьютер*. Например, Williams@Cpandl.com или WilliamS@CorpPC12. Эта папка содержит подпапку, которой присвоено имя компьютера пользователя, например CORPC12; эта папка в свою очередь содержит вложенные папки Configuration и Data. В случае хранения резервной копии данных пользователя на съемном носителе, сначала создается папка верхнего уровня с именем FileHistory.

Включение функциональности *История файлов* и настройка носителей хранения

При использовании для хранения резервных копий данных пользователя USB-флешек или других съемных носителей включение функциональности автоматического создания резервной копии и первое резервное копирование выполняется следующим образом:

1. Подсоедините флешку или другой съемный носитель к компьютеру.
2. В Панели управления в разделе **Система и безопасность** щелкните по ссылке **Сохранение резервных копий файлов с помощью истории файлов**.
3. В открывшемся окне **История файлов** нажмите кнопку **Включить** (Turn on). Система включит функциональность **История файлов** и создаст первую резервную копию.

При использовании для хранения резервных копий данных сетевых дисков включение функциональности автоматического создания резервной копии и первое резервное копирование выполняется следующим образом:

1. В Панели управления в разделе **Система и безопасность** щелкните по ссылке **Сохранение резервных копий файлов с помощью истории файлов**.
2. В левой панели окна **История файлов** щелкните по ссылке **Смена диска** (Select drive), а затем в окне **Выбор диска** нажмите кнопку **Добавить сетевое расположение** (Add network location). Если выводится сообщение, что сетевое обнаружение отключено, щелкните на этом сообщении, а в контекстном меню выберите команду **Включить сетевое обнаружение и общий доступ к файлам** (Turn on network discovery and file sharing).
3. В диалоговом окне **Выбор папки** (Select Folder) в поле **Папка** введите путь в формате UNC к папке, в которой следует хранить резервную копию данных пользователя, например \\CorpServer172\CorpData, а затем нажмите кнопку **Выбор папки**.
4. Выбрав сетевой диск, нажмите кнопку **OK**, чтобы возвратиться обратно в окно **История файлов**, и здесь щелкните по ссылке **Запустить**. Система включит функциональность **История файлов** и создаст первую резервную копию.

С помощью опций на странице **История файлов** используемые по умолчанию настройки резервного копирования можно изменить несколькими способами. Каждый пользователь может одновременно иметь только один диск для хранения резервной копии истории фай-

лов. Этот диск можно изменить на другой сетевой диск и Windows позволит перенести резервную копию файлов пользователя со старого диска на новый. Это можно сделать следующим образом:

1. В левой панели окна **История файлов** щелкните по ссылке **Смена диска**, а затем в окне **Выбор диска** нажмите кнопку **Добавить сетевое расположение**.
2. В диалоговом окне **Выбор папки** (Select Folder) в поле **Папка** введите путь в формате UNC к папке, в которой следует хранить резервную копию данных пользователя, например \\CorpServer96\UserData, а затем нажмите кнопку **Выбор папки**. Обратите внимание на то, что указанная папка не может содержать существующую резервную копию персональных данных для этого пользователя.
3. Выбрав сетевую папку, нажмите кнопку **OK**. Нажмите кнопку **Да** в окне запроса на перемещение резервной копии в новое место из старого. Если новое место уже содержит резервную копию данных пользователя, перенос данных не будет выполнен, и нужно нажать кнопку **Да** в окне запроса на подтверждение.

Изменить место сохранения резервной копии данных пользователя с сетевой папки на съемный носитель или с одного съемного носителя на другой можно следующим образом:

1. Подсоедините флешку или другой съемный носитель к компьютеру.
2. В левой панели окна **История файлов** щелкните по ссылке **Смена диска**.
3. В окне **Выбор диска** укажите требуемый сменный носитель, а затем нажмите кнопку **OK**.
4. Нажмите кнопку **Да** в окне запроса на перемещение резервной копии в новое место из старого. Если новое место уже содержит резервную копию данных пользователя, перенос данных не будет выполнен, и будет нужно нажать кнопку **Да** в окне запроса на подтверждение.

Исключение папок из резервной копии *Истории файлов*

По умолчанию резервная копия создается для подпапок **Общие документы**, **Общие изображения** и **Общие видео** папки **Пользователи\Общие** (Users\Public), а также подпапок **Контакты**, **Рабочий стол**, **Мои документы**, **Избранное**, **Изображения**, **Моя музыка** и **Мои видео** папки профиля пользователя. Любую из этих папок можно исключить из резервной копии следующим образом:

1. В Панели управления в разделе **Система и безопасность** щелкните по ссылке **Сохранение резервных копий файлов с помощью истории файлов**.
2. В левой панели окна **История файлов** щелкните по ссылке **Исключение папок** (Exclude folders). Откроется окно **Исключить папки** (Exclude Folders), содержащее список папок личных данных пользователя, уже исключенных из резервного копирования.
3. Чтобы добавить в этот список новую папку, которую требуется исключить, нажмите кнопку **Добавить**. В открывшемся диалоговом окне для навигации по файловой системе выберите требуемую папку, а затем нажмите кнопку **Выбор папки**. Например, чтобы исключить из резервного копирования папку **Общие документы**, разверните в левой панели окна **Выбор папки** узел **Библиотеки**, в нем узел **Документы** и выберите в этом узле папку **Общие документы**, после чего нажмите кнопку **Выбор папки**, а затем кнопку **Сохранить изменения** (Save changes).
4. Если же, наоборот, нужно включить в резервное копирование ранее исключенную папку, выберите ее в списке исключенных папок, нажмите кнопку **Удалить**, а затем кнопку **Сохранить изменения**.

Изменение параметров сохранения по умолчанию

По умолчанию средство **История файлов** сохраняет резервные копии каждый час, и эти версии резервных копий хранятся в течение неограниченного времени при условии, что их объем не превышает 5% объема диска, на котором они хранятся. Эти параметры по умолчанию можно изменить следующим образом:

1. В Панели управления в разделе **Система и безопасность** щелкните по ссылке **Сохранение резервных копий файлов с помощью истории файлов**.
2. В левой панели окна **История файлов** щелкните по ссылке **Дополнительные параметры**. Окно **Дополнительные параметры** содержит значения по умолчанию настроек для сохранения резервных копий папок личных данных пользователя (рис. 10.7).

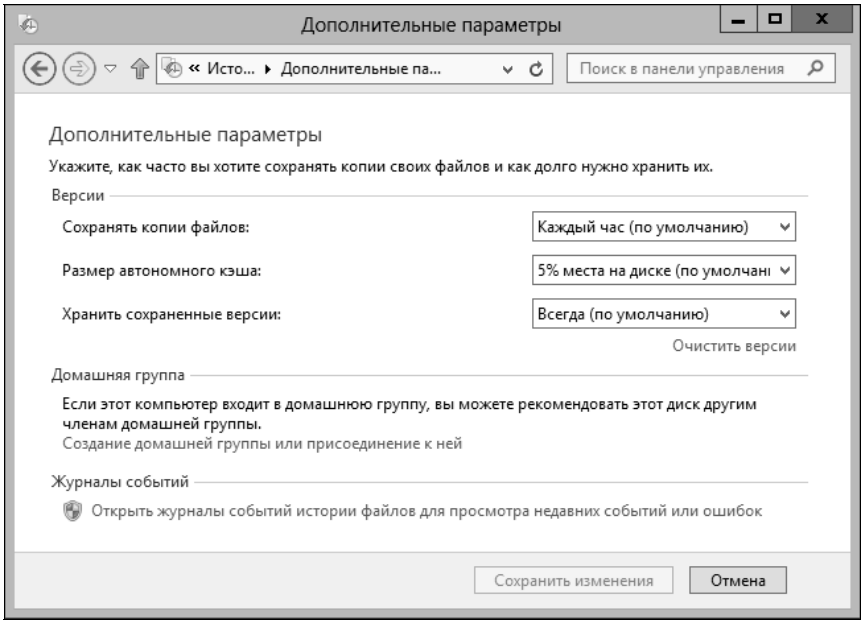


Рис. 10.7. Окно для настройки параметров средства **История файлов**

3. Изменить интервал сохранения резервной копии можно, выбрав требуемое значение в раскрывающемся списке **Сохранять копии файлов** (Save copies of files). Пользователи могут использовать сохраняемые версии как для восстановления, так и для других целей, например, сравнения данных двух разных версий. Уменьшить расход дискового пространства можно, установив более длительный интервал, например, каждые 3 часа или каждые 6 часов. Максимальный интервал между сохранениями составляет 1 день.
4. Настройка максимального объема дискового пространства, используемого для хранения резервной копии, выполняется выбором требуемого значения в раскрывающемся списке **Размер автономного кэша** (Size of offline cache). Обязательно проверьте размер используемого диска и установите это значение соответственно общему объему диска и его свободному пространству. Например, для диска объемом 2 Тбайт этому параметру можно присвоить значение 2%, в то время как для диска объемом 100 Гбайт желательно установить максимальный размер кэша равным 10% от объема диска.

5. Длительность хранения версий резервных копий настраивается выбором требуемого значения в раскрывающемся списке **Хранить сохраненные версии** (Keep saved versions). Здесь следует выбирать значение, соответствующее стилю работы пользователя. Если выбрать **Всегда** (Forever), сохраненные версии резервной копии будут храниться вечно, без перезаписывания при заполнении дискового пространства, выделенного под хранение резервной копии. Если же выбрать опцию **Пока не понадобится место** (Until space is needed), при заполнении выделенного пространства диска, старые версии будут удаляться по мере необходимости, чтобы освободить место для вновь создаваемых резервных копий. При установке любого другого значения из списка, кроме уже описанных, версии резервных копий будут храниться в течение указанного времени, а затем удаляться. Но если при этом выделенное дисковое пространство заполнится, создание новых версий будет невозможным, пока для них не освободится достаточно места (удалением старых копий, достигших предельного срока своего хранения).

Практический совет

На странице **Дополнительные параметры** версии резервной копии можно удалить вручную в любое время. Для этого щелкните в этом окне по ссылке **Очистить версии** (Clean up versions), в открывшемся диалоговом окне **Очистка истории файлов** (File History Cleanup) выберите возраст версий для удаления, а затем нажмите кнопку **Очистить** (Clean up). Например, можно задать удаление версий старше 6 месяцев или всех версий, кроме последней.

Восстановление личных данных пользователя

Восстановить данные личных папок пользователя из резервных копий, сохраненных с помощью средства **История файлов**, можно следующим образом:

1. В Панели управления в разделе **Система и безопасность** щелкните по ссылке **Сохранение резервных копий файлов с помощью истории файлов**.
2. В левой панели окна **История файлов** щелкните по ссылке **Восстановление личных файлов** (Restore personal files). На домашней странице диалогового окна **История файлов** выберите требуемую версию резервной копии для восстановления, перемещаясь по версиям с помощью кнопок **Предыдущая версия** и **Следующая версия** внизу окна. По отображаемым в этом окне папкам можно перемещаться подобно перемещению по ним в Проводнике Windows.
3. Версии резервной копии помечены датой и временем их создания и номером версии (например, `24 февраля 2013г. 14:55 | Версия 5 из 12`). Выбрав требуемый файл или папку для восстановления, нажмите кнопку[1] **Восстановление в исходном расположении** (Restore to the original location). Для восстановления можно также выбрать несколько элементов.

Совет

Файлы и папки также можно восстанавливать в иное, чем их исходное расположение. Для этого нужно после указания элементов для восстановления нажать кнопку **Параметры** (кнопка в виде значка шестеренки) в правом верхнем углу окна восстановления файлов и в контекстном меню выбрать команду **Восстановить в** (Restore to). В открывшемся окне навигации по файловой системе можно будет указать другое место для восстановления выбранных элементов резервной копии личных файлов пользователя.

[1] Круглая кнопка внизу окна, между кнопок перемещения по версиям.

Поиск и устранение неполадок запуска и завершения работы

Администраторам часто приходится диагностировать проблемы с запуском и завершением работы системы. В этом разделе мы рассмотрим методы, которые могут быть полезными в решении распространенных проблем этого типа.

Решение проблем перезапуска и завершения работы

Обычно завершение работы или перезапуск Windows 8 осуществляется посредством выбора соответствующих опций кнопки **Выключение** (Power). Это означает, что для завершения работы или перезагрузки компьютера с экрана **Пуск** или рабочего стола нужно выполнить следующие действия:

1. Откройте кнопочную панель, поместив указатель мыши в правый нижний угол экрана.
2. В открывшейся с правой стороны экрана кнопочной панели нажмите опцию **Параметры**. Откроется панель **Параметры**, на которой нажмите кнопку **Выключение**.
3. В открывшемся контекстном меню нажмите требуемую опцию — **Завершение работы** или **Перезагрузка**.

В стандартной конфигурации также можно нажать физическую кнопку питания компьютера, в результате чего выполняется упорядоченное завершение работы, с выходом пользователя из системы и последующим выключением компьютера. В то время, как эти подходы обычно работают должным образом, иногда операционная система отказывается выключаться или перезагружаться после их применения, и требуется предпринимать дополнительные действия. В случае проблем с выключением или перезагрузкой компьютера вышерассмотренными подходами это можно попытаться сделать следующим образом:

1. Нажмите комбинацию клавиш <Ctrl>+<Alt>+<Del>. Откроется экран меню Windows. Щелкните в этом меню на опции **Диспетчер задач**. Если окно диспетчера задач откроется в сжатом виде, щелкните внизу по его ссылке **Подробнее** (More details).
2. Выберите вкладку **Процессы** и посмотрите, нет ли в списке процесса, чье состояние помечено, как **Не отвечает** (Not responding). Если неотвечающих процессов нет, перейдите к шагу 5.
3. Выберите неотвечающее приложение и нажмите кнопку **Снять задачу** (End task) в правом нижнем углу диспетчера задач.
4. Откроется окно сообщения, что данное приложение не отвечает, предоставляющее выбор немедленного завершения работы приложения или отмены запроса на завершение. Нажмите кнопку **Завершить сейчас**.
5. Попытайтесь выключить или перезагрузить компьютер. Для этого нажмите комбинацию клавиш <Ctrl>+<Alt>+<Del> и на экране меню Windows нажмите кнопку **Завершение работы** в правом нижнем углу, а в открывшемся меню выберите требуемую опцию — **Перезагрузить** или **Завершение работы**.

Кроме этого, при нажатии физической кнопки питания компьютера Windows 8 выполняет выход текущего пользователя и осуществляет упорядоченное выключение компьютера. В таком случае, если какая-либо программа не отвечает, Windows 8 предоставляет пользователю опцию принудительно завершить ее выполнение самому или же подождать несколько секунд, чтобы это сделала Windows 8.

ПРАКТИЧЕСКИЙ СОВЕТ

Если никакой из вышеописанных способов не дает желаемого результата, можно, в качестве последнего средства, выполнить полный сброс, нажав и удерживая кнопку питания компьютера или отключив сетевое питание. В таком случае существует вероятность, что при следующем запуске компьютера будет запущено средство **Проверка диска** (Check Disk). Таким образом система проверяет наличие ошибок и проблем, которые могли возникнуть вследствие полного сброса. Если средство **Проверка диска** не запустится автоматически, запустите его вручную.

Как разобраться в сообщениях об ошибках

В *разд. "Настройка параметров восстановления" главы 2* подробно рассматривается настройка Windows 8 для записи отладочной информации. В случае возникновения серьезной ошибки при запуске Windows 8, установке программы или выполнении еще какой-либо операции, на весь экран выводится сообщение ошибки останова. Внимательно ознакомьтесь с содержанием этого сообщения и запишите следующую информацию.

- **Имя ошибки.** Имя ошибки должно быть в третьей строке сообщения, полностью прописными буквами, например `KERNEL_STACK_INPAGE_ERROR`.
- **Рекомендации по диагностированию.** После имени ошибки следуют рекомендации по диагностированию. Содержимое этих рекомендаций зависит от типа произошедшей ошибки и предоставляет общие советы по устранению проблемы.
- **Номер ошибки.** После рекомендаций по диагностированию указывается техническая информация об ошибке. В следующей строке после заголовка Technical Information будет слово `STOP`, номер ошибки и список параметров ошибки. Номер ошибки после слова `STOP`, например `STOP:0X00000050`, следует записать.
- **Сведения о драйвере.** Сразу же после строки с номером ошибки STOP следует строка с именем драйвера, связанным с данной ошибкой. Но эта информация предоставляется только в том случае, если системе удалось отследить ошибку к определенному драйверу. Запишите имя драйвера, если указано.

Если система настроена в случае ошибки останова на запись этого события в журналы событий, и если такую запись удалось выполнить, прежде чем система полностью вышла из строя, номер и параметры ошибки будут зафиксированы в журнале событий **Система**, а источник события указан как **Save Dump**. В записи события также будет указано, был ли создан файл дампа, и если создан, его местонахождение.

ПРАКТИЧЕСКИЙ СОВЕТ

Операционная система Windows 8 содержит возможность онлайнового анализа сбоев Online Crash Analysis, которая позволяет отправить файл дампа в службу технической поддержки продуктов Microsoft. Если включена функциональность отправки отчетов об ошибках, при перезапуске системы будет выведен запрос об отправке отладочной информации в Microsoft. Предоставляется опция отправить эту информацию анонимно или с использованием своей учетной записи Microsoft. Если отправить отладочную информацию со своим именем и контактной информацией посредством Microsoft Connect, с вами может связаться технический специалист с просьбой предоставить дополнительные сведения, который также может порекомендовать действие для устранения проблемы.

После сохранения информации, связанной с ошибкой останова, может потребоваться перезапустить систему в безопасном режиме, как рассматривается в *разд. "Восстановление возможности запуска системы" ранее в этой главе*. В этом режиме можно попробовать решить проблему, выполнив следующие действия.

- **Выполнить поиск сведений об ошибке в базе знаний Microsoft.** Посетите веб-сайт **support.microsoft.com** и выполните поиск в базе знаний по номеру ошибки. Если с дан-

ным кодом ошибки связана известная проблема, для нее должна быть соответствующая статья в базе знаний. В таком случае следуйте инструкциям в этой статье, чтобы решить проблему.

- **Проверьте драйвер (при наличии информации о драйвере).** Перезагрузив систему, проверьте, снабжен ли цифровой подписью связанный с ошибкой драйвер. Если драйвер был недавно обновлен, рекомендуется рассмотреть возможность его отката к предыдущей версии. Но сам факт наличия информации о драйвере в сообщении об ошибке не обязательно означает, что с ним что-то не в порядке и что его нужно заменить. Ошибка останова вполне могла быть вызвана другими факторами.
- **Определите, какие изменения были выполнены недавно.** Причина ошибки останова может крыться как в аппаратном, так и в программном обеспечении. Тщательно проверьте все программы или устройства, которые были недавно установлены на компьютере. Если было добавлено новое оборудование, проверьте правильность его установки, использование самых последних версий драйверов для него, а также правильность настройки устройства. В случае установки нового программного обеспечения проверьте правильность установки. Также рекомендуется проверить наличие обновлений или исправлений для него.
- **Проверьте использование системных ресурсов.** Причиной ошибок останова также может быть критически низкий уровень свободной памяти или дискового пространства. Запустив систему, проверьте объем свободного пространства дисков и, если необходимо, удалите ненужные файлы, чтобы освободить место на диске, используя для этого средство **Очистка диска** или другие инструменты. Также откройте диспетчер задач, нажав комбинацию клавиш <Ctrl>+<Alt>+<Del> и выбрав в меню Windows опцию **Диспетчер задач**. На вкладке **Производительность диспетчера задач** проверьте объем доступной физической и виртуальной памяти. Если доступен небольшой объем памяти, определите, какие программы используют ее, а также не исполняются ли на компьютере проблемные программы, такие как шпионские или рекламные.
- **Исправьте системные файлы.** Еще одной возможной причиной ошибок останова являются поврежденные системные файлы или использование неправильных версий системных файлов. При наличии подозрений, что причиной проблемной загрузки системы может быть повреждение системных файлов, может потребоваться исправить или даже полностью переустановить операционную систему. Дополнительную информацию по этому вопросу *см. в разд. "Восстановление возможности запуска системы" ранее в этой главе*.
- **Проверьте аппаратное и микропрограммное обеспечение.** Ошибки останова также могут вызываться неисправным оборудованием. В случае частых зависаний, перезагрузок или других серьезных проблем с компьютером рекомендуется тщательно проверить аппаратное обеспечение. Сначала проверьте драйверы устройств, т. к. проблемный драйвер может быть причиной ошибки останова. Затем проверьте физические устройства, в особенности жесткие диски, память, центральный процессор и видеоадаптер. Возможно, что сыпется жесткий диск, неисправна оперативная память, перегревается центральный процессор или же графический адаптер не поддерживает Windows 8. Также тщательно проанализируйте настройки параметров микропрограммного обеспечения. Касательно микропрограммного обеспечения, рекомендуется проверить на веб-сайте производителя системной платы наличие обновлений для него и, если оно имеется, выполнить обновление.

ГЛАВА 11

Использование технологии TPM и средства шифрования дисков BitLocker

Многие из встроенных в Windows 8 функциональностей обеспечения безопасности предназначены защищать компьютер от атак злоумышленников, которые пытаются получить доступ к компьютеру по локальной сети или через Интернет. Но что если злоумышленник имеет непосредственный физический доступ к компьютеру или его устройствам хранения данных? В таких случаях меры обеспечения безопасности Windows не защитят данные. Если злоумышленник способен загрузить компьютер, он может получить доступ к любым хранящимся на этом компьютере данным, включая и конфиденциальные. Кроме этого, при все более распространенном использовании флешек и других съемных устройств хранения данных на основе флеш-памяти пользователи все чаще берут свои данные с работы домой. Но данные на таких носителях обычно не защищены никаким образом, и в случае утери такой флешки будут доступны любому, нашедшему ее.

Защиту данных в подобных случаях Windows 8 обеспечивает такими средствами, как измеряемая загрузка[1], шифрование дисков посредством BitLocker и BitLocker To Go, а также архитектура служб модуля TPM. Все вместе эти возможности помогают защитить данные, хранящиеся на жестких дисках компьютеров и флеш-накопителях. Функциональность шифрования дисков BitLocker применяется для шифрования томов жестких дисков. Технология шифрования виртуальных томов BitLocker To Go служит для шифрования USB-флешек и других съемных носителей на основе флеш-памяти. А технологию модуля TPM можно использовать для повышения уровня защиты данных посредством шифрования дисков BitLocker.

Создание доверенных платформ

Чтобы воспользоваться службами TPM, компьютер под управлением Windows 8 должен быть оснащен совместимым модулем TPM и микропрограммным обеспечением. Операционная система Windows 8 поддерживает технологию TPM 1.2 и требует наличия микропрограммного обеспечения, отвечающего требованиям организации TCG[2]. Микропрограммное обеспечение, которое отвечает требованиям организации TCG, поддерживает статический

[1] Measured Boot.

[2] Trusted Computing Group — группа (разработки и исследований) доверенных вычислений.

источник оценки[1] соответственно определению организации TCG. Для некоторых конфигураций модуля TPM и шифрования дисков BitLocker также необходимо, чтобы микропрограммное обеспечение обладало возможностью чтения USB-устройств флеш-памяти при загрузке.

Основы технологии модуля TPM

В состав Windows 8 входит шифрующая файловая система EFS (Encrypting File System) для автоматического шифрования файлов и папок. С помощью этой системы пользователи могут защитить свои конфиденциальные данные, чтобы доступ к ним можно было получить, только используя свой сертификат открытого ключа. Сертификаты шифрования сохраняются среди данных в профилях пользователей. До тех пор, пока пользователи имеют доступ к своим профилям и хранящимся в них ключам шифрования, они могут работать со своими зашифрованными файлами.

Но хотя шифрующая файловая система обеспечивает надежную защиту данных от удаленной атаки, она не может защитить их, когда злоумышленник имеет физический доступ к компьютеру. Например, в случае утери или кражи компьютера или локального входа злоумышленником в систему файловая система EFS может не защитить данные, т. к. злоумышленник может получить доступ к ним до загрузки операционной системы. Затем он может получить управления компьютером, загрузив его другой операционной системой, и изменить конфигурацию компьютера. После этого он может взломать какую-либо учетную запись исходной операционной системы и выполнить вход по этой учетной записи или настроить компьютер для входа, как локальный администратор. В любом случае, так или иначе, в конечном итоге злоумышленник сможет получить полный доступ к компьютеру и хранящимся на его носителях данным.

Чтобы защитить данные в случае физического доступа к ним, Windows 8 помещает их в дополнительную защитную оболочку, используя архитектуру служб TPM. Службы TPM обеспечивают сохранность данных, используя специализированный аппаратный компонент, называющийся *доверенным платформенным модулем* (модуль TPM, Trusted Platform Module). Модуль TPM представляет собой микросхему, которая обычно встроена в системную плату компьютера и взаимодействует с системой по специальной шине. Компьютеры под управлением Windows 8 могут использовать модуль TPM для обеспечения повышенной безопасности данных, проверки целостности файлов загрузки на раннем этапе запуска системы и для гарантирования отсутствия несанкционированного вмешательства в содержимое диска, когда система была выключена.

Модуль TPM может создавать ключи шифрования, а затем зашифровывать эти ключи, делая невозможным их разглашение без предварительной расшифровки самим модулем TPM. Этот процесс, который называется *обертыванием* (wrapping) или *привязкой* (binding), надежно защищает ключи от несанкционированного разглашения. Модуль TPM использует главный "оберточный" ключ, который называется *корневым ключом хранилища* (ключ SRK, Storage Root Key). Ключ SRK хранится внутри модуля TPM, чтобы обеспечить сохранность личной части ключа.

Оснащенные модулем TPM компьютеры могут не только заворачивать ключи в защитную обертку шифрования, но и опечатывать этот сверток. Процесс опечатывания заключается в привязке ключа к конкретным параметрам платформы, вследствие чего ключ может быть распечатан только в том случае, если при распечатывании значения параметров платформы

[1] Static Root of Trust of Measurement.

соответствуют значениям при запечатывании. Все это делает компьютеры, оснащенные модулем TPM, более устойчивыми к атакам.

Так как модуль TPM хранит личные части криптографических пар в отдельном хранилище, чем память, управляемая операционной системой, ключи можно запечатать с привязкой к самому модулю TPM, обеспечивая, таким образом, абсолютную уверенность в состоянии системы и ее надежности. Ключи модуля TPM можно распечатать только при условии отсутствия нарушения целостности системы. Более того, так как для обработки инструкций, связанных с ключами, модуль TPM использует свое встроенное микропрограммное обеспечение и логические схемы, он не зависит от операционной системы и не подвержен уязвимостям внешнего программного обеспечения.

Модуль TPM можно также использовать для опечатывания и распечатывания данных, создаваемых вне модуля. Вот в этой возможности модуля TPM и заключается его настоящая сила. В операционной системе Windows 8 для доступа к модулю TPM и для его использования с целью защиты данных компьютера применяется шифрование дисков BitLocker. Хотя эту функциональность можно использовать как с модулем TPM, так и без него, подход с использованием модуля TPM обеспечивает более высокий уровень защиты.

Если диспетчер загрузки и загрузочные файлы компьютера опечатать посредством возможности BitLocker и модуля TPM, их можно распечатать только в том случае, если они не были изменены после опечатывания. Это означает, что модуль TPM можно использовать для проверки целостности загрузочных файлов компьютера в среде предзагрузки операционной системы. А опечатанный с помощью модуля TPM жесткий диск можно распечатать, только если данные диска не были изменены после опечатывания. Таким образом, гарантируется отсутствие несанкционированного доступа к диску, пока компьютер был выключен.

При использовании BitLocker для опечатывания диспетчера загрузки и загрузочных файлов компьютера без модуля TPM, модуль TPM нельзя использовать для проверки целостности загрузочных файлов компьютера в среде предзагрузки операционной системы. Это означает, что в таком случае гарантировать целостность диспетчера загрузки и загрузочных файлов компьютера нет никакой возможности.

Управление и политики модуля TPM

Операционная система Windows 8 предоставляет несколько инструментов для работы с модулем TPM, включая следующие.

- **Управление доверенным платформенным модулем (TPM)** (Trusted Platform Module Management) — консоль для настройки и управления модулем TPM. Запустить эту консоль можно, выполнив в командной строке или в поле поиска панели **Приложения** команду `tpm.msc`.
- **Управление оборудованием безопасности для TPM** (Manage the TPM security hardware) — мастер для создания необходимого пароля владельца модуля TPM. Запустить этот мастер можно, выполнив в командной строке или в поле поиска панели **Приложения** команду `tpminit`.

> ***Практический совет***
>
> Доступ к консоли **Управление доверенным платформенным модулем (TPM)** может быть заблокирован в групповой политике. В случае проблем с открытием этой консоли проверьте, не отключен ли в текущем объекте групповой политики параметр **Управление TPM**, который находится в узле редактора групповой политики **Конфигурация пользователя\Административные шаблоны\Компоненты Windows\Консоль управления (MMC)\Запрещенные и разрешенные оснастки**.

Для выполнения задач управления модулем TPM на локальном компьютере необходимо выполнить вход в систему по учетной записи администратора локального компьютера. С помощью консоли **Управление доверенным платформенным модулем (TPM)** можно определить точное состояние модуля TPM. Если запустить эту консоль, когда модуль TPM не включен, выдается соответствующее сообщение об ошибке. Также если этот модуль не включен, при попытке запуска мастера **Управление оборудованием безопасности для TPM** выводится соответствующее сообщение об ошибке.

Только когда модуль TPM включен в микропрограммном обеспечении компьютера, можно выполнять задачи по его управлению с использованием соответствующих инструментов операционной системы. При работе с консолью **Управление доверенным платформенным модулем (TPM)** (рис. 11.1) следует обратить внимание на состояние модуля TPM и информацию об его производителе.

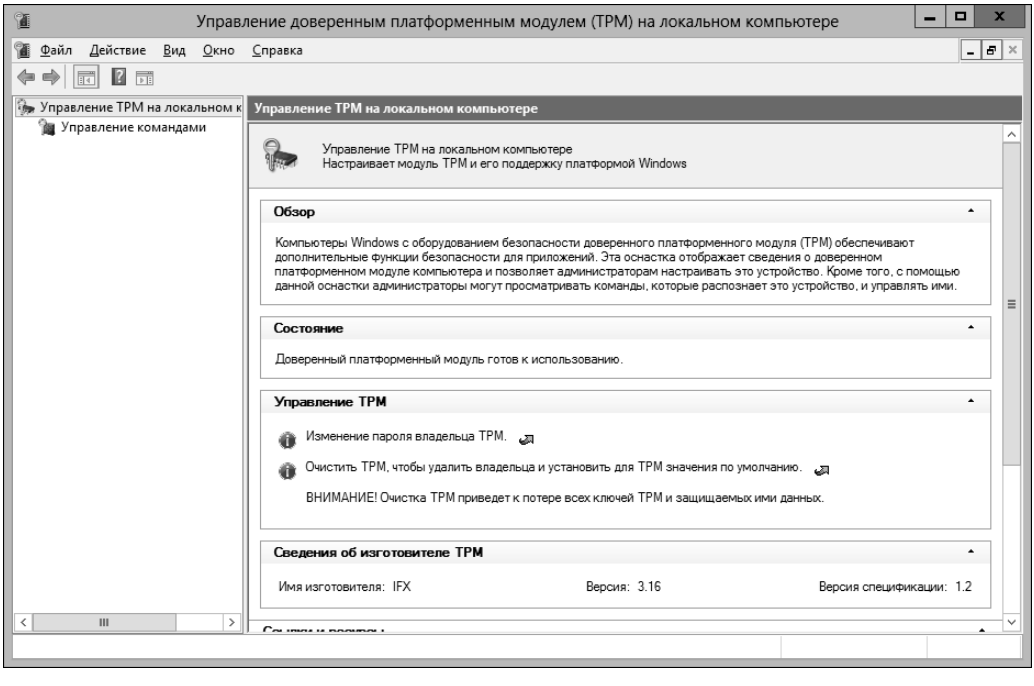


Рис. 11.1. Консоль **Управление доверенным платформенным модулем (TPM)** для работы с модулем TPM

Состояние модуля TPM отображается в разделе **Состояние** консоли. В табл. 11.1 приведен список сообщений состояния и краткое описание их значений. А в разделе **Сведения об изготовителе TPM** (TPM Manufacturer Information) отображается, поддерживает ли модуль версию спецификации 1.2 или 2.0. Для Windows 8 требуется, чтобы модуль TPM поддерживал версию спецификации 1.2 или более позднюю версию.

Таблица 11.1. *Сообщения о состоянии модуля TPM и их значение*

Состояние TPM	Значение
Модуль TPM включен, владелец не назначен. (The TPM is on and ownership has not been taken.)	Модуль TPM включен в микропрограммном обеспечении, но еще не был инициализирован
Модуль TPM включен, владелец назначен. (The TPM is on and ownership has been taken.)	Модуль TPM включен в микропрограммном обеспечении и был инициализирован

Таблица 11.1 *(окончание)*

Состояние TPM	Значение
Модуль TPM выключен, владелец не назначен. (The TPM is off and ownership has not been taken.)	Модуль TPM отключен в программном обеспечении и также еще не был инициализирован
Модуль TPM выключен, владелец назначен. (The TPM is off and ownership has been taken.)	Модуль TPM был инициализирован, но выключен в программном обеспечении

Примечание

Хотя в предыдущих версиях Windows указывалось точное состояние модуля TPM, Windows 8 обычно показывает его состояние как или "Готов к использованию" или "Не готов к использованию". Если модуль TPM готов к использованию, он был включен и владелец назначен.

По умолчанию Windows 8 и Windows Server 2012 сохраняют полную информацию авторизации для владельца модуля TPM в реестре локального компьютера. Это значительное изменение по сравнению с предыдущими версиями Windows позволяет администраторам локального компьютера выполнять задачи администрирования модуля TPM без необходимости предоставления пароля владельца модуля TPM.

Уровень авторизационной информации, хранящейся в реестре, определяется параметром политики **Настроить уровень сведений авторизации владельца TPM, доступных операционной системе** (Configure the level of TPM owner authorization information available to the operating system). Этот параметр находится в узле **Конфигурация компьютера\Административные шаблоны\Система\Службы доверенного платформенного модуля** (Computer Configuration\Administrative Templates\System\Trusted Platform Module Services) редактора локальной групповой политики. Параметру можно присвоить три значения.

- **Полный режим** (Full). В реестре сохраняются полные сведения авторизации владельца модуля TPM, большой двоичный объект делегирования административных полномочий модуля TPM и большой двоичный объект делегирования пользователя модуля TPM. Это значение позволяет использовать модуль TPM, не требуя удаленного или внешнего хранения авторизационной информации владельца модуля. Обратите внимание, что приложения на основе модуля TPM для более ранних версий Windows или приложения, которые полагаются на логику противодействия подбора паролей модуля TPM[1], могут не поддерживать хранение в реестре полной авторизационной информации владельца модуля TPM.
- **Делегировано** (Delegated). В реестре сохраняются только большой двоичный объект делегирования административных полномочий модуля TPM и большой двоичный объект делегирования пользователя модуля TPM. Этот уровень подходит для приложений на основе модуля TPM, которые полагаются на логику противодействия подбора паролей модуля TPM. При использовании этого значения разработчики Microsoft рекомендуют сохранять авторизационную информацию владельца модуля TPM в удаленном месте или внешнем хранилище.
- **Отсутствует** (None). В реестре не сохраняется никакая авторизационная информация владельца модуля TPM. Это значение параметра используется для совместимости с предыдущими версиями Windows и для приложений, для которых требуется хранение авторизационной информации владельца модуля TPM в удаленном месте или на внешнем носителе. При использовании этого значения необходимо наличие удаленного или внешнего носителя для хранения авторизационной информации владельца модуля TPM, подобно тому, как это требовалось в предыдущих версиях Windows.

[1] TPM anti-hammering logic.

Осторожно!

Если изменить значение этого параметра с **Полный режим** на **Делегировано** и наоборот, выполняется повторное создание авторизационного значения владельца модуля TPM, и первоначальное значение будет недействительным.

Когда значение этого параметра установлено в **Делегировано** или **Отсутствует**, прежде чем будет разрешено выполнять большинство задач администрирования модуля TPM, необходимо предоставить пароль владельца модуля TPM. На рис. 11.2 показано окно запроса на предоставление этого пароля.

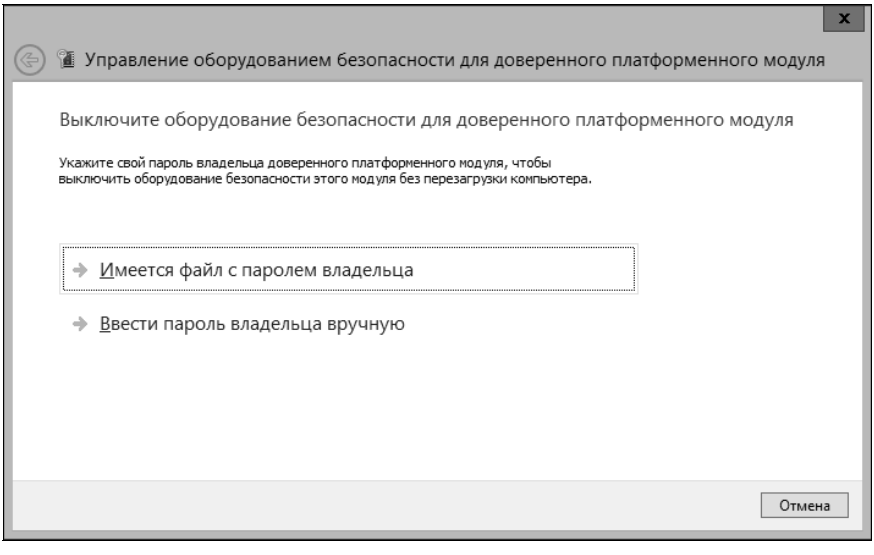


Рис. 11.2. Окно запроса на предоставление пароля владельца модуля TPM

Для предыдущих версий Windows разработчики Microsoft рекомендуют сохранять авторизационную информацию владельцев модулей TPM доменных компьютеров в удаленном хранилище службы каталогов Active Directory. Это можно сделать, включив параметр политики **Включить резервное копирование TPM в доменные службы Active Directory** (Turn on TPM backup to Active Directory Domain Services).

Включение резервного копирования в службу каталогов Active Directory изменяет метод хранения по умолчанию авторизационной информации владельца модуля TPM. В частности, когда включен параметр **Включить резервное копирование TPM в доменные службы Active Directory**, а параметр **Настроить уровень сведений авторизации владельца TPM, доступных операционной системе** выключен или не задан, в реестре сохраняются только большой двоичный объект делегирования административных полномочий модуля TPM и большой двоичный объект делегирования пользователя модуля TPM. В таком случае для хранения полной авторизационной информации владельца модуля TPM необходимо использовать значение параметра **Полный режим** (или отключить резервное копирование в службе каталогов Active Directory авторизационной информации владельца модуля TPM).

Узел **Службы доверенного платформенного модуля** также содержит следующие связанные параметры:

- **Игнорировать список заблокированных команд TPM по умолчанию** (Ignore the default list of blocked TPM commands);

- **Игнорировать локальный список заблокированных команд TPM** (Ignore the local list of blocked TPM commands);
- **Длительность блокировки обычных пользователей** (Standard user lockout duration);
- **Индивидуальный порог блокировки обычных пользователей** (Standard user individual lockout threshold);
- **Общий порог блокировки обычных пользователей** (Standard user total lockout threshold).

Эти параметры политики определяют способ использования списков блокировки команд и обстоятельства активирования блокировки после нескольких неудачных попыток авторизации. Администратор может полностью сбросить все связанные с блокировкой параметры в консоли **Управление доверенным платформенным модулем (TPM)**. Для этого в меню **Действие** следует выбрать команду **Сброс блокировки доверенного платформенного модуля** (Reset TPM Lockout). Когда полная авторизационная информация владельца модуля TPM хранится в реестре, предоставлять пароль владельца модуля TPM не требуется. В противном случае следуйте выводимым запросам и предоставьте пароль или выберите содержащий пароль файл.

Включение модуля TPM

Архитектура служб TPM в Windows 8 предоставляет основные возможности, требуемые для настройки и использования компьютеров с модулем TPM. Эту архитектуру можно расширить возможностью шифрования дисков BitLocker, которая рассматривается в *разд. "Основы шифрования дисков с помощью BitLocker" далее в этой главе*.

Но прежде чем использовать модуль TPM, его нужно включить в микропрограммном обеспечении компьютера. В некоторых случаях эта возможность может быть уже включенной, но в большинстве случаев это не так. Точная процедура включения модуля TPM зависит от конкретного компьютера. На одном из компьютеров автора этой книги для включения данного модуля потребовалось выполнить следующие шаги:

1. Включить компьютер и нажать клавишу <F2>, чтобы получить доступ к микропрограммному обеспечению. В микропрограммном обеспечении открыть экран **Advanced**, а затем экран **Peripheral Configuration**.
2. Одной из опций этого экрана была опция **Trusted Platform Module**. С помощью клавиши <↓> выбрать эту опцию и нажать клавишу <Enter>, чтобы отобразить меню параметров для этой опции. Выбрать в меню опцию **Enable** и нажать клавишу <Enter>.
3. Нажать клавишу <F10>, чтобы сохранить внесенные изменения, и выйти из интерфейса настройки микропрограммного обеспечения. На запрос подтвердить выход из интерфейса настройки нажать клавишу <Y>, после чего компьютер был перезагружен.

А чтобы включить модуль TPM на другом компьютере автора, потребовалось выполнить следующую процедуру:

1. Включить компьютер и нажать клавишу <F2>, чтобы получить доступ к микропрограммному обеспечению. В интерфейсе настройки открыть меню **Security**, а в нем открыть экран **TPM Security**.
2. На этом экране установить флажок **TPM Security** и нажать кнопку **Apply**.
3. Было выведено напоминание, что для включения модуля TPM необходимо выключить, а затем перезапустить компьютер.

4. После выхода из интерфейса настройки микропрограммного обеспечения компьютер перезагрузился.

Включив модуль TPM в микропрограммном обеспечении, его необходимо инициализировать и подготовить к использованию в операционной системе. Частью процесса является назначение владельца модулю TPM, это устанавливается паролем владельца для модуля. После включения модуля TPM можно выполнять настройку его параметров.

Инициализация и подготовка модуля TPM для использования

Инициализация модуля TPM подготавливает его для использования на компьютере, чтобы с его помощью можно было обезопасить тома жестких дисков компьютера. Процесс инициализации заключается во включении модуля TPM, а затем в назначении его владельца. При установке владельца модуля TPM устанавливается пароль, что способствует обеспечению доступа и управлению модулем TPM только авторизованным владельцем модуля. Пароль модуля TPM требуется и для его отключения, когда в нем больше нет надобности, а также для очистки содержимого модуля, прежде чем сдавать компьютер в утилизацию. В домене Active Directory для хранения паролей модуля TPM можно настроить групповую политику.

Чтобы инициализировать модуль TPM и создать пароль владельца, войдите в систему по учетной записи администратора, а затем выполните следующую процедуру:

1. Запустите консоль **Управление доверенным платформенным модулем (TPM)**. В меню **Действие** выберите команду **Подготовить TPM** (Prepare the TPM). Будет запущен мастер **Управление оборудованием безопасности для TPM** (файл tpminit.exe).

> ***Примечание***
>
> Если мастер инициализации оборудования TPM обнаружит микропрограммное обеспечение, которое не отвечает требованиям Windows, или не обнаружит модуль TPM, процедуру инициализации модуля TPM нельзя будет продолжить, пока эти требования не будут удовлетворены.

> ***Практический совет***
>
> Если модуль TPM был инициализирован, а затем задана команда очистить его, система выводит запрос перезагрузить компьютер и следовать выводимым инструкциям при загрузке компьютера, чтобы очистить модуль TPM в микропрограммном обеспечении. При следующем входе в систему должен быть опять запущен мастер управления оборудованием TPM. Но на компьютерах автора процесс очистки не пошел так, как он должен был пойти. Вместо этого, после того как я нажал кнопку **Завершение работы** и перезапустил компьютер, при загрузке мне понадобилось нажать клавишу <F2>, чтобы войти в интерфейс микропрограммного обеспечения компьютера. Там я должен был вручную отключить модуль TPM, сохранить изменения, а затем выйти из интерфейса микропрограммного обеспечения. Это активировало автоматическую перезагрузку. После этого мне нужно было снова войти в интерфейс микропрограммного обеспечения, включить модуль TPM, сохранить изменения и выйти из интерфейса. Это опять активировало автоматическую перезагрузку. После загрузки операционной системы потребовался перезапуск мастера **Управление оборудованием безопасности для TPM**.

2. Когда мастер завершит выполнение задач первоначального этапа, выводится окно запроса перезагрузить компьютер (рис. 11.3). Нажмите кнопку **Завершение работы** (Restart), чтобы перезагрузить компьютер.
3. Обычно разработанное под Windows 8 и Windows Server 2012 аппаратное обеспечение может завершить процесс инициализации автоматически. С другим оборудованием потребуется физический доступ к компьютеру, чтобы ответить на запрос действия по настройке модуля TPM, выводимый микропрограммным обеспечением. Пример такого

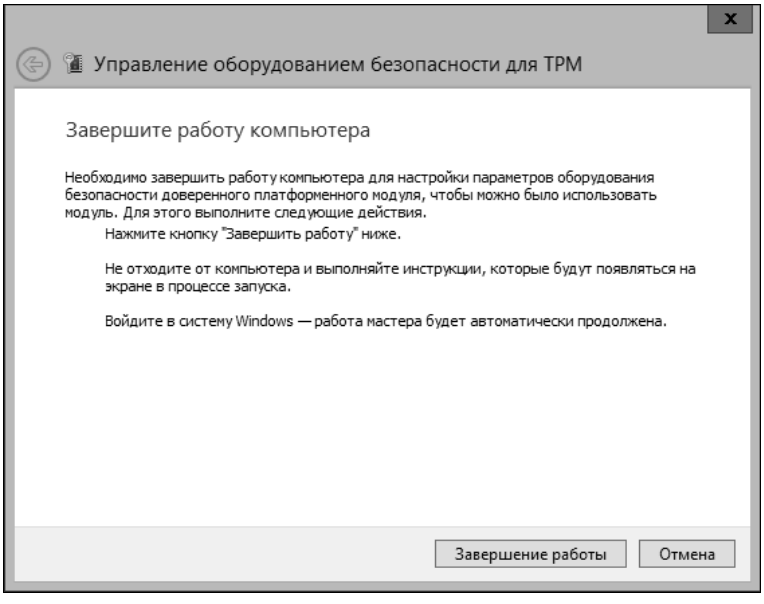


Рис. 11.3. Для продолжения подготовки модуля TPM в настройках микропрограммного обеспечения необходимо перезагрузить компьютер

запроса показан на рис. 11.4. В данном случае нужно нажать клавишу <F10>, чтобы активировать модуль TPM и позволить пользователю стать его владельцем.

4. После запуска компьютера и входа в систему, возобновляется выполнение мастера **Управление оборудованием безопасности для TPM** и Windows присваивает владение модуля TPM. Присвоение владения модуля TPM подготавливает его для работы с операционной системой.

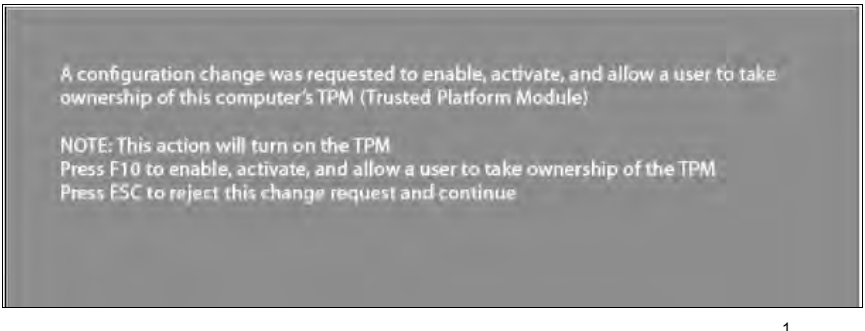


Рис. 11.4. Запрос на подтверждение изменения конфигурации модуля TPM[1]

[1] На рисунке сообщение:

"Подан запрос на изменение конфигурации, чтобы включить и активировать модуль TPM (доверенный платформенный модуль) этого компьютера и позволить пользователю стать его владельцем

ПРИМЕЧАНИЕ: Это действие включит модуль TPM

Нажмите клавишу <F10>, чтобы включить и активировать модуль TPM и позволить пользователю стать его владельцем.

Нажмите клавишу ESC, чтобы отклонить этот запрос и продолжить загрузку".

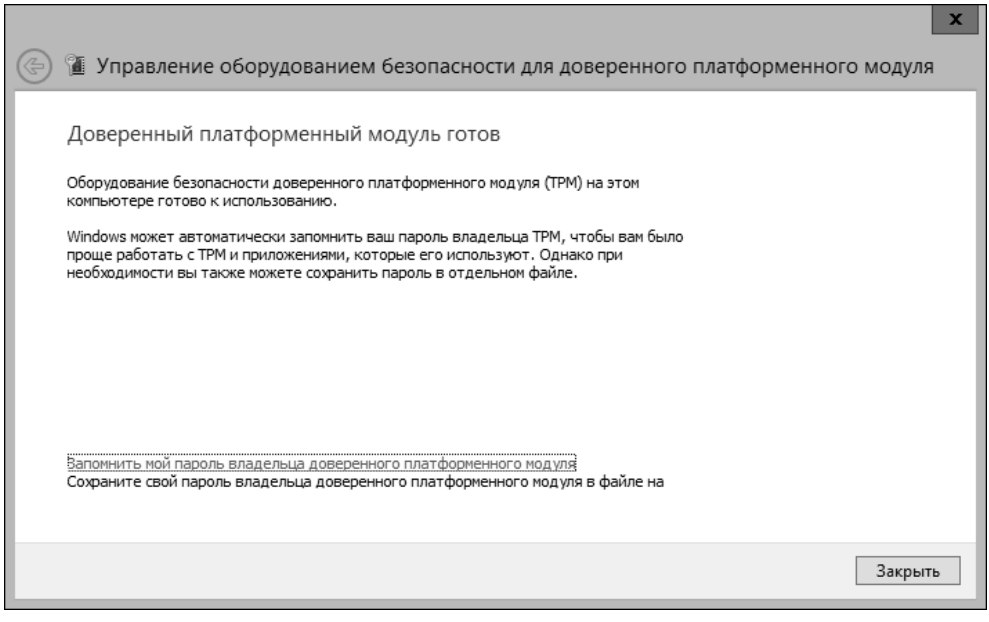


Рис. 11.5. Сообщение об установке владельца и готовности модуля TPM к использованию

5. После установки владельца TPM-модуля он готов к работе, о чем выводится соответствующее сообщение (рис. 11.5).
6. Прежде чем закрывать это сообщение, рекомендуется сохранить пароль владельца модуля TPM, щелкнув для этого по ссылке **Запомнить мой пароль владельца доверенного платформенного модуля** (Remember my TPM owner password). В открывшемся диалоговом окне навигации по файловой системе укажите папку для сохранения файла с паролем, а затем нажмите кнопку **Сохранить**.
7. После этого в консоли управления модулем TPM его состояние должно указываться как **Доверенный платформенный модуль готов к использованию** (The TPM is ready for use).

Примечание

По умолчанию файл пароля сохраняется под именем *Имя_компьютера*.tpm. Лучше всего будет сохранить этот файл пароля владельца модуля TPM на съемном носителе, например флешке, и поместить его на хранение в безопасное место. В домене, в котором используется политика **Включить резервное копирование TPM в доменные службы Active Directory**, возможности сохранить пароль владельца модуля TPM не предоставляется. Вместо этого пароль автоматически сохраняется в службе Active Directory.

Дополнительная информация

Файл пароля владельца модуля TPM представляет собой незашифрованный документ XML, который можно открыть для просмотра в любом текстовом редакторе. Далее приводится пример содержимого файла пароля владельца модуля TPM на компьютере ENGPC85:

```
<?xml version="1.0" encoding="UTF-8"?>
<!--
Эта страница является резервной копией сведений авторизации владельца доверенного
платформенного модуля (TPM). При получении запроса используйте сведения авторизации
для подтверждения владения доверенным платформенным модулем компьютера (TPM).
```

```
Внимание! Храните этот файл в безопасном месте — не на локальном жестком диске
данного компьютера.
-->
<tpmOwnerData version="1.0" softwareAuthor="Microsoft Windows [Version 6.2.8400]"
creationDate="2013-03-21T01:01:59+04:00" creationUser="ENGPC85\Administrator"
machineName="ENGPC85">
  <tpmInfo manufacturerId="1229346816"/>
  <ownerAuth>syEmhGriXi00agGFOVkw9XLUnw4=</ownerAuth>
</tpmOwnerData>
```

Включение и выключение инициализированного модуля TPM

Компьютеры, оснащенные модулем TPM, могут поставляться с включенным модулем. Если в функциональности модуля TPM нет надобности, нужно стать владельцем модуля, а затем выключить его. Таким образом, операционная система будет оставаться владельцем модуля TPM, но сам модуль будет неактивным. Если компьютер нужно переконфигурировать или утилизировать, модуль TPM необходимо очистить. Очистка модуля TPM уничтожает все хранящиеся в нем ключи, вследствие чего зашифрованные с помощью этих ключей данные станут недоступными.

Чтобы выключить модуль TPM, войдите в систему по учетной записи администратора, а затем выполните следующую процедуру:

1. Запустите консоль **Управление доверенным платформенным модулем (TPM)**.
2. В меню **Действие** выберите опцию **Отключить TPM** (Turn TPM off).
3. Когда полная авторизационная информация владельца модуля TPM хранится в реестре, предоставлять пароль владельца модуля TPM не требуется. В противном случае следуйте выводимым запросам и предоставьте пароль или выберите содержащий пароль файл.

Отключив модуль TPM в операционной системе, используя вышеизложенную процедуру, его можно опять включить, следуя процедуре, описанной в *разд. "Инициализация и подготовка модуля TPM для использования" ранее в этой главе.*

Очистка модуля TPM

Операция очистки модуля TPM удаляет хранящуюся в нем информацию и отменяет связанное владение модулем. Очистку модуля TPM всегда следует выполнять при сдаче компьютера в утилизацию. Очистка модуля TPM уничтожает все хранящиеся в нем ключи, вследствие чего зашифрованные с помощью этих ключей данные станут недоступными.

После очистки модуля TPM следует стать его владельцем. Таким образом, в модуль TPM будет записана новая информация. После этого модуль можно отключить, если в его функциональности нет надобности.

Чтобы очистить модуль TPM, войдите в систему по учетной записи администратора, а затем выполните следующую процедуру:

1. Запустите консоль **Управление доверенным платформенным модулем (TPM)**. В меню **Действие** выберите команду **Очистить TPM** (Clear TPM). Будет запущен мастер **Управление оборудованием безопасности для TPM**.

> ***Осторожно!***
>
> Очистка модуля TPM возвращает его к настройкам по умолчанию производителя, в результате чего теряются все ключи и зашифрованные этими ключами данные. Для очистки модуля TPM предоставлять пароль его владельца не требуется.

2. Ознакомьтесь с инструкциями по процедуре очистки модуля на начальной странице мастера (рис. 11.6), а затем нажмите кнопку **Завершение работы** (Restart). Чтобы отменить очистку модуля TPM, завершите работу мастера, нажав кнопку **Отмена**.
3. Обычно, разработанное под Windows 8 и Windows Server 2012 аппаратное обеспечение может завершить процесс очистки модуля TPM автоматически. С другим оборудовани-

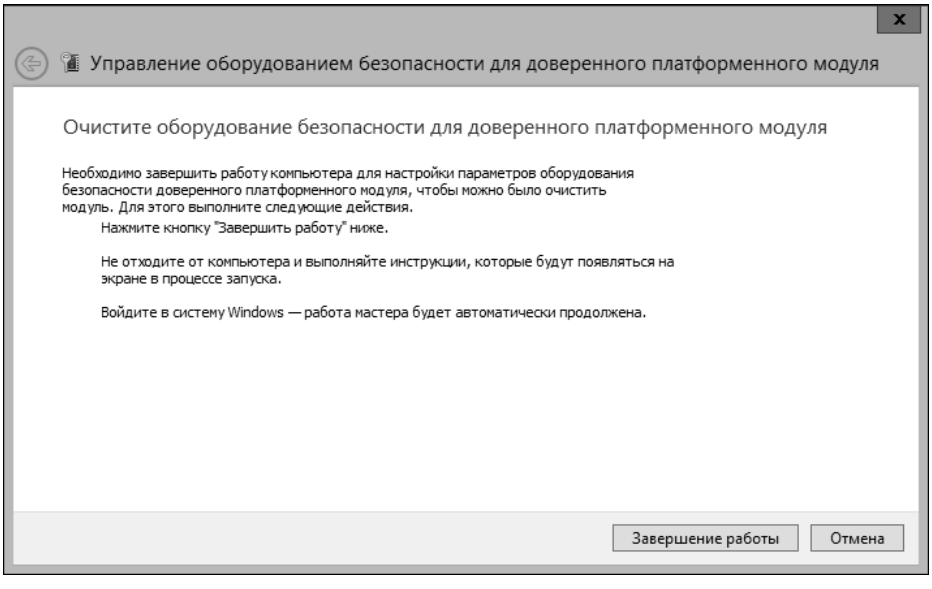


Рис. 11.6. Окно мастера для очистки модуля TPM

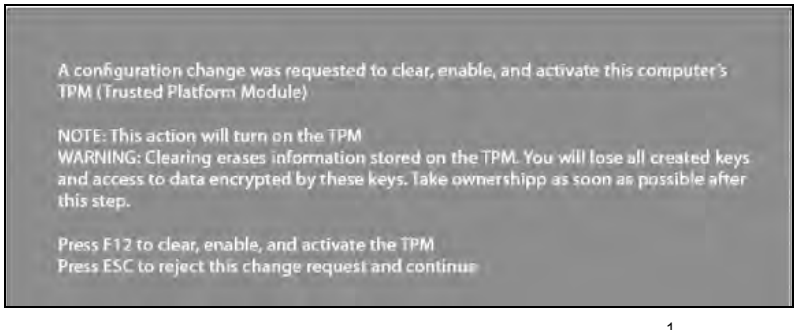


Рис. 11.7. Запрос на подтверждение очистки модуля TPM[1]

[1] На рисунке сообщение:

"Подан запрос на очистку, включение и активирование модуля TPM (доверенного платформенного модуля) этого компьютера

ПРИМЕЧАНИЕ: Это действие включит модуль TPM
ВНИМАНИЕ: Операция очистки модуля TPM удаляет хранящуюся в нем информацию. Будут утеряны все созданные вами ключи, вследствие чего данные, зашифрованные этими ключами, будут больше недоступными. Возьмите владение модулем как можно быстрее после выполнения этой операции.

Нажмите клавишу <F12>, чтобы очистить, включить и активировать модуль TPM
Нажмите клавишу <ESC>, чтобы отклонить этот запрос и продолжить загрузку".

ем потребуется физический доступ к компьютеру, чтобы ответить на запрос действия по настройке модуля TPM, выводимый микропрограммным обеспечением. Пример такого запроса показан на рис. 11.7. В данном случае нужно нажать клавишу <F12>, чтобы очистить, включить и активировать модуль TPM. Чтобы отменить операцию очистки, нужно нажать клавишу <ESC>.

4. Выполните шаги 4—7 процедуры подготовки модуля TPM, изложенной в *разд. "Инициализация и подготовка модуля TPM для использования" ранее в этой главе.*

Изменение пароля владельца модуля TPM

Пароль владельца модуля TPM можно изменить в любое время. Основной причиной для смены пароля будет подозрение, что пароль стал доступен постороннему лицу. Кроме этого, политика безопасности компании также может требовать изменения пароля владельца модуля TPM в определенных обстоятельствах.

Сменить пароль владельца модуля TPM можно следующим образом:

1. Запустите консоль **Управление доверенным платформенным модулем (TPM)**. В меню **Действие** выберите команду **Изменить пароль владельца** (Change owner password). Будет запущен мастер **Управление оборудованием безопасности для TPM**.
2. Когда полная авторизационная информация владельца модуля TPM хранится в реестре, предоставлять пароль владельца модуля TPM не требуется. В противном случае следуйте выводимым запросам и предоставьте пароль или выберите содержащий пароль файл.
3. На следующей странице мастера, **Создайте пароль владельца доверенного платформенного модуля** (Create the TPM owner password) (рис. 11.8), можно выбрать опцию **создать пароль автоматически или вручную**.
4. Чтобы создать пароль автоматически, щелкните по ссылке **Автоматически создать пароль (рекомендуется)** (Automatically create the password (recommended)). Откроется

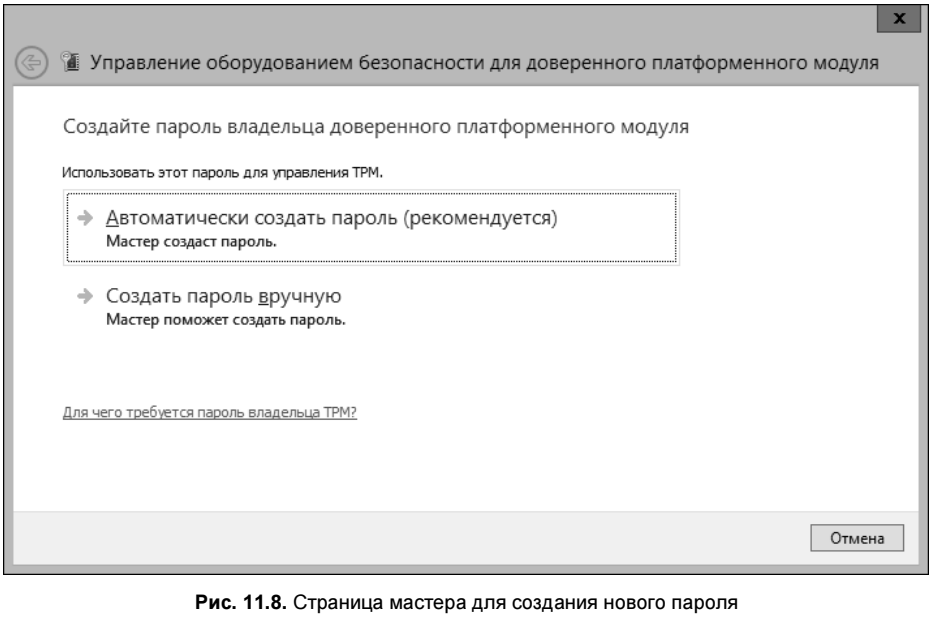


Рис. 11.8. Страница мастера для создания нового пароля

окно с новым паролем владельца модуля TPM. Нажмите в этом окне кнопку **Изменить пароль** (Change password).

5. Чтобы создать пароль самому, щелкните по ссылке **Создать пароль вручную** (Manually create the password). На следующей странице мастера введите и подтвердите пароль длиной минимум в восемь символов, а затем нажмите кнопку **Изменить пароль**.
6. Прежде чем закрывать это сообщение, рекомендуется сохранить пароль владельца модуля TPM, щелкнув для этого по ссылке **Запомнить мой пароль владельца доверенного платформенного модуля**. В открывшемся диалоговом окне навигации по файловой системе укажите папку для сохранения файла с паролем, а затем нажмите кнопку **Сохранить**.

Основы шифрования дисков с помощью BitLocker

Функциональность шифрования дисков BitLocker является составной частью Windows 8 и предоставляется как опция для всех версий Windows Server. Хотя функциональность шифрования дисков BitLocker и функциональность BitLocker To Go часто называют одинаково просто BitLocker, они являются хоть и похожими, но отдельными функциональностями. Функциональность шифрования дисков BitLocker представляет собой технологию шифрования на уровне томов и предназначена для защиты данных на внутренних жестких дисках в случае утери, кражи или ненадлежащей утилизации компьютера. А функциональность BitLocker To Go представляет собой технологию шифрования виртуальных томов и предназначена для защиты данных на съемных носителях, например внешних жестких дисках или флешках. Шифрования дисков BitLocker обеспечивает защиту данных, зашифровывая весь том или его часть. А функциональность BitLocker To Go, с другой стороны, создает на флешке виртуальный том, который затем кодируется хранящимся на флешке ключом шифрования.

Функциональность шифрования дисков BitLocker

Злоумышленник, который имеет прямой физический доступ к компьютеру без функциональности шифрования дисков BitLocker, может разными способами получить полный контроль над этим компьютером, а затем получить доступ к хранящимся на его дисках данным независимо от того, зашифрованы ли эти данные посредством шифрующей файловой системы или нет. Например, он может использовать загрузочный диск, чтобы загрузить компьютер и изменить пароль администратора. Злоумышленник также может установить на компьютер другую операционную систему, а затем использовать ее, чтобы получить доступ к первоначальной операционной системе.

Функциональность шифрования дисков BitLocker предотвращает любой доступ к жесткому диску, за исключением санкционированного персонала, защищая весь том или только его используемую часть, стойким к взлому шифрованием. Любая попытка просмотра или манипулирования данными на диске, зашифрованном с помощью BitLocker, несанкционированным лицом не будет иметь успеха. Это существенно понижает уровень риска получения доступа к конфиденциальным данным несанкционированным лицом посредством прямого доступа к компьютеру или его жестким дискам.

Осторожно!

Функциональность шифрования дисков BitLocker понижает производительность диска. Она предназначена для использования в тех обстоятельствах, когда компьютер не находится в безопасной среде и требует дополнительной защиты.

Функциональность шифрования дисков BitLocker может использовать модуль TPM для проверки целостности диспетчера загрузки и загрузочных файлов компьютера и для гарантирования отсутствия несанкционированного модифицирования содержимого жестких дисков, пока система была выключенной. Функциональность BitLocker также сохраняет в модуле TPM характеристики основных файлов операционной системы.

При каждом запуске компьютера Windows проверяет загрузочные файлы, файлы операционной системы и все зашифрованные тома, чтобы удостовериться, что они не были изменены, пока система была выключена. В случае выявления изменений файлов Windows оповещает об этом пользователя и отказывается выдавать ключ, требуемый для доступа к Windows. Затем компьютер переходит в режим восстановления, запрашивая у пользователя ключ восстановления, прежде чем позволить доступ к загрузочному тому. Режим восстановления также запускается, когда зашифрованный посредством BitLocker диск был перенесен на другую систему.

Функциональность шифрования дисков BitLocker можно использовать на компьютерах как оснащенных модулем TPM, так и не оснащенных таковым. Если компьютер оснащен модулем TPM, функциональность BitLocker использует этот модуль для повышения уровня безопасности данных и обеспечения целостности файлов на раннем этапе загрузки. Совместно эти возможности помогают предотвратить несанкционированный доступ к данным, зашифровывая весь том Windows и защищая загрузочные файлы от несанкционированного изменения. Если компьютер не оснащен модулем TPM или оснащен модулем, несовместимым с Windows, функциональность BitLocker можно использовать, чтобы полностью зашифровать диски, таким образом, предотвращая несанкционированную модификацию их данных. Но такой подход не предоставляет дополнительной безопасности проверки целостности файлов на раннем этапе загрузки.

На компьютерах, оснащенных совместимым с Windows и инициализированным модулем TPM, BitLocker обычно использует один из следующих режимов модуля TPM.

- **Только модуль TPM.** В этом режиме для проверки целостности файлов используется только модуль TPM. В процессе загрузки компьютера модуль TPM применяется для проверки целостности загрузочных файлов, файлов операционной системы и зашифрованных томов. Так как пользователю не требуется предоставлять дополнительный ключ для начала загрузки, этот режим является прозрачным для него, и процедура входа в систему ничем не отличается от обычной. Но в случае отсутствия модуля TPM или нарушения целостности файлов или томов, функциональность BitLocker запускает режим восстановления и требует ввода ключа восстановления или пароля, чтобы восстановить доступ к загрузочному тому.
- **Модуль TPM и ПИН-код.** В этом режиме для проверки целостности файлов применяется как модуль TPM, так и вводимый пользователем код. В процессе загрузки компьютера модуль TPM используется для проверки целостности загрузочных файлов, файлов операционной системы и зашифрованных томов. Чтобы продолжить загрузку, пользователь должен ввести правильный ПИН-код. Если пользователь не введет или введет неправильный ПИН-код, BitLocker прекращает процесс загрузки операционной системы и переходит в режим восстановления. Как и ранее, в случае отсутствия модуля TPM или нарушения целостности загрузочных файлов или изменения содержимого зашифрованных томов, функциональность BitLocker переходит в режим восстановления.
- **Модуль TPM и ключ запуска.** В этом режиме для проверки целостности файлов применяется как модуль TPM, так и предоставляемый пользователем ключ запуска. В процессе загрузки компьютера модуль TPM используется для проверки целостности загрузочных файлов, файлов операционной системы и зашифрованных томов. Кроме этого,

для входа в систему пользователь также должен предоставить ключ запуска на флешке. Если пользователь не предоставит или предоставит неправильный код запуска, BitLocker прекращает процесс загрузки и переходит в режим восстановления. Как и ранее, в случае отсутствия модуля TPM или нарушения целостности загрузочных файлов или изменения содержимого зашифрованных томов, BitLocker также переходит в режим восстановления.

- **Модуль TPM и сертификат на смарт-карте.** В этом режиме для проверки используется как модуль TPM, так и сертификат на смарт-карте. В процессе загрузки компьютера модуль TPM используется для проверки целостности загрузочных файлов, файлов операционной системы и зашифрованных томов. Кроме этого, для входа в систему пользователь также должен предоставить действительный сертификат на смарт-карте. Если пользователь не предоставит или предоставит смарт-карту с неправильным сертификатом, функциональность BitLocker прекращает процесс загрузки и переходит в режим восстановления. Как и ранее, в случае отсутствия модуля TPM или нарушения целостности загрузочных файлов или изменения содержимого зашифрованных томов, функциональность BitLocker также переходит в режим восстановления.

На компьютерах под управлением Windows 8 или Windows Server 2012 сетевая разблокировка (network unlock) позволяет автоматическую разблокировку при запуске системного тома компьютера, оснащенного модулем TPM, при условии, что компьютер является членом домена и подключен к нему. Для компьютера, не подключенного к домену, могут использоваться другие средства проверки, например ПИН-код запуска.

На компьютерах, не оснащенных или оснащенных несовместимым модулем TPM, Windows 8 и Windows Server 2012 можно настроить на использование пароля разблокировки диска операционной системы. Для этого в редакторе объекта групповой политики нужно включить параметр политики **Этот параметр политики позволяет настроить использование паролей для дисков операционной системы** (Configure use of passwords for operating system drives), который находится в узле **Конфигурация компьютера\Административные шаблоны\Компоненты Windows\Этот параметр политики позволяет выбрать шифрование диска BitLocker\Диски операционной системы** (Computer Configuration\Administrative Templates\Windows Components\BitLocker Drive Encryption\Operating System Drives). Для пароля разблокировки можно задать минимальную длину и уровень сложности. По умолчанию минимальная длина пароля разблокировки составляет восемь символов. Уровень сложности может быть одним из следующих:

- **Требовать сложный пароль** (Require password complexity);
- **Разрешить сложность пароля** (Allow password complexity);
- **Не разрешать сложность пароля** (Do not allow password complexity).

Пароль разблокировки проверяется при включенной функциональности BitLocker и установке пароля, а также при смене пароля пользователем. При установленном требовании сложного пароля, пароль можно установить (и включить шифрование) только тогда, когда компьютер может подключаться к контроллеру домена и проверить сложность пароля. При установленном разрешении сложного пароля компьютер будет пытаться проверить сложность пароля при его установке, но при отсутствии доступных контроллеров домена позволит установить пароль любой сложности и включить шифрование.

На компьютерах, не оснащенных или оснащенных несовместимым модулем TPM, функциональность BitLocker также может использовать режим **Только ключ запуска** (Startup key only) или **Только сертификат на смарт-карте** (Smart card certificate only). В режиме **Только ключ запуска** требуется наличие флешки, содержащей ключ запуска. Прежде чем

включить компьютер, пользователь должен вставить флешку с ключом запуска в один из USB-портов компьютера. Хранящийся на флешке ключ запуска разблокирует компьютер.

В режиме **Только сертификат на смарт-карте** требуется наличие смарт-карты, содержащей действительный сертификат. Проверка действительности сертификата выполняется после включения компьютера. Действительный сертификат разблокирует компьютер.

Также важно отметить то обстоятельство, что обычные пользователи могут выполнять сброс ПИН-кода и пароля BitLocker для диска операционной системы и несъемных и съемных дисков данных. Это важное отличие Windows 8 от Windows 7, где для выполнения этих задач требуется обладать полномочиями администратора. Чтобы запретить обычным пользователям выполнять эти задания, нужно включить параметр политики **Этот параметр политики позволяет запретить обычным пользователям изменять ПИН-код или пароль** (Disallow standard users from changing the PIN or password), который находится в узле редактора объекта групповой политики **Конфигурация компьютера\Административные шаблоны\Компоненты Windows\Этот параметр политики позволяет выбрать шифрование диска BitLocker\Диски операционной системы**.

С тех пор как технология BitLocker была впервые применена в Windows Vista, в нее было внесено несколько важных изменений. В частности, для Windows 7 и более поздних версий Windows функциональность BitLocker позволяет выполнять следующее.

- Зашифровывать как тома FAT, так и тома NTFS, тогда как ранее можно было шифровать только тома NTFS. При шифровании томов FAT предоставляется возможность указать, можно ли эти тома разблокировать и просматривать на компьютерах под управлением Windows Vista или более поздних версий Windows. Эта возможность настраивается в групповой политике и включается при включении функциональности BitLocker. Узел объекта групповой политики **Конфигурация компьютера\Административные шаблоны\Компоненты Windows\Этот параметр политики позволяет выбрать шифрование диска BitLocker** содержит несколько отдельных параметров политики для более ранних версий Windows, которые позволяют разблокировать и просматривать несъемные и съемные диски с файловой системой FAT.
- Использовать с BitLocker агента восстановления данных. Эта возможность также настраивается в групповой политике. Агент восстановления данных позволяет разблокировать и восстановить зашифрованный том, используя личный сертификат агента восстановления или 48-разрядный пароль восстановления. По выбору, информацию восстановления можно сохранить в службе каталогов Active Directory. Узел объекта групповой политики **Конфигурация компьютера\Административные шаблоны\Компоненты Windows\Этот параметр политики позволяет выбрать шифрование диска BitLocker** содержит отдельные параметры для восстановления системных, несъемных и съемных дисков.
- Запрещать запись съемных носителей, не защищенных шифрованием BitLocker. Эта возможность также настраивается в групповой политике. При включенном параметре пользователи могут только просматривать незашифрованные съемные диски и просматривать и записывать зашифрованные.

В домене агентами восстановления по умолчанию являются администраторы домена. Домашние и рабочие группы не имеют агентов восстановления по умолчанию, но их можно назначить. При этом, чтобы пользователя можно было назначить агентом восстановления, он должен обладать личным сертификатом шифрования. Сертификат шифрования можно создать с помощью утилиты командной строки Cipher, а затем использовать этот сертификат для назначения агента восстановления в узле **Политики открытого ключа\Шифрование диска BitLocker** консоли **Локальная политика безопасности**.

Операционные системы Windows Vista и Windows 7 поддерживают алгоритм шифрования AES с диффузором (diffuser). В Windows 8 вместо этого алгоритма по умолчанию применяется 128-разрядное AES-шифрование. Также может использоваться 256-разрядное AES-шифрование, если включить параметр политики **Этот параметр политики позволяет выбрать метод шифрования диска и стойкость шифра** (Choose drive encryption method and cipher strength) и выбрать данный режим шифрования. Стойкость шифра необходимо задать до включения на диске функциональности BitLocker. Изменение стойкости шифра не имеет никакого эффекта, если диск уже был зашифрован или находится в процессе шифрования.

Аппаратное шифрование, безопасная загрузка и сетевое разблокирование

В Windows 8 и Windows Server 2012 в функциональность BitLocker было добавлено несколько усовершенствований. Управление большинством этих усовершенствований выполняется посредством параметров политики узла **Конфигурация компьютера\Административные шаблоны\Компоненты Windows\Этот параметр политики позволяет выбрать шифрование диска BitLocker** и будет рассмотрено в этом разделе.

В Windows 8 добавлена поддержка жестких дисков с аппаратным шифрованием, которые называются *зашифрованными жесткими дисками* (encrypted hard drives). Аппаратное шифрование выполняется с более высокой скоростью, чем программное, и перемещает бремя обработки с процессора компьютера на специализированный процессор на жестком диске. По умолчанию, если компьютер имеет функциональность аппаратного шифрования, Windows 8 будет использовать эту функциональность с BitLocker.

В групповой политике можно задать, разрешать ли программное шифрование при отсутствии возможности аппаратного шифрования, а также ограничить ли применяемые алгоритмы и стойкость шифрования только теми, которые поддерживаются аппаратно. Эти настройки выполняются включением и настройкой параметра политики **Этот параметр политики позволяет настроить использование аппаратного шифрования для съемных носителей с данными** (Configure use of hardware-based encryption for fixed data drives). Когда этот параметр включен и аппаратное шифрование недоступно, программное шифрование нужно задать явным образом, установив соответствующий флажок.

> ***Дополнительная информация***
>
> Параметр политики **Этот параметр политики позволяет выбрать метод шифрования диска и стойкость шифра** не применяется для аппаратного шифрования. Требуемые методы аппаратного шифрования задаются посредством параметра политики **Этот параметр политики позволяет настроить использование аппаратного шифрования для несъемных дисков с данными** узла **Несъемные диски с данными** (Fixed Data Drives). Алгоритм аппаратного шифрования задается при создании разделов жесткого диска.

Далее желательно настроить политику для управления разрешенными типами шифрования. Операционная система Windows 8 позволяет зашифровывать весь том или только используемое на нем пространство. Зашифровывание всего тома занимает больше времени, но обеспечивает более высокий уровень безопасности, т. к. защищается весь том. Шифрование используемого пространства защищает только ту часть диска, на которой хранятся данные. По умолчанию может использоваться любая из этих двух опций. Чтобы разрешить только один из этих методов шифрования, нужно включить и настроить параметр политики **Применить тип шифрования диска** (Enforce encryption type) для требуемого типа носителей. Существует отдельный вариант этого параметра для системных и несъемных/съемных дисков хранения данных.

ПРАКТИЧЕСКИЙ СОВЕТ

В среде с высокими требованиями к безопасности рекомендуется применять шифрование всего тома. На момент написания этой книги при шифровании только занимаемого пространства тома удаленные файлы отображаются как пустое пространство. В результате этого (если только этот недостаток не будет исправлен в будущем), до тех пор, пока пространство, занимаемое удаленными файлами, не будет перезаписано или очищено, информация из этих файлов может быть восстановлена с помощью специальных средств.

К шифрованию системных дисков применяется особый подход. Операционная система Windows 8 допускает предварительную установку BitLocker, чтобы шифрование можно было включить до начала установки операционной системы. Кроме этого, Windows 8 можно настроить на выполнение следующих операций.

- Требовать дополнительную аутентификацию при запуске. Если включить и настроить соответствующий параметр политики **Этот параметр политики позволяет настроить требование дополнительной проверки подлинности при запуске** (Require additional authentication at startup), пользователю необходимо будет ввести данные, даже если платформа не оснащена средствами, позволяющими ввод до загрузки операционной системы. Чтобы разрешить использование USB-клавиатуры на таких системах до загрузки операционной системы, следует включить параметр политики **Этот параметр политики позволяет включить использование проверки подлинности BitLocker, требующей предзагрузочного ввода с клавиатуры на планшетах** (Enable use of BitLocker authentication requiring preboot keyboard input on slates).
- Разрешить безопасную загрузку для проверки целостности. Безопасная загрузка используется по умолчанию для проверки целостности данных конфигурации загрузки (BCD) в соответствии с параметрами профиля проверки достоверности модуля TPM (также называемого политикой безопасной загрузки). При использовании безопасной загрузки игнорируются настройки параметра политики **Этот параметр политики позволяет настроить использование улучшенного профиля проверки данных конфигурации загрузки** (Use enhanced boot configuration data validation profile).

Параметры профиля проверки модуля TPM устанавливаются в зависимости от платформы. Для платформ с микропрограммным обеспечением на основе BIOS используется параметр политики **Этот параметр политики позволяет настроить профиль проверки платформы доверенного платформенного модуля для конфигурации встроенного ПО на базе BIOS** (Configure TPM platform validation profile for BIOS-based firmware configurations). А для UEFI-платформ применяется параметр политики **Этот параметр политики позволяет настроить профиль проверки платформы доверенного платформенного модуля для основных конфигураций встроенного ПО UEFI** (Configure TPM platform validation profile for native UEFI firmware configurations). При включении этих параметров политики указываются точные регистры PCR[1], подлежащие проверке в процессе загрузки (рис. 11.9).

Для BIOS-платформ Microsoft рекомендует проверять регистры PCR 0, 2, 4, 8, 9, 10 и 11, а для UEFI-платформ — регистры 0, 2, 4, 7 и 11. В обоих случаях для применения защиты BitLocker требуется проверка регистра PCR 11. Для поддержки безопасной загрузки UEFI-платформ требуется проверка регистра PCR 7 (для этого необходимо выбрать связанную опцию).

При использовании BitLocker для защиты компьютера может потребоваться дополнительная проверка подлинности при запуске. Обычно это означает, что пользователь должен иметь ключ запуска на флешке, ПИН-код запуска или оба варианта. Сетевая разблокировка

[1] Platform Configuration Registers — регистры конфигурации платформы.

предусматривает этот дополнительный уровень безопасности без необходимости предоставления ключа или ПИН-кода запуска посредством автоматического разблокирования системного диска при запуске компьютера при соблюдении следующих условий:

- на компьютере, защищаемом BitLocker, должен быть включен и активирован модуль TPM;
- компьютер должен быть подключен к доверенной проводной сети;
- компьютер должен быть членом домена и подключенным к нему;
- должен быть доступен сервер сетевой разблокировки с соответствующим сертификатом сетевой разблокировки.

Так как для работы сетевой разблокировки компьютер должен быть членом и подключенным к домену, аутентификация пользователя все равно требуется, когда компьютер не подключен к домену. Когда клиентский компьютер подключен к домену, для разблокировки системного диска он подключается к серверу сетевой разблокировки. Обычно сервером сетевой разблокировки является контроллер доменов, настроенный на использование и распределение сертификатов сетевой разблокировки клиентам. Сертификаты сетевой разблокировки в свою очередь используются для создания ключей сетевой разблокировки.

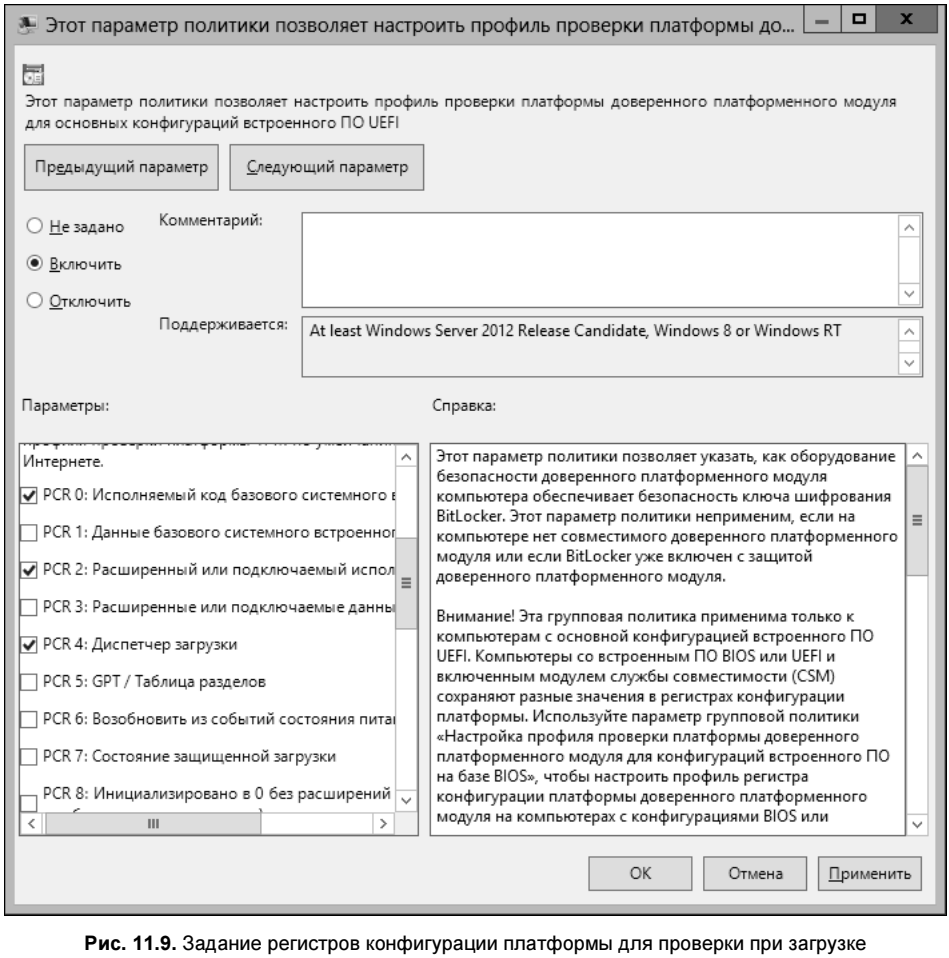


Рис. 11.9. Задание регистров конфигурации платформы для проверки при загрузке

Для распределения этого сертификата клиентам можно настроить контроллер домена. Для этого создайте сертификат X.509 для сервера (используя, например, утилиту certmgr.msc), а затем в параметре политики **Сертификат сетевой разблокировки шифрования диска BitLocker** (BitLocker Drive Encryption Network Unlock Certificate) добавьте этот сертификат к объекту групповой политики контроллера доменов. Этот параметр находится в узле редактора групповой политики **Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Политики открытого ключа\Шифрование диска BitLocker** (Computer Configuration\Windows Settings\Security Settings\Public Key Policies\BitLocker Drive Encryption).

Наконец, Windows 8 также позволяет предоставлять услуги BitLocker в процессе загрузки операционной системы из предзагрузочной среды WinPE. Важно отметить, что оболочка Windows PowerShell содержит модуль DISM, который можно импортировать. Так как этот модуль не поддерживает подстановочные знаки при поиске имен функциональностей, для вывода списка имен функциональностей можно использовать командлет `Get-WindowsOptionalFeatures`, как показано ниже:

```
get-windowsoptionalfeatures –online\ft
```

Чтобы полностью установить BitLocker и связанные средства управления, выполните следующую команду:

```
enable-windowsoptionalfeature –online –featurename bitlocker,
     bitlocker-utilities, bitlocker-networkunlock –all
```

Применение функциональности шифрования дисков BitLocker

Применение функциональности шифрования дисков BitLocker в организации изменяет способ работы администраторов и пользователей с компьютерами. Компьютер, на котором задействована эта функциональность, обычно требует вмешательства пользователя для загрузки операционной системы. В частности, пользователь должен ввести ПИН-код, вставить флешку, содержащую ключ запуска, или использовать смарт-карту, содержащую действительный сертификат. Вследствие этого требования, после задействования функциональности BitLocker больше нельзя выполнять задачи удаленного администрирования, требующие перезагрузки компьютера. Для этого может потребоваться содействие кого-либо с физическим доступом к компьютеру, чтобы предоставить необходимые данные для аутентификации.

Эту проблему можно обойти, настроив функциональность сетевой разблокировки на доверенных проводных сетях. Прежде чем использовать функциональность BitLocker, следует выполнить всестороннюю оценку компьютеров организации. Также необходимо разработать планы и процедуры для выполнения следующих задач:

- оценки различных методов аутентификации для BitLocker и применения их должным образом;
- определения, поддерживают ли компьютеры модуль TPM, и, следственно, какую конфигурацию BitLocker использовать — с модулем TPM или без него;
- хранения, использования и периодического изменения ключей шифрования, паролей восстановления и других механизмов проверки подлинности, используемых с BitLocker.

Также необходимо разработать процедуры для выполнения таких задач, как следующие:

- выполнение повседневных операций с дисками, зашифрованными посредством BitLocker;

- предоставление административной поддержки дискам, зашифрованным посредством BitLocker;
- восстановление компьютеров с дисками, зашифрованными посредством BitLocker.

При разработке этих процедур следует учитывать особенности шифрования BitLocker и требование иметь в наличии ПИН-коды, ключи запуска, смарт-карты с сертификатами и ключи восстановления при работе с компьютерами, оснащенными дисками, зашифрованными посредством BitLocker. После оценки компьютеров организации и разработки основных планов и процедур необходимо разработать конфигурационный план для применения шифрования дисков BitLocker.

Существует несколько реализаций функциональности BitLocker: первая версия функциональности BitLocker была выпущена с Windows Vista, с Windows Server 2008 и Windows 7 была выпущена обновленная версия, а с Windows 8 и Windows Server 2012 — еще одна обновленная версия. Хотя компьютеры под Windows 8 и Windows Server 2012 могут работать со всеми выпущенными версиями BitLocker, более ранние версии Windows не обязательно могут работать с последней версией этой функциональности. Например, чтобы разрешить доступ с более ранних версий Windows, может потребоваться выполнить соответствующие настройки в групповой политике.

Чтобы включить шифрование BitLocker на диске, содержащем операционную систему Windows, диск должен иметь, по крайней мере, два раздела:

- первый раздел используется функциональностью BitLocker. Он помечается активным и содержит файлы, необходимые для начала загрузки операционной системы. Этот раздел не зашифрован;
- второй раздел является основным разделом для операционной системы и пользовательских данных. Когда включается BitLocker, этот раздел зашифровывается.

Для версий BitLocker до Windows 7 разделы необходимо было создавать особым способом, чтобы обеспечить совместимость. Для Windows 7 и более поздних версий это не требуется. При установке Windows 7 и более поздних версий Windows дополнительный раздел создается автоматически в процессе установки. По умолчанию этот дополнительный раздел используется средой восстановления Windows. Но при включении шифрования BitLocker для системного диска, Windows обычно перемещает среду восстановления на системный раздел, а дополнительный раздел использует для нужд BitLocker.

Использование BitLocker для шифрования дисков не представляет никакого труда. Для компьютеров, оснащенных совместимым модулем TPM, необходимо инициализировать этот модуль *(см. разд. "Инициализация и подготовка модуля TPM для использования" ранее в этой главе)*, а затем нужно включить BitLocker. Для компьютеров, не оснащенных совместимым модулем TPM, нужно только включить BitLocker.

Для управления и содержания настроек модуля TPM и функциональности BitLocker можно использовать локальную групповую политику и групповую политику для службы каталогов Active Directory. Параметры групповой политики для служб TPM находятся в узле **Конфигурация компьютера\Административные шаблоны\Система\Службы доверенного платформенного модуля** (Computer Configuration\Administrative Templates\System\Trusted Platform Module Services) редактора групповой политики. Параметры групповой политики для функциональности BitLocker находятся в узле **Конфигурация компьютера\Административные шаблоны\Компоненты Windows\Этот параметр политики позволяет выбрать шифрование диска BitLocker** (Computer Configuration\Administrative Templates\Windows Components\BitLocker Drive Encryption) редактора групповой политики. Параметры политики для системных дисков и съемных/несъемных дисков для данных размещены в отдельных папках.

Параметры политик, которые желательно настроить, включают следующие:

- параметры политики **Службы доверенного платформенного модуля** (Trusted Platform Module Services):
  - **Настроить уровень сведений авторизации владельца TPM, доступных операционной системе** (Configure the level of TPM owner authorization information available to the operating system);
  - **Настроить список заблокированных команд TPM** (Configure the list of blocked TPM commands);
  - **Игнорировать список заблокированных команд TPM по умолчанию** (Ignore the default list of blocked TPM commands);
  - **Игнорировать локальный список заблокированных команд TPM** (Ignore the local list of blocked TPM commands);
  - **Индивидуальный порог блокировки обычных пользователей** (Standard User Individual Lockout Threshold);
  - **Длительность блокировки обычных пользователей** (Standard User Lockout Duration);
  - **Общий порог блокировки обычных пользователей** (Standard User Total Lockout Threshold);
  - **Включить резервное копирование TPM в доменные службы Active Directory** (Turn On TPM backup to Active Directory Domain Services);
- параметры политики **Этот параметр политики позволяет выбрать шифрование диска BitLocker** (BitLocker Drive Encryption):
  - **Этот параметр политики позволяет выбрать папку по умолчанию для пароля восстановления** (Choose default folder for recovery password);
  - **Этот параметр политики позволяет выбрать метод шифрования диска и стойкость шифра** (Choose drive encryption method and cipher strength);
  - **Запретить перезапись памяти при перезагрузке** (Prevent memory overwrite on restart);
  - **Этот параметр политики позволяет указать уникальные идентификаторы для организации** (Provide the unique identifiers for your organization);
  - **Этот параметр политики позволяет проверить согласованность правил использования сертификатов смарт-карт** (Validate smart card certificate usage rule compliance);
- параметры политики **Несъемные диски с данными** (Fixed Data Drives):
  - **Этот параметр политики позволяет разрешить доступ к несъемным дискам с данными, защищенными с помощью BitLocker, из более ранних версий Windows** (Allow access to BitLocker-protected fixed data drives from earlier versions of Windows);
  - **Этот параметр политики позволяет выбрать метод восстановления несъемных дисков, защищенных с помощью BitLocker** (Choose how BitLocker-protected fixed drives can be recovered);
  - **Этот параметр политики позволяет настроить использование аппаратного шифрования для несъемных дисков с данными** (Configure use of hardware-based encryption for fixed data drives);

- **Этот параметр политики позволяет настроить использование паролей для несъемных дисков с данными** (Configure use of passwords for fixed data drives);
- **Этот параметр политики позволяет настроить использование смарт-карт для несъемных дисков с данными** (Configure use of smart cards on fixed data drives);
- **Этот параметр политики позволяет запретить запись на несъемные диски, не защищенные BitLocker** (Deny write access to fixed drives not protected by BitLocker);
- **Применить тип шифрования диска к несъемным дискам с данными** (Enforce drive encryption type on fixed data drives);

♦ параметры политики **Диски операционной системы** (Operating System Drives):

- **Этот параметр политики позволяет разрешить использование улучшенных ПИН-кодов при запуске компьютера** (Allow enhanced PINs for startup);
- **Этот параметр политики позволяет вам разрешить сетевое разблокирование при запуске** (Allow network unlock at startup);
- **Разрешить защищенную загрузку для проверки целостности** (Allow secure boot for integrity validation);
- **Этот параметр политики позволяет выбрать метод восстановления дисков операционной системы, защищенных с помощью BitLocker** (Choose how BitLocker-protected operating system drives can be recovered);
- **Этот параметр политики позволяет установить минимальную длину ПИН-кода для запуска** (Configure minimum PIN length for startup);
- **Этот параметр политики позволяет настроить профиль проверки платформы доверенного платформенного модуля для конфигурации встроенного ПО на базе BIOS** (Configure TPM platform validation profile for BIOS-based firmware configurations);
- **Этот параметр политики позволяет настроить профиль проверки платформы доверенного платформенного модуля для основных конфигураций встроенного ПО UEFI** (Configure TPM platform validation profile for native UEFI firmware configurations);
- **Этот параметр политики позволяет настроить профиль проверки платформы доверенного платформенного модуля (Windows Vista, Windows Server 2008, Windows 7, Windows Server 2008 R2)** (Configure TPM platform validation profile (Windows Vista, Windows 7, Windows Server 2008, Windows Server 2008 R2));
- **Этот параметр политики позволяет настроить использование паролей для дисков операционной системы** (Configure use of passwords for operating system drives);
- **Этот параметр политики позволяет запретить обычным пользователям изменять ПИН-код или пароль** (Disallow standard users from changing the PIN or password);
- **Применить тип шифрования к дискам операционной системы** (Enforce drive encryption type on operating system drives);
- **Этот параметр политики позволяет включить использование проверки подлинности BitLocker, требующей предзагрузочного ввода с клавиатуры на планшетах** (Enable user of BitLocker authentication requiring preboot keyboard input on slates);
- **Этот параметр политики позволяет настроить требование дополнительной проверки подлинности при запуске** (Require additional authentication at startup);

- **Этот параметр политики позволяет настроить сброс данных проверки подлинности после восстановления BitLocker** (Reset platform validation data after BitLocker recovery);

♦ параметры политики **Съемные диски с носителями** (Removable Data Drives):

- **Этот параметр политики позволяет разрешить доступ к съемным носителям с данными, защищенными с помощью BitLocker, из более ранних версий Windows** (Allow access to BitLocker-protected removable data drives from earlier versions of Windows);
- **Этот параметр политики позволяет выбрать метод восстановления съемных носителей, защищенных с помощью BitLocker** (Choose how BitLocker-protected removable drives can be recovered);
- **Этот параметр политики позволяет настроить использование аппаратного шифрования для съемных носителей с данными** (Configure use of hardware-based encryption for removable data drives);
- **Этот параметр политики позволяет настроить использование паролей для съемных носителей с данными** (Configure use of passwords for removable data drives);
- **Этот параметр политики позволяет настроить использование смарт-карт на съемных носителях с данными** (Configure use of smart cards on removable data drives);
- **Этот параметр политики позволяет управлять использованием BitLocker на съемных носителях** (Control use of BitLocker on removable drives);
- **Этот параметр политики позволяет запретить запись на съемные носители, не защищенные BitLocker** (Deny write access to removable drives not protected by BitLocker);
- **Применить тип шифрования диска к съемным носителям с данными** (Enforce drive encryption type on removable data drives).

Служба каталогов Active Directory содержит расширения восстановления для модуля TPM и BitLocker для объектов `Computer`. Для модуля TPM расширения определяют одно свойство объекта `Computer`, которое называется `ms-TPM-OwnerInformation`. При инициализации модуля TPM или смене пароля его владельца хэш пароля владельца TPM-модуля можно сохранить, как значение атрибута `ms-TPM-OwnerInformation` связанного объекта `Computer`. Для функциональности BitLocker эти расширения определяют объекты `Recovery`, как дочерние объекты объекта `Computer`, и используются для хранения паролей восстановления и ассоциирования их с конкретными томами, зашифрованными посредством BitLocker.

По умолчанию Windows 8 сохраняет в реестре полные сведения авторизации владельца модуля TPM, большой двоичный объект делегирования административных полномочий модуля TPM и большой двоичный объект делегирования пользователя модуля TPM. Вследствие такого изменения, эту информацию больше не требуется сохранять отдельно для целей восстановления в службе каталогов Active Directory. Дополнительную информацию *см. в разд. "Управление и политики модуля TPM" ранее в этой главе*.

Чтобы обеспечить постоянную доступность информации восстановления для BitLocker, групповую политику можно настроить для сохранения этой информации в службе каталогов Active Directory. Процедура для этого следующая.

♦ Включите параметр политики **Этот параметр политики позволяет выбрать метод восстановления несъемных дисков, защищенных с помощью BitLocker**, приняв зна-

чения его опций по умолчанию, чтобы разрешить использование агента восстановления данных и сохранения информации восстановления в службе каталогов Active Directory.

- Включите параметр политики **Этот параметр политики позволяет выбрать метод восстановления дисков операционной системы, защищенных с помощью BitLocker**, приняв значения его опций по умолчанию, чтобы разрешить использование агента восстановления данных и сохранения информации восстановления в службе каталогов Active Directory.
- Включите параметр политики **Этот параметр политики позволяет выбрать метод восстановления съемных носителей, защищенных с помощью BitLocker**, приняв значения его опций по умолчанию, чтобы разрешить использование агента восстановления данных и сохранения информации восстановления в службе каталогов Active Directory.

Практический совет

Согласно требованиям стандарта FIPS[1], нельзя самому создавать или сохранять пароли восстановления для BitLocker. Вместо этого нужно настроить Windows на создание ключей восстановления. Соответствующий параметр, **Системная криптография: использовать FIPS-совместимые алгоритмы для шифрования, хэширования и подписывания** (System Cryptography: Use FIPS-compliant algorigthms for encryption, hashing, and signing), находится в узле **Локальные политики\Параметры безопасности** (Local Policies\Security Options) консоли редактора политики безопасности.

Чтобы настроить BitLocker для использования ключей восстановления, включите этот параметр в локальной или доменной групповой политике, как требуется. Когда этот параметр включен, пользователи могут только генерировать ключи восстановления.

Управление функциональностью BitLocker

Функциональность шифрования дисков BitLocker можно использовать как для системных томов, так и для томов, хранящих данные. При шифровании системных томов компьютер необходимо разблокировать при запуске, обычно используя для этого модуль TPM и сетевую разблокировку, когда компьютер подключен к домену, или модуль TPM, ключ запуска, ПИН-код запуска или любую обязательную или необязательную комбинацию всех перечисленных. Для обеспечения самых жестких мер безопасности, которые возможны, используйте все три метода проверки подлинности.

В текущей реализации BitLocker зашифровывать системный диск перед шифрованием дисков хранения данных не требуется. Операционная система подключает зашифрованные посредством BitLocker тома, как обычные тома, но требует либо ввода пароля, либо предоставления действительного сертификата на смарт-карте, чтобы разблокировать том.

Ключ шифрования для защищенного диска данных создается и сохраняется отдельно от системного тома и всех других защищенных томов данных. Чтобы операционная система могла подключать зашифрованные тома, цепочка ключей для защиты тома данных должна храниться в зашифрованном виде на томе операционной системы. Если операционная система переходит в режим восстановления, тома данных остаются заблокированными до тех пор, пока система не выйдет из этого режима.

Чтобы настроить BitLocker для применения, необходимо выполнить следующие операции:

1. Создать на жестком диске необходимые разделы и установить операционную систему (при настройке нового компьютера). Программа установки Windows создает требуемые

[1] Federal Information Processing Standard — федеральный (США) стандарт обработки информации.

разделы автоматически. Но данные BitLocker всегда должны храниться на активном системном томе.

2. Инициализировать и настроить модуль TPM компьютера (если компьютер оснащен таковым).
3. Включить функциональность шифрования дисков BitLocker (если требуется).
4. Проверить в микропрограммном обеспечении, что компьютер настроен для загрузки с привода жесткого диска, содержащего активный, системный и загрузочный разделы, а не с привода CD/DVD или флешки.
5. Включить и настроить функциональность шифрования дисков BitLocker.

> ***Примечание***
>
> При использовании учетной записи Microsoft на компьютере, не являющемся членом домена, имеется дополнительная возможность сохранения ключа восстановления на Windows Live SkyDrive. В этом случае учетная запись SkyDrive пользователя будет содержать папку для BitLocker, содержащую отдельный файл для каждого сохраненного ключа восстановления.

Включив и настроив шифрование BitLocker, можно использовать несколько способов содержания среды и выполнения восстановления.

Подготовка для шифрования посредством BitLocker

Как рассматривалось ранее, шифрование BitLocker можно применять как с модулем TPM, так и без него. Но в любом случае, прежде чем можно включать и настраивать функциональность BitLocker, необходимо выполнить определенные подготовительные работы.

Для версий Windows 7 Pro и Enterprise функциональность BitLocker должна устанавливаться по умолчанию при инсталляции операционной системы. Если по какой-либо причине эта функциональность не установилась, ее можно установить вручную с помощью мастера добавления компонентов. Для завершения установки функциональности нужно будет перезагрузить компьютер.

Определить готовность компьютера к использованию шифрования BitLocker можно из консоли управления этой функциональностью. Открыть ее можно, щелкнув в Панели управления по ссылке **Система и безопасность** и в открывшемся списке элементов этой категории выбрав ссылку **Шифрование диска BitLocker** (BitLocker Disk Encryption). Если система не настроена должным образом на использование этой функциональности, будет выведено соответствующее сообщение об ошибке. В этом случае обратите внимание на следующее:

- если содержимое сообщения об ошибке связано с модулем TPM на компьютере, оснащенном совместимым модулем TPM, *см. разд. "Включение модуля TPM" ранее в этой главе*, чтобы получить дополнительную информацию о состояниях модуля TPM и его включении в микропрограммном обеспечении;
- если содержимое сообщения об ошибке связано с модулем TPM на компьютере, не оснащенным или оснащенным несовместимым модулем TPM, нужно изменить настройки групповой политики компьютера, чтобы BitLocker можно было включить для использования без модуля TPM.

Параметры политики для шифрования BitLocker можно настроить в локальной или доменной групповой политике. В локальной политике настройки применяются к локальному объекту групповой политики компьютера. Для доменной политики настройки применяются к объекту групповой политики, обрабатываемому данным компьютером. При работе с доменной политикой также можно задать требования для компьютеров, оснащенных модулем TPM.

Настроить BitLocker для работы с использованием или без использования модуля TPM можно следующим образом:

1. В редакторе управления групповыми политиками откройте для редактирования требуемый объект групповой политики.
2. Разверните узел **Конфигурация компьютера\Административные шаблоны\Компоненты Windows\Этот параметр политики позволяет выбрать шифрование диска BitLocker\Диски операционной системы** и в правой панели редактора дважды щелкните на параметре **Этот параметр политики позволяет настроить требование дополнительной проверки подлинности при запуске**.

> ***Важно!***
>
> Существует несколько версий этого параметра, каждый из которых специфичный для определенной операционной системы. Выполняйте настройку той версии или версий этой политики, которая соответствует вашей рабочей среде и компьютерам, к которым эта политика будет применяться. Опции разных версий параметра слегка отличаются друг от друга, т. к. каждая версия Windows поддерживает слегка разные возможности модуля TPM.

3. В диалоговом окне параметра включите его, установив одноименный переключатель.
4. Далее, выполните одно из следующих действий.
   - Если требуется использовать BitLocker без модуля TPM, установите флажок **Этот параметр политики позволяет разрешить BitLocker без совместимого доверенного платформенного модуля** (Allow BitLocker without a compatible TPM). Это позволит использовать шифрование BitLocker на компьютере, вводя при запуске пароль или предоставляя ключ запуска.
   - Если требуется использовать BitLocker с модулем TPM, снимите флажок **Этот параметр политики позволяет разрешить BitLocker без совместимого доверенного платформенного модуля**. Это позволит использовать шифрование BitLocker на компьютере, предоставляя ключ запуска, ПИН-код запуска или оба.
5. На компьютере с совместимым модулем TPM при запуске можно использовать несколько разных методов проверки подлинности для предоставления дополнительной защиты зашифрованных данных. Эти методы проверки подлинности могут разрешаться или требоваться. В табл. 11.2 приведены разные комбинации использования модуля TPM с этими методами проверки подлинности. Доступность методов зависит от версии параметра политики, специфичной для конкретной версии Windows, для которого выполняется настройка.

Таблица 11.2. *Основные опции использования модуля TPM с BitLocker*

Настройка для				
При запуске компьютера	**Настройка запуска модуля TPM**	**Настройка ПИН-кода запуска модуля TPM**	**Настройка ключа запуска модуля TPM**	**Настройка ключа запуска модуля TPM и ПИН-кода**
Разрешить использовать модуль TPM при запуске	Разрешить модуль TPM	Запретить	Запретить	Запретить
Требовать использовать модуль TPM при запуске	Требовать модуль TPM	Запретить	Запретить	Запретить

Таблица 11.2 *(окончание)*

Настройка для				
При запуске компьютера	**Настройка запуска модуля TPM**	**Настройка ПИН-кода запуска модуля TPM**	**Настройка ключа запуска модуля TPM**	**Настройка ключа запуска модуля TPM и ПИН-кода**
Использовать модуль TPM только с ключом запуска	Разрешить или требовать модуль TPM	Разрешить или требовать ПИН-код запуска с модулем TPM	Запретить	Запретить
Использовать модуль TPM только с ПИН-кодом запуска	Разрешить или требовать модуль TPM	Запретить	Разрешить или требовать ключ запуска с модулем TPM	Запретить
Использовать модуль TPM только с ключом запуска и ПИН-кодом запуска	Разрешить или требовать модуль TPM	Запретить	Запретить	Разрешить или требовать ключ запуска и ПИН-код с модулем TPM
Разрешить модель TPM с любым другим методом проверки подлинности	Разрешить или требовать модуль TPM	Разрешить ПИН-код запуска с модулем TPM	Разрешить ключ запуска с модулем TPM	Разрешить ключ запуска и ПИН-код с модулем TPM

6. Нажмите кнопку **OK**, чтобы сохранить и применить выполненные настройки. Параметр с настройками будет применен при следующем использовании групповой политики.
7. Закройте редактор управления групповыми политиками. Чтобы немедленно применить групповую политику к компьютеру, на котором вы работаете в настоящий момент, выполните команду `gpudate.ex /force` в поле поиска панели **Приложения**.

Компьютеры, которые имеют ключ запуска или ПИН-код запуска, также имеют пароль или сертификат восстановления. Пароль или сертификат восстановления требуются на случай следующего:

- изменения информации запуска системы;
- необходимости переместить зашифрованный привод на другой компьютер;
- проблем с предоставлением пользователем правильного ключа запуска или ПИН-кода.

Управление и хранение пароля или сертификата восстановления нужно выполнять отдельно от ключа запуска или ПИН-кода. Хотя ключ запуска или ПИН-код запуска выдаются пользователям, пароль или сертификат восстановления должны находиться только у администраторов. Администраторам необходимо иметь пароль или сертификат восстановления для того, чтобы разблокировать зашифрованные данные на томе, если BitLocker перейдет в состояние блокировки. Обычно, если только не используется агент восстановления, пароль или сертификат восстановления является уникальным для данного шифрования BitLocker. Это означает, что его нельзя использовать для восстановления зашифрованных данных с других томов, зашифрованных посредством BitLocker, даже если они находятся на одном и том же компьютере. Чтобы повысить уровень безопасности, ключи запуска и данные для восстановления должны храниться отдельно от компьютера.

Когда на компьютере установлен компонент BitLocker, в Панели управления для него создается значок для открытия его консоли управления. Опции настройки для BitLocker зависят от того, установлен ли на компьютере модуль TPM, и от настроек групповой политики.

Включение BitLocker для несистемных дисков

Шифрование несистемных дисков позволяет защитить хранящиеся на них данные. С помощью BitLocker можно зашифровывать тома, отформатированные под FAT, FAT32, exFAT или NTFS. Сколько времени занимает зашифровать диск, зависит от объема данных, вычислительной мощности компьютера и уровня занятости компьютера.

Прежде чем включать BitLocker в групповой политике, следует настроить соответствующие параметры узла **Несъемные диски с данными**, а затем дождаться обновления групповой политики. Если включить BitLocker, не сделав этого, может возникнуть необходимость выключить его и снова включить, т. к. при включении BitLocker устанавливаются определенные флаги состояния и управления.

Если на компьютере установлены две операционные системы или зашифрованные диски переносятся между компьютерами, то, чтобы обеспечить доступ к дискам на других операционных системах или компьютерах, нужно включить параметр **Этот параметр политики позволяет разрешить доступ к несъемным дискам с данными, защищенными с помощью BitLocker, из более ранних версий Windows** (Allow access to BitLocker-protected fixed data drives from earlier versions of Windows). Разблокированные в другой системе диски доступны только для чтения. Чтобы обеспечить восстановление зашифрованного тома, необходимо разрешить работу агентов восстановления данных и сохранить информацию для восстановления в службе каталогов Active Directory.

Включить шифрование BitLocker для несистемного тома можно следующим образом:

1. В Проводнике Windows щелкните правой кнопкой мыши на требуемом диске и в контекстном меню выберите команду **Включить BitLocker**. Будет проведена проверка на соответствие компьютера требованиям BitLocker, в случае успеха которой выполнится инициализация диска.

   Примечание

   Если BitLocker для диска уже включен, вместо опции **Включить BitLocker** предлагается опция **Управление BitLocker**.

2. На странице **Выберите способы снятия блокировки диска** (Choose how you want to unlock this drive) открывшегося мастера шифрования BitLocker (рис. 11.10) установите один или оба флажка, а затем нажмите кнопку **Далее**.

   - **Использовать пароль для снятия блокировки диска** (Use a password to unlock the drive). Установите этот флажок, чтобы пользователю выводился запрос ввести пароль для разблокирования диска. Пароль позволяет разблокировать диск в любом месте, а также разрешает совместное использование диска несколькими пользователями.
   - **Использовать смарт-карту для снятия блокировки диска** (Use my smart card to unlock the drive). Установите этот флажок, чтобы для разблокировки диска использовать смарт-карту с предоставлением ее ПИН-кода. Так как для применения этой опции требуется наличие на компьютере устройства чтения смарт-карт, она обычно применяется для разблокировки дисков на работе, но не для дисков, которые могут использоваться в обстановке без доступа к такому устройству.

   Примечание

   После нажатия кнопки **Далее** мастер создает ключ восстановления. С помощью этого ключа можно разблокировать диск, если BitLocker обнаружит обстоятельство, не позволяющее ему разблокировать диск при загрузке компьютера. Обратите внимание, что ключ восстановления следует сохранить на съемном носителе или сетевом диске. Ключ восстановления нельзя сохранить на самом зашифрованном диске или в корневом каталоге несъемного диска.

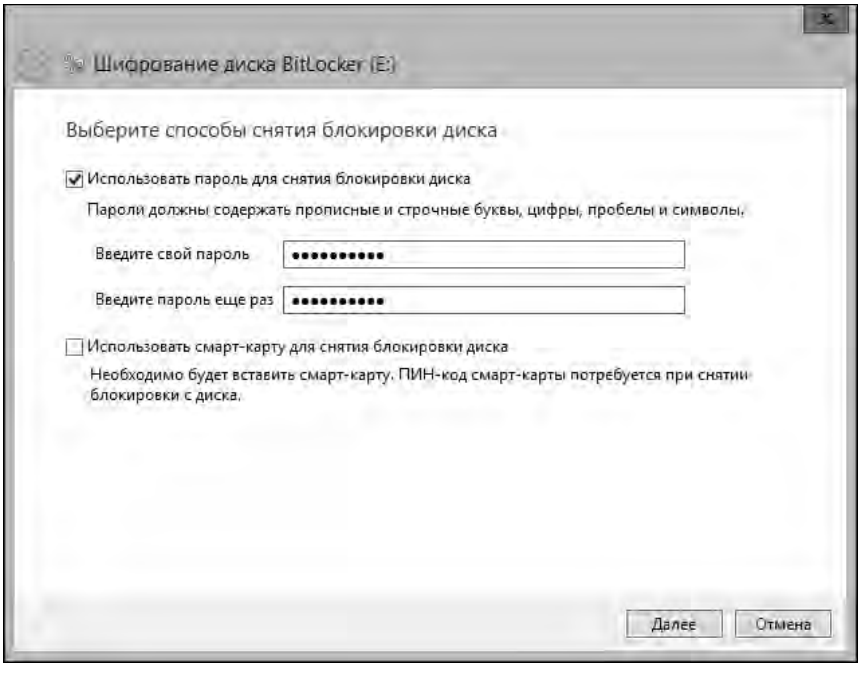


Рис. 11.10. Страница выбора способа разблокировки диска

3. На следующей странице мастера шифрования BitLocker, **Как вы хотите архивировать свой ключ восстановления?** (How do you want to back up you recovery key?), укажите, где сохранить ключ восстановления. Желательно сохранить его на флешке или другом съемном носителе.
4. Также предоставляется опция сохранить ключ восстановления в файл на другом диске компьютера, распечатать его, или сделать то и другое. Щелкните по ссылке требуемой опции, а затем следуйте выводимым инструкциям, чтобы сохранить или распечатать ключ восстановления. Завершив сохранение или распечатку ключа восстановления, нажмите кнопку **Далее**.
5. Если это разрешено в групповой политике, можно выбрать шифрование всего диска или только занятого места на диске. Установив требуемую опцию, нажмите кнопку **Далее**. Шифрование только занятого места диска выполняется быстрее, чем шифрование всего диска. Эта опция также рекомендуется для более новых компьютеров и дисков (за исключением сред с высокими требованиями к обеспечению безопасности).
6. На следующей странице мастера, **Зашифровать этот диск?** (Are your ready to encrypt this drive), нажмите кнопку **Начать шифрование** (Start Encrypting). Будет запущен процесс шифрования диска, длительность которого зависит от объема зашифровываемых данных и других факторов.

Но процесс шифрования можно приостанавливать и возобновлять, поэтому в случае необходимости компьютер можно выключить, прежде чем шифрование будет завершено. При следующем включении компьютера шифрование будет возобновлено. Состояние шифрования поддерживается также в случае потери питания.

Использование BitLocker с флешками

Шифрование флешек обеспечивает сохранность содержащихся на них данных от несанкционированного доступа. С помощью BitLocker можно зашифровывать флешки, отформатированные под FAT, FAT32, exFAT или NTFS. Сколько времени занимает зашифровать флешку, зависит от ее размера, вычислительной мощности компьютера и уровня занятости компьютера.

Прежде чем включать BitLocker, в групповой политике следует настроить соответствующие параметры узла **Съемные носители с данными**, а затем дождаться обновления групповой политики. Если включить BitLocker, не сделав этого, его может понадобиться выключить и снова включить, т. к. при включении BitLocker устанавливаются определенные флаги состояния и управления.

Чтобы обеспечить восстановление зашифрованной флешки, необходимо разрешить работу агентов восстановления данных и сохранить информацию для восстановления в службе каталогов Active Directory. Чтобы обеспечить доступ к флешке в других операционных системах или компьютерах, нужно включить параметр **Этот параметр политики позволяет разрешить доступ к съемным носителям с данными, защищенными с помощью BitLocker, из более ранних версий Windows** (Allow access to BitLocker-protected removable data drives from earlier versions of Windows). Разблокированные в других системах носители доступны только для чтения.

Включить шифрование BitLocker для флешки можно следующим образом:

1. Вставьте флешку в разъем USB-порта. В Проводнике Windows щелкните на значке флешки правой кнопкой мыши и в контекстном меню выберите команду **Включить BitLocker**. Будет проведена проверка на соответствие компьютера требованиям BitLocker, в случае успеха которой выполнится инициализация диска.
2. На странице **Выберите способы снятия блокировки диска** открывшегося мастера шифрования BitLocker выберите одну или обе из следующих опций, а затем нажмите кнопку **Далее**.
   - **Использовать пароль для снятия блокировки диска**. Установите этот флажок, чтобы пользователю выводился запрос ввести пароль для разблокирования диска. Использование пароля позволяет разблокировать диск в любом месте, а также разрешает совместное использование диска несколькими пользователями.
   - **Использовать смарт-карту для снятия блокировки диска.** Установите этот флажок, чтобы для разблокировки диска использовать смарт-карту с предоставлением ее ПИН-кода. Так как для применения этой опции требуется наличие на компьютере устройства чтения смарт-карт, она обычно применяется для разблокировки дисков на работе, но не для дисков, которые могут использоваться в обстановке без доступа к такому устройству.
3. На следующей странице мастера, **Как вы хотите архивировать свой ключ восстановления?**, щелкните на опции **Сохранить в файл** (Save the recovery key to a file).
4. В открывшемся диалоговом окне **Сохранение ключа восстановления BitLocker как** (Save BitLocker recovery key as) укажите расположение сохраняемого ключа восстановления и нажмите кнопку **Сохранить**.
5. Ключ восстановления также можно распечатать. Завершив сохранение или распечатку ключа восстановления, нажмите кнопку **Далее**.
6. Если это разрешено в групповой политике, можно выбрать шифрование всего носителя или только занятого места на носителе. Установив требуемую опцию, нажмите кнопку

Далее. Шифрование только занятого места носителя выполняется быстрее, чем шифрование всего носителя. Эта опция также рекомендуется для более новых компьютеров и носителей (за исключением сред с высокими требованиями к обеспечению безопасности).

7. На следующей странице мастера, **Зашифровать этот диск?**, нажмите кнопку **Начать шифрование**. Если флешку понадобится извлечь перед тем, как будет завершен процесс шифрования, приостановите шифрование, нажав кнопку **Пауза**. Шифрование можно будет продолжить в дальнейшем, нажав кнопку **Продолжить**. Не извлекайте флешку иным образом, пока процесс шифрования не будет завершен. Длительность процесса шифрования диска зависит от объема зашифровываемых данных и других факторов.

Процесс шифрования выполняет следующие действия:

1. Записывает на флешку файл aurorun.inf, средство чтения BitLocker To Go и файл ReadMe.txt.
2. Создает виртуальный том, содержащий зашифрованное содержимое флешки.
3. Зашифровывает виртуальный том, чтобы обезопасить его содержимое. Скорость шифрования флешек составляет 6—10 минут на гигабайт. Процесс шифрования можно приостанавливать, а затем возобновлять при условии, что флешка не извлекается из разъема.

Когда зашифрованная с помощью BitLocker флешка вставляется в USB-разъем компьютера под управлением Windows 8, на безопасном рабочем столе выводится сообщение о том, что она заблокирована (рис. 11.11).

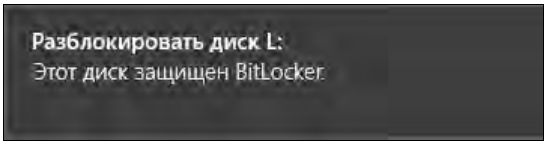


Рис. 11.11. Сообщение, выводимое при подключении зашифрованной BitLocker флешки

Рис. 11.12. Диалоговое окно для разблокировки зашифрованной BitLocker флешки

Если это сообщение закроется, прежде чем вы успеете щелкнуть по нему, просто извлеките, а затем снова вставьте флешку.

Щелчок по сообщению открывает диалоговое окно BitLocker (рис. 11.12), которое также выводится на безопасном рабочем столе.

Введите в текстовое поле пароль, чтобы разблокировать флешку. Чтобы не вводить пароль при каждом подключении флешки, щелкните по ссылке **Дополнительные параметры**,

чтобы отобразить опцию **Автоматически разблокировать на этом ПК** (Automatically unlock on this computer). Установка этого флажка сохраняет пароль в зашифрованном файле на системном диске компьютера. Наконец, нажмите кнопку **Разблокировать**, чтобы получить доступ к флешке.

Если вы забыли или потеряли пароль для флешки, но у вас есть ключ восстановления, щелкните по ссылке **Дополнительные параметры** и в расширенном представлении окна разблокировки щелкните по ссылке **Введите ключ восстановления** (Enter recovery key). В следующем окне введите 48-цифровой ключ восстановления и нажмите кнопку **Разблокировать** (Unlock). Этот ключ сохраняется в тестовом файле ключа восстановления.

Задействование BitLocker для системных дисков

Прежде чем приступать к шифрованию системного диска, необходимо извлечь все загрузочные носители из приводов CD/DVD компьютера, а также извлечь все флешки и другие съемные носители на флеш-памяти. После этого можно включить шифрование BitLocker на системном диске, выполнив следующую процедуру:

1. В Проводнике Windows щелкните правой кнопкой мыши по значку системного диска и в контекстном меню выберите команду **Включить BitLocker**. Windows выполнит проверку компьютера и диска на возможность применения BitLocker. В случае успешного результата проверки на следующей странице мастера, **Настройка шифрования дисков BitLocker**, предоставляется возможность продолжить процесс включения BitLocker. Нажмите на этой странице кнопку **Далее**.

   Примечание

   Если BitLocker для диска уже включен, вместо опции **Включить BitLocker** предлагается опция **Управление BitLocker**. Как часть процесса настройки BitLocker, Windows подготавливает необходимый для BitLocker дополнительный раздел, если это требуется. Если такой дополнительный раздел уже существует, но содержит среду восстановления Windows, эта среда перемещается на системный диск, а затем система использует этот раздел для нужд BitLocker.

   Примечание

   Если компьютер не оснащен модулем TPM, чтобы разрешить применение BitLocker на системном диске, необходимо включить параметр **Этот параметр политики позволяет настроить требование дополнительной проверки подлинности при запуске**, а затем установить в окне настройки параметра флажок **Этот параметр политики позволяет разрешить BitLocker без совместимого доверенного платформенного модуля**.

2. По завершению подготовки диска для BitLocker система сообщает о необходимости перезагрузки, а после перезагрузки возобновляет работу мастера BitLocker на странице настройки способов разблокировки диска при запуске (рис. 11.13). Продолжите процедуру включения BitLocker, согласно одной из изложенных далее процедур. Если компьютер не оснащен модулем TPM, опции разблокировки при запуске будут несколько иными. В частности, будут доступны только первые две опции — использование пароля или ключа запуска на флешке.

Если компьютер оснащен модулем TPM, BitLocker можно использовать для выполнения основных проверок целостности тома, не требуя никаких дополнительных ключей. В этой конфигурации BitLocker защищает системный диск, зашифровывая его. Эта конфигурация обеспечивает:

- предоставление доступа к диску пользователям, которые могут выполнять вход в операционную систему;

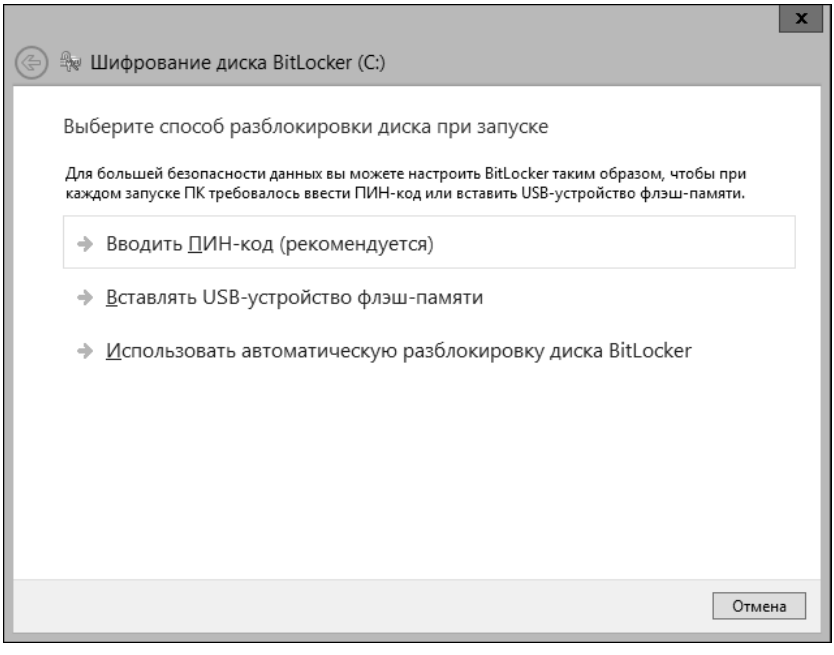


Рис. 11.13. Страница для настройки способов разблокировки системного диска при запуске компьютера

- предотвращение доступа к данным диска несанкционированными лицами, имеющими физический доступ к компьютеру, выполнив загрузку компьютера альтернативной операционной системой;
- возможность использования компьютера как с модулем TPM для предоставления дополнительной безопасности при запуске, так и без него;
- отсутствие требования пароля или смарт-карты с ПИН-кодом.

Для использования BitLocker без дополнительных ключей применяется следующая процедура:

1. На странице мастера **Выберите способ разблокировки диска при запуске** (Choose how to unlock your drive at startup) щелкните по ссылке **Использовать автоматическую разблокировку диска BitLocker** (Let BitLocker automatically unlock my drive).
2. На следующей странице мастера, **Как вы хотите архивировать свой ключ восстановления?**, щелкните на опции **Сохранить в файл**.
3. В открывшемся диалоговом окне **Сохранение ключа восстановления BitLocker как** укажите размещение флешки или сетевого диска для хранения ключа восстановления и нажмите кнопку **Сохранить**. Не используйте для хранения ключа восстановления флешку, зашифрованную посредством BitLocker.
4. Также предоставляется опция сохранить ключ восстановления в файл на другом диске компьютера, распечатать его или сделать то и другое. Щелкните по ссылке требуемой опции, а затем следуйте выводимым инструкциям, чтобы сохранить или распечатать ключ восстановления. Завершив сохранение или распечатку ключа восстановления, нажмите кнопку **Далее**.
5. Если это разрешено в групповой политике, можно выбрать шифрование всего диска или только занятого места на нем. Установив требуемую опцию, нажмите кнопку **Далее**.

Шифрование только занятого места диска выполняется быстрее, чем шифрование всего диска. Эта опция также рекомендуется для более новых компьютеров и дисков (за исключением сред с высокими требованиями к обеспечению безопасности).

6. На следующей странице мастера, **Зашифровать этот диск?**, нажмите кнопку **Начать шифрование**. Длительность процесса шифрования диска зависит от объема зашифровываемых данных и других факторов.

Чтобы повысить уровень безопасности, можно требовать дополнительную проверку подлинности при запуске системы. Эта конфигурация обеспечивает следующее:

- разрешает доступ к диску только тем пользователям, которые могут предоставить действительный ключ;
- предотвращает доступ к данным диска несанкционированным лицам, имеющим физический доступ к компьютеру, выполнив загрузку компьютера альтернативной операционной системой;
- возможность использования компьютера как с модулем TPM для предоставления дополнительной безопасности при запуске, так и без него;
- требовать пароль или смарт-карту с ПИН-кодом;
- факультативно использовать сетевую разблокировку диска, когда компьютер подключен к домену.

Включить шифрование BitLocker с использованием ключа запуска можно следующим образом:

1. Вставьте флешку в USB-разъем компьютера. Не используйте флешку, зашифрованную посредством BitLocker.
2. На странице мастера **Выберите способ разблокировки диска при запуске** щелкните на опции **Вставлять USB-устройство флеш-памяти** (Insert a USB flash drive).
3. На следующей странице мастера, **Сохраните ключ запуска** (Back up your startup key), выберите требуемую флешку и нажмите кнопку **Сохранить**.
4. Далее нужно сохранить ключ восстановления. Так как ключ восстановления не следует хранить на той же самой флешке, что ключ запуска, извлеките первую флешку и вставьте другую.

> ***Примечание***
>
> Ключ запуска имеет другое назначение, чем ключ восстановления. Ключ запуска используется для запуска компьютера, а ключ восстановления требуется для разблокировки компьютера, если BitLocker перейдет в режим восстановления. Это может произойти в том случае, если BitLocker считает, что пока компьютер был выключен, были попытки получить доступ к содержимому зашифрованного диска в обход BitLocker.

5. На следующей странице мастера, **Как вы хотите архивировать свой ключ восстановления?**, щелкните на опции **Сохранить в файл**.
6. В открывшемся диалоговом окне **Сохранение ключа восстановления BitLocker как** укажите размещение флешки для хранения ключа восстановления и нажмите кнопку **Сохранить**. Не извлекайте флешку с ключом восстановления.
7. Также предоставляется опция сохранить ключ восстановления в файл на сетевом диске, распечатать его или сделать то и другое. Щелкните по ссылке требуемой опции, а затем следуйте выводимым инструкциям, чтобы сохранить или распечатать ключ восстановления. Завершив сохранение или распечатку ключа восстановления, нажмите кнопку **Далее**.

8. Если это разрешено в групповой политике, можно выбрать шифрование всего диска или только занятого места на нем. Установив требуемую опцию, нажмите кнопку **Далее**. Шифрование только занятого места диска выполняется быстрее, чем шифрование всего диска. Эта опция также рекомендуется для более новых компьютеров и дисков (за исключением сред с высокими требованиями к обеспечению безопасности).
9. На странице мастера **Зашифровать этот диск?** проверьте, что установлен флажок **Запустить проверку системы BitLocker** (Run BitLocker system check), а затем нажмите кнопку **Далее**.
10. В открывшемся окне запроса подтвердите перезагрузку компьютера, нажав кнопку **Перезагрузить сейчас** (Restart now). Выполнится перезапуск компьютера, и BitLocker проверит, что компьютер совместим с BitLocker и готов к применению шифрования. Если компьютер не отвечает требованиям для применения шифрования, появится сообщение об ошибке с указанием решить проблему, чтобы можно было завершить данную процедуру. Если же компьютер готов к шифрованию, начинается процесс шифрования диска и выведется диалоговое окно с индикатором прогресса. Нажав кнопку **Закрыть**, это окно можно свернуть в значок в области уведомлений на панели задач. Поместив указатель мыши над этим значком, можно получить сведения о процессе шифрования. А щелчок на этом значке снова восстанавливает окно с индикатором хода процесса шифрования. Также предоставляется возможность приостановления и возобновления процесса шифрования. Зашифровка диска занимает приблизительно 1 минуту на гигабайт.

    По завершению процесса системный диск будет зашифрован, а также будет создан ключ восстановления, уникальный для данного диска. При следующем включении компьютера в USB-разъем компьютера должна быть вставлена флешка, содержащая ключ запуска, или же компьютер должен быть подключен к доменной сети, чтобы выполнить сетевую разблокировку. Если требуемая для запуска компьютера флешка с ключом запуска отсутствует, чтобы получить доступ к системному диску, потребуется использовать режим восстановления и предоставить ключ восстановления.

Включить шифрование BitLocker с использованием ПИН-кода запуска можно следующим образом:

1. На странице мастера **Выберите способ разблокировки диска при запуске** щелкните на опции **Вводить ПИН-код** (Enter a PIN).
2. На следующей странице, **Введите ПИН-код**, введите и подтвердите ПИН-код. Это может быть любой номер, содержащий от 4 до 20 цифр. ПИН-код хранится на компьютере.
3. Вставьте в USB-разъем компьютера флешку, на которой сохраните ключ восстановления, а затем нажмите кнопку **Задать ПИН-код** (Set PIN). Не используйте флешку, зашифрованную посредством BitLocker.
4. Далее выполните шаги 5—9 предыдущей процедуры.

По завершению процесса системный диск будет зашифрован, а также будет создан ключ восстановления, уникальный для данного диска. Если был создан ключ запуска или ПИН-код, для запуска компьютера потребуется ввести ключ или код (или же компьютер должен быть подключен к доменной сети и использовать сетевую разблокировку). В противном случае запуск будет выполняться обычным образом, если только не будет изменений в модуле TPM или этот модуль будет недоступным, или в случае попытки несанкционированного изменения содержимого диска, пока компьютер был выключен. В таком случае компьютер переходит в режим восстановления, и понадобится ввести ключ восстановления, чтобы разблокировать компьютер.

Управление, поиск и устранение неполадок BitLocker

Определить, используется ли шифрование BitLocker для системного диска, диска данных или съемного носителя можно в консоли **Шифрование диска BitLocker**. Открыть эту консоль можно, щелкнув в Панели управления по ссылке **Система и безопасность**, а в следующем окне — ссылку **Шифрование диска BitLocker**. В этой консоли отображается состояние шифрования BitLocker для всех дисков системы, как показано в примере на рис. 11.14.

Для правильной работы шифрования BitLocker необходимо, чтобы работала **Служба шифрования дисков BitLocker**. Обычно она настраивается на автоматический запуск и исполняется под системной учетной записью **Локальная система**.

А для использования с BitLocker смарт-карт необходимо, чтобы работала служба **Смарт-карта**. Обычно она настраивается на ручной запуск и исполняется под системной учетной записью **Локальная система**.

После создания для компьютера ключа или ПИН-кода запуска и ключа восстановления можно создать дубликат ключа запуска, ПИН-кода запуска или ключа восстановления в качестве резервной копии, используя соответствующие опции окна **Шифрование диска BitLocker**.

Примечание

Это окно также можно открыть, щелкнув правой кнопкой мыши в Проводнике Windows на значке диска, зашифрованного BitLocker, и выбрав в контекстном меню команду **Управление BitLocker**. (Если диск не зашифрован посредством BitLocker, для него отображается команда **Включить BitLocker**.)

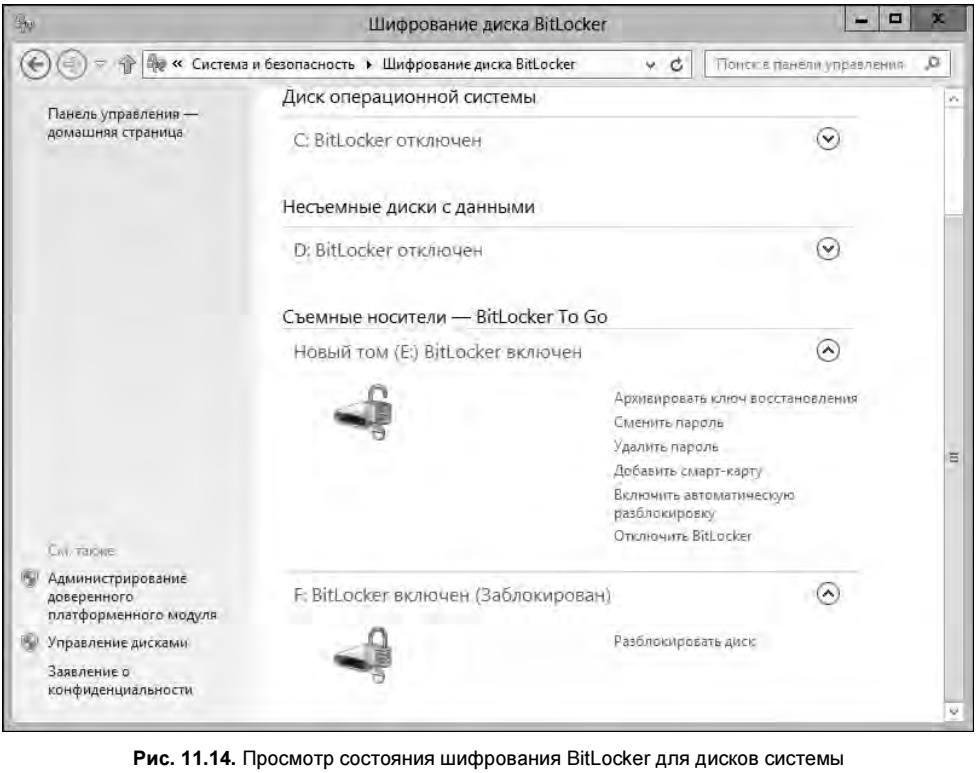


Рис. 11.14. Просмотр состояния шифрования BitLocker для дисков системы

Предоставляемые опции управления зависят от типа диска и его параметров шифрования. Доступные опции включают следующие.

- **Архивировать ключ восстановления** (Back up recovery key). Позволяет сохранить ключ восстановления в файл или распечатать его. Щелкните на этой опции и следуйте выводимым инструкциям.
- **Сменить пароль** (Change password). Позволяет сменить пароль шифрования. Щелкните на этой опции, введите в соответствующие поля старый пароль, новый пароль и подтверждение нового пароля, а затем нажмите кнопку **Изменить пароль**.
- **Удалить пароль** (Remove password). Позволяет удалить требование ввода пароля для разблокировки диска. Удалить пароль можно только в том случае, если существует другой способ разблокировки диска.
- **Добавить смарт-карту** (Add a smart card). Позволяет добавить смарт-карту, как способ разблокировки диска. Щелкните на этой опции и следуйте выводимым инструкциям.
- **Удалить смарт-карту** (Remove smart card). Позволяет удалить требование предоставления смарт-карты для разблокировки диска.
- **Изменить смарт-карту** (Change smart card). Позволяет изменить смарт-карту, используемую для разблокировки диска. Щелкните на этой опции и следуйте выводимым инструкциям.
- **Включить автоматическую разблокировку** (Turn on auto-unlock). Позволяет включить автоматическую разблокировку диска.
- **Отключить автоматическую разблокировку** (Turn off auto-unlock). Позволяет отключить автоматическую разблокировку диска.
- **Отключить BitLocker** (Turn off BitLocker). Отключает BitLocker и расшифровывает диск.

Восстановление данных, зашифрованных посредством BitLocker

Если для зашифрованного посредством BitLocker диска компьютер переходит в режим восстановления, необходимо разблокировать компьютер. Для разблокирования компьютера посредством ключа восстановления, сохраненного на флешке, применяется следующая процедура:

1. Включите компьютер. Если компьютер заблокирован, откроется консоль восстановления BitLocker.
2. В ответ на запрос вставьте флешку с ключом восстановления в USB-разъем компьютера и нажмите клавишу <Enter>.
3. Компьютер должен автоматически разблокироваться и перезагрузиться, без необходимости вводить ключ восстановления вручную.

Если ключ восстановления был сохранен на диске другого компьютера или съемном носителе, файл ключа восстановления можно открыть и проверить на другом компьютере. Чтобы найти правильный файл ключа восстановления, в консоли восстановления заблокированного компьютера посмотрите идентификатор пароля и запишите его. Файл, содержащий ключ восстановления, содержит этот идентификатор, как вторую часть своего имени, после части **Ключ восстановления BitLocker**. Откройте этот файл и найдите в нем ключ восстановления.

Чтобы разблокировать компьютер, введя вручную ключ восстановления, выполните следующие действия:

1. Включите компьютер. Если компьютер заблокирован, откроется консоль восстановления BitLocker.

2. Введите ключ восстановления и нажмите клавишу <Enter>. Компьютер должен автоматически разблокироваться и перезагрузиться.

В случае нескольких неудачных попыток ввода ключа восстановления компьютер может заблокироваться. В таком случае в консоли восстановления дважды нажмите клавишу <Esc>, чтобы выйти из режима восстановления и выключить компьютер. Компьютер также может заблокироваться в случае ошибки, связанной с модулем TPM, или при изменении данных загрузки. В таком случае процесс загрузки прерывается на очень раннем этапе, перед запуском операционной системы. На этом этапе заблокированный компьютер может не принимать ввод стандартных цифровых клавиш. В таком случае для ввода ключа восстановления нужно использовать функциональные клавиши. Иными словами, клавиши <F1>—<F9> представляют цифры 1—9, а клавиша <F10> — цифру 0.

Приостановка и отключение шифрования BitLocker

Когда нужно настроить параметры модуля TPM или внести модификации в другие параметры системы, может быть необходимым сначала временно отключить шифрование системного диска. Приостановить шифрование дисков данных нельзя, можно только полностью отключить.

Приостановить шифрование BitLocker системного диска можно следующим образом:

1. В Панели управления щелкните по ссылке **Система и безопасность**, а в открывшемся списке элементов этой категории выберите ссылку **Шифрование диска BitLocker**.
2. В разделе опций системного диска щелкните по ссылке **Выключить шифрование BitLocker**.
3. В открывшемся диалоговом окне **Укажите требуемый уровень расшифровки** (What level of decryption do you want?) выберите опцию **Отключение программы шифрования диска BitLocker** (Disable BitBlocker drive encryption).

Выполнение этой процедуры временно отключает шифрование BitLocker для системного диска.

Отключить шифрование BitLocker диска данных и расшифровать диск можно следующим образом:

1. В Панели управления щелкните по ссылке **Система и безопасность**, а в открывшемся списке элементов этой категории выберите ссылку **Шифрование диска BitLocker**.
2. В разделе опций требуемого диска данных щелкните по ссылке **Выключить шифрование BitLocker** (Turn off BitLocker drive encryption).
3. В открывшемся диалоговом окне **Укажите требуемый уровень расшифровки** выберите опцию **Расшифровать диск** (Decrypt the volume).

Отключить шифрование BitLocker и расшифровать съемный носитель можно следующим образом:

1. В Панели управления щелкните по ссылке **Система и безопасность**, а в открывшемся списке элементов этой категории выберите ссылку **Шифрование диска BitLocker**.
2. В разделе опций требуемого съемного диска щелкните по ссылке **Выключить шифрование BitLocker**.
3. В открывшемся диалоговом окне **Укажите требуемый уровень расшифровки** выберите опцию **Расшифровать диск**.

ГЛАВА 12

Управление дисковыми приводами и файловыми системами

Большинство компьютеров оснащено разными типами дисковых приводов, включая внутренние и внешние приводы. Основным устройством хранения данных обычно является внутренний дисковый привод. В большинстве случаев первый установленный привод жестких дисков помечается как `Диск 0`. При установке дополнительных приводов жестких дисков они помечаются как `Диск 1`, `Диск 2` и т. д. В этой главе рассматриваются инструменты и методы для управления жесткими дисками и файловыми системами. В частности, обсуждается разбиение жестких дисков на разделы и их форматирование, а также преобразование дисков из одного типа в другой. Также рассматриваются функциональности Windows 8, которые влияют на использование дисков, включая Windows ReadyBoost, Windows ReadyDrive и Windows SuperFetch.

Основы управления дисками

В операционной системе Windows 8 жесткие диски могут использоваться как *базовые* (basic) или *динамические* (dynamic).

- **Базовые диски.** Диски этого типа широко использовались в прошлом; их можно разбивать на несколько разделов. *Раздел* (partition) представляет собой логическую часть диска, которая работает как отдельный физический диск. Чтобы использовать раздел диска, его нужно сначала отформатировать под определенную файловую систему и присвоить ему букву диска. Отформатированный раздел называется *базовым томом* (basic volume) и отображается как локальный диск компьютера. В Windows 8 базовые диски могут иметь как *основные* (primary), так и *расширенные* (extended) разделы. Основной раздел используется для установки операционной системы. Доступ к основному разделу осуществляется напрямую, по его букве диска. Основной раздел нельзя разбивать на дополнительные разделы. Доступ к расширенному разделу выполняется косвенным образом. В расширенном разделе нужно дополнительно создать один или несколько логических дисков, к которым можно обращаться, опять же, как к отдельным физическим дискам.
- **Динамические диски.** Динамические диски позволяют выполнять основные задачи по обслуживанию компьютера без необходимости перезагрузки. Подобно базовым дискам, динамические диски можно разбивать на логические части. Но разбивка выполняется не на разделы, а на *тома* (volume). Том очень похож на раздел. Наиболее часто используются простые (simple) тома. *Простой том* — это том, состоящий из всего физического диска; такой том можно использовать для запуска операционной системы и для хране-

ния общих данных. Можно также использовать другие типы томов, включая тома, которые охватывают несколько физических дисков одним логическим томом. Такие тома называются *охватывающими* или *составными* (spanned volume). Подобно разделу или логическому диску, прежде чем использовать том динамического диска, его нужно отформатировать и присвоить ему букву. Отформатированный том называется *динамическим томом* (dynamic volume) и отображается как локальный диск компьютера. Динамический том, охватывающий несколько физических дисков, отображается как один логический диск и обозначается одной буквой.

Тип диска можно преобразовывать с базового в динамический и наоборот. При преобразовании базового диска в динамический разделы автоматически преобразуются в тома соответствующего диска и утеря данных не происходит. Преобразование динамического диска в базовый не такое безболезненное. Чтобы динамический диск сделать базовым, на нем нужно удалить все тома. Но при этом также удалится вся содержащаяся на них информация, поэтому, если ее нужно сохранить, перед тем как выполнять преобразование, следует создать резервную копию.

Кроме разных типов дисков также существуют различные типы разделов дисков, которые могут быть либо типа MBR[1], либо типа GPT[2]. Хотя как 32-разрядная, так и 64-разрядная версии Windows 8 поддерживают оба типа разделов, более ранние версии Windows не поддерживают разделов типа GPT.

Диски с разделами типа MBR содержат таблицу разделов, которая описывает расположение разделов на диске. В разделах этого типа первый сектор жесткого диска содержит запись MBR и двоичный файл, называющийся *основным загрузочным кодом* (master boot code), который используется для загрузки операционной системы. Этот сектор не используется при разбиении диска на разделы и скрыт с целью защиты системы.

Диски с разделами типа MBR могут поддерживать тома размером до 4 Тбайт и разбиваться на два типа разделов — основной и расширенный. Диск типа MBR может содержать до четырех основных разделов или три основных раздела и один расширенный раздел. Основные разделы представляют собой части диска, к которым можно иметь прямой доступ для хранения файлов. Для этого на них создаются файловые системы.

В отличие от основных разделов, к расширенным разделам нельзя обращаться напрямую. Чтобы получить доступ к расширенному разделу, на нем сначала нужно создать один или несколько логических дисков, к которым затем и выполняется обращение. Возможность разделять расширенные разделы на логические диски позволяет разбить физический диск не более четырех логических секций.

Диски с разделами типа GPT были изначально разработаны для высокопроизводительных компьютеров на основе процессоров Itanium. Использование разделов типа GPT рекомендуется для дисков с объемов больше 2 Тбайт для компьютеров на основе процессоров *x*86 или *x*64. Ключевая разница между дисками типа GPT и MBR заключается в способе хранения на них данных. На дисках с разделами типа GPT критические данные о разделе сохраняются в отдельных разделах, а для повышения структурной целостности используются избыточные основные и запасные таблицы разделов.

Хотя основы реализации разделов типа GPT и MBR разные, большинство дисковых операций по работе с ними выполняются одинаково. Это означает, что установив и настроив диски, при работе с ними тип раздела не имеет значения.

---

[1] Master Boot Record — главная загрузочная запись.

[2] GUID partition table — таблица разделов GUID.

Однако нужно иметь в виду следующее.

- Большинство дисков типа MBR могут иметь до четырех основных разделов, или три основных раздела и один расширенный раздел, содержащий один или несколько логических дисков. Динамические диски типа MBR могут содержать неограниченное количество томов.
- Диски типа GPT могут быть объемом до 18 экзабайтов (Эбайт) и содержать до 128 разделов. Загрузочные диски типа GPT имеют два обязательных раздела и один или более необязательных разделов (для нужд производителя или для хранения данных). В частности, требуется наличие раздела ESP[1] и раздела MSR[2]. Хотя типы необязательных разделов зависят от конфигурации системы, чаще встречается основной раздел. На дисках типа GPT основные разделы применяются для хранения данных.
- На компьютерах с процессорами *x*86 и *x*64 с BIOS диски типа MBR можно использовать как для установки системы, так и для хранения данных, а диски типа GPT — только для хранения данных. На 64-разрядных компьютерах с интерфейсом EFI можно использовать как GPT-, так и MBR-диски, но при этом требуется наличие хотя бы одного диска GPT, содержащего раздел ESP, раздел MSR и либо основной раздел, либо простой том, содержащий операционную систему для загрузки.

Операционная система Windows 8 поддерживает файловые системы FAT, FAT32, exFAT и NTFS. Тип используемой файловой системы FAT и максимальный размер тома определяется количеством битов, используемых в таблице размещения файлов для адресации кластеров дискового пространства. В таблице размещения файлов файловой системы FAT16, которая обычно называется просто FAT, используется 16 битов. Файловой системой FAT16 можно форматировать тома размером 4 Гбайт или меньше[3]. Также существует 32-разрядная версия FAT, которая называется FAT32. В таблице размещения файлов этой версии FAT для адресации используются 32 бита. С помощью средств форматирования Windows под эту файловую систему можно форматировать тома размером до 32 Гбайт. Хотя Windows 8 может использовать тома FAT32 большего размера, чем 32 Гбайт, отформатированные средствами сторонних разработчиков, для томов большего размера, чем 32 Гбайт следует использовать файловую систему NTFS.

Существенная разница между более ранними версиями Windows и Windows XP и более поздними версиями Windows состоит в том, что в последних предпочитаемыми форматами для внутренних и внешних дисков большого объема являются NTFS и exFAT. Расширенная файловая система FAT, или exFAT, является улучшенной версией FAT. Технически, exFAT можно было бы называть FAT64 (как некоторые ее и называют). Таблицы размещения файлов exFAT используют 64 бита, что позволяет exFAT преодолеть предел в 4 Гбайт для размера файлов и в 32 Гбайт для объема тома файловой системы FAT32. Формат exFAT поддерживает кластеры размером до 128 Кбайт для томов размером до 256 Тбайт. Этот формат предназначен для использования с любыми совместимыми операционными системами и устройствами, что дает ему преимущество над FAT.

Формат exFAT позволяет иметь больше, чем 1024 файлов в одной папке, а также поддерживает списки управления доступом и транзакции. Кроме этого, формат exFAT использует

---

[1] EFI system partition — системный раздел EFI.

[2] Microsoft Reserved Partition — резервный раздел Microsoft.

[3] В файловой системе дисковое пространство для данных выделяется не битами или байтами, а кластерами. Чтобы обратиться к данным на диске, нужно знать адрес кластера. В FAT16 под номер кластера отведено 16 разрядов. Поэтому максимальное количество кластеров составляет 2^{16}, а максимальный размер кластера равен $128 = 2^7$ секторов, размер сектора — 512 байт = 2^9. В таком случае максимальный размер разделов или дисков в FAT16 составляет $2^{16} \times 2^7 \times 2^9 = 2^{32}$ байт = 2 Гбайт.

битовую карту распределения кластеров для быстрого выделения пространства и бит смежности для каждого файла, что позволяет улучшить общую производительность. Улучшенное непрерывное размещение файлов на диске повышает производительность операций с мультимедиа, таких как запись и воспроизведение.

Примечание

Операционная система Windows Server 2012 реализует файловую систему ReFS[1]. Первоначальный выпуск Windows 8 не поддерживает эту файловую систему, хотя такая поддержка может быть предоставлена в будущем посредством исправления или пакета обновлений.

Операционная система Windows 8 предоставляет несколько инструментов для работы с дисками компьютера. Основным из них, однако которому часто не придают должного значения, является консоль **Компьютер**. Также используется такие инструменты, как **Управление дисками**, FSUtil и DiskPart. Разделы и тома дисков типа MBR и GPT можно форматировать под файловую систему exFAT и NTFS. При создании разделов или томов с помощью инструмента **Управление дисками** предоставляется возможность отформатировать диск и присвоить его букву или папку подключения. С помощью инструмента **Управление дисками** разделы и тома дисков типа MBR можно форматировать как под exFAT, так и под NTFS, но тома и разделы дисков типа GPT можно форматировать только под NTFS. Отформатировать диск типа GPT под FAT или FAT32 можно с помощью утилит командной строки `format` или `diskpart`.

Тип таблицы разделов диска можно изменять с MBR на GPT и наоборот. Эта возможность полезна в том случае, когда нужно перемещать приводы между компьютерами с BIOS и EFI, или при получении новых дисков, тип которых не соответствует требуемому. Но тип таблицы разделов можно преобразовывать только на пустых дисках. Это означает, что диск должен быть новым или отформатированным. Очистить диск, конечно же, можно, удалив его разделы или тома.

Как рассматривается в *разд. "Аппаратное шифрование, безопасная загрузка и сетевое разблокирование" главы 11*, Windows 8 предоставляет поддержку для приводов дисков с аппаратным шифрованием данных (которые называются *зашифрованными жесткими дисками*). Зашифрованные жесткие диски имеют встроенные процессоры, которые выполняют шифрование и расшифровывание данных вместо операционной системы, снижая нагрузку на ее ресурсы. При наличии аппаратного шифрования Windows 8 использует с ним возможность BitLocker.

Операционная система Windows 8 поддерживает приводы жестких дисков как *стандартного* (Standard Format), так и *расширенного* формата (Advanced Format). Размер физического сектора жестких дисков стандартного формата составляет 512 байт; такие диски также называются *дисками 512b* (512b disks). Размер физического сектора жестких дисков стандартного формата составляет 4096 байт; такие диски также называются *дисками 512e* (512e disks). Технология 512e представляет важную смену направления в области жестких дисков, позволяя создавать многотерабайтные диски.

Практический совет

Гранулярность обновления физического носителя диска определяется размером его физического сектора. Наименьшей единицей доступа дисков 512b является 512 байт, а дисков 512e — 4096 байт. Определить количество байтов в физическом секторе можно, выполнив в консоли командной строки, открытой с полномочиями администратора, следующую команду утилиты FSUtil:

```
Fsutil fsinfo ntfsinfo Буква_диска
```

[1] Resilient File System — устойчивая файловая система.

где параметр *Буква_диска* обозначает требуемый диск. Например:

```
Fsutil fsinfo ntfsinfo c:
```

Больший размер физического сектора позволяет увеличить емкость дисков далеко за границы физических емкостей, возможных ранее. Но когда запись производится только по 512 байт за раз, жесткие диски должны выполнять дополнительные операции, чтобы осуществить запись сектора. Чтобы улучшить производительность, приложения нужно обновить, чтобы они могли должным образом считывать и записывать по 4096 байт.

Использование консоли *Компьютер*

Чтобы открыть консоль **Компьютер**, щелкните по значку Проводника Windows на панели задач, а затем — по значку **Компьютер** в левой панели Проводника.

С помощью консоли **Компьютер** (рис. 12.1) можно быстро определить устройства хранения данных, доступные на компьютере.

В частности, вкладка **Компьютер** содержит следующие опции, позволяющие получить сведения об устройствах хранения данных компьютера:

- **Свойства** (Properties) — открывает диалоговое окно **Свойства** для текущего выбранного элемента;
- **Открыть** (Open) — открывает выбранный элемент в этом же окне Проводника Windows;
- **Переименовать** (Переименовать) — позволяет переименовать выбранный элемент;
- **Доступ к мультимедиа** (Access media) — позволяет подключаться и отключаться от сервера мультимедиа;

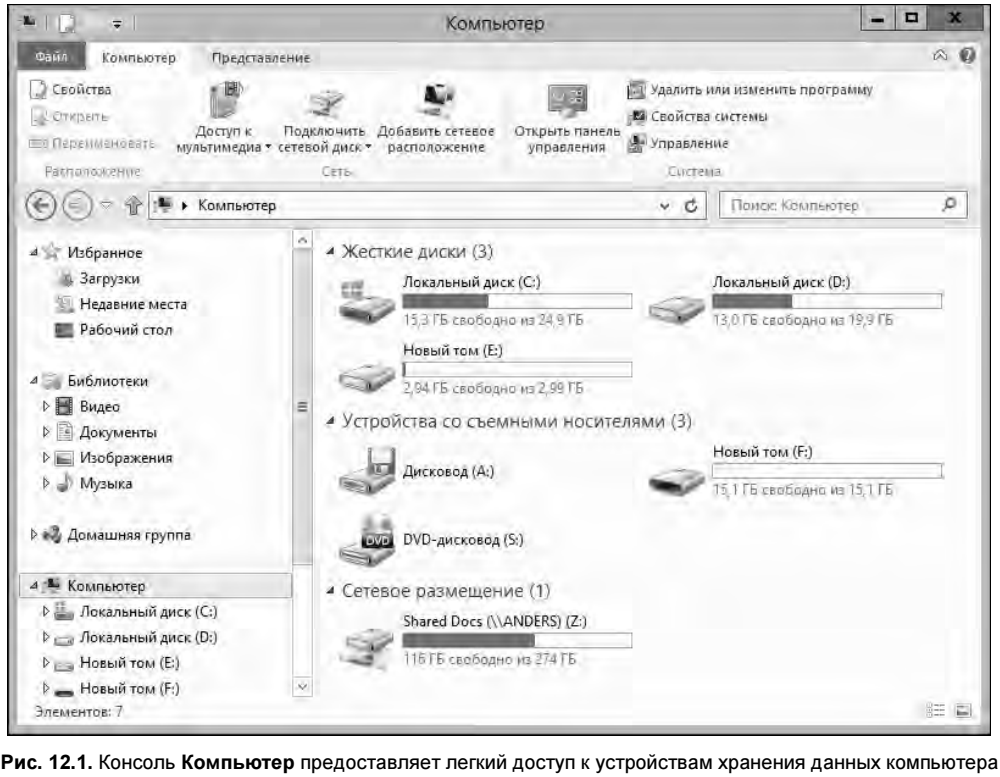


Рис. 12.1. Консоль **Компьютер** предоставляет легкий доступ к устройствам хранения данных компьютера

- **Подключить сетевой диск** (Map network drive) — позволяет подключать и отключать сетевой диск;
- **Добавить сетевое расположение** (Add a network location) — позволяет создать ярлык для веб-сайта, FTP-сайта, хранилища данных или другого сетевого расположения;
- **Открыть панель управления** (Open Control Panel) — открывает Панель управления в текущем окне Проводника Windows;
- **Удалить или изменить программу** (Uninstall or change a program) — открывает страницу Программы и компоненты (Programs and Features) Панели управления;
- **Свойства системы** (System properties) — открывает страницу **Система** Панели управления;
- **Управление** (Manage) — открывает консоль **Управление компьютером** (Computer Management) в новом окне.

Панель сведений консоли **Компьютер** содержит следующие разделы.

- **Жесткие диски** (Hard Disk Drives). Отображает локальные жесткие диски компьютера. Щелчок правой кнопкой мыши по требуемому диску открывает контекстное меню с опциями управления, в том числе опцию **Открыть**, которая открывает данный диск в Проводнике Windows. А щелчок по команде **Управление** (Manage) на вкладке **Компьютер** отображает на ленте основные инструменты для работы с дисками.
- **Устройства со съемными носителями** (Devices with Removable Storage). Отображает установленные на компьютере устройства со съемными носителями, включая приводы CD/DVD, приводы гибких дисков и накопители с флеш-памятью. Щелчок правой кнопкой мыши по требуемому устройству открывает контекстное меню с доступными для работы с данным устройством опциями, включая опцию **Извлечь** (Eject), которая позволяет извлечь текущий носитель, чтобы можно было вставить новый.

> ***Совет***
>
> Вместо гибких дисков и других типов съемных носителей все чаще используются флешки и внешние приводы жестких дисков с интерфейсом eSATA или USB/FireWire. Такие флешки и внешние жесткие диски можно оперативно присоединять и отсоединять. Но прежде чем отсоединять флешку или внешний жесткий диск eSATA, USB или FireWire, необходимо подготовить его к этому. Одним из способов подготовить флешку или внешний жесткий диск к отсоединению является опция **Извлечь** контекстного меню такого устройства. Щелкните по значку требуемого диска в Проводнике Windows, выберите команду **Управления** на вкладке **Компьютер** и щелкните по значку **Извлечь**. При условии, что диск не используется, теперь его можно безопасно извлечь.

- **Сетевое размещение** (Network Location). Отображает подключенные сетевые диски. Сетевой диск представляет доступ к общей папке или диску на другом компьютере. Чтобы подключить общую папку на другом компьютере в виде сетевого диска к локальному компьютеру, на вкладке **Компьютер** ленты выберите команду **Подключить сетевой диск** (Map network drive). Запустится мастер подключения сетевого диска, в котором нужно указать букву и путь к общей папке. Чтобы отключить сетевой диск, щелкните на нем правой кнопкой мыши и в контекстном меню выберите команду **Отключить** (Disconnect).

Работа с утилитой *Управление дисками*

Предпочтительным средством для настройки дисков является утилита **Управление дисками**. Эта утилита содержит инструменты для управления дисками, разделами, томами, логическими дисками и их связанными файловыми системами. Утилита **Управление дисками**

представляет собой оснастку консоли MMC, доступ к которой можно получить через предварительно сконфигурированную консоль **Управление компьютером** или посредством добавления этой оснастки в базовую консоль MMC. Средство **Управление дисками** позволяет выполнять следующие задачи:

- определять общую емкость, свободное пространство, статус и другие свойства дисков;
- создавать разделы и логические диски на базовых дисках;
- создавать тома на динамических дисках;
- расширять тома, чтобы увеличить их размер;
- форматировать тома под выбранную файловую систему;
- присваивать буквы дискам и пути томам;
- преобразовывать базовые диски в динамические и наоборот.

Оснастка **Управление дисками** входит в состав консоли **Управление компьютером**, которую можно открыть, выполнив в консоли командной строки команду `compmgmt.msc`. Эту команду также можно выполнить в поле поиска панели **Приложения**.

По умолчанию консоль **Управление компьютером** подключена к локальному компьютеру. Для управления дисками на другом компьютере нажмите или щелкните правой кнопкой мыши по корневому узлу **Управление компьютером** в дереве консоли и в контекстном меню выберите команду **Подключиться к другому компьютеру**. В открывшемся диалоговом окне **Выбор компьютера** установите переключатель **другим компьютером** и выберите требуемый компьютер. Подключить другой компьютер при запуске консоли **Управление компьютером** из командной строки можно, выполнив команду `compmgmt.msc /computer=` *`Имя_компьютера`*, где параметр *`Имя_компьютера`* обозначает имя удаленного компьютера, к которому требуется подключиться.

В конфигурации по умолчанию (рис. 12.2) оснастка **Управление дисками** отображает представление дисков или томов в верхней части панели сведений и графическое представление в нижней.

Хотя одновременно можно отображать только два представления оснастки, всего доступно три представления.

- **Список томов** (Volume List). Предоставляет подробные сведения о дисках компьютера. Щелчок по названию столбца представления, например **Тип** (Layout) или **Состояние** (Status), сортирует диски по этому столбцу.
- **Список дисков** (Disk List). Предоставляет сводную информацию о физических приводах. Эта информация включает номер диска и его тип (например, базовый, съемный или DVD), емкость диска, объем свободного пространства (если имеется), состояние (в сети, нет носителя и т. п.), тип интерфейса устройства (IDE или SATA).
- **Графическое представление** (Graphical View). Предоставляет графическое представление доступных физических и логических дисков. Отображает такую сводную информацию для физических дисков, как номер и тип устройства (базовый, съемный или DVD), объем диска и его состояние (в сети, нет носителя и т. п.). Также отображаются сведения для логических дисков физического диска, включая букву диска и метку тома, тип файловой системы (например, exFAT или NTFS), размер логического диска и его состояние (исправен или нет).

Представление верхней и нижней частей панели сведений можно менять, используя команды меню **Вид**. Для этого в меню **Вид** выберите команду **Верх** (или **Низ**), а затем требуемый вид.

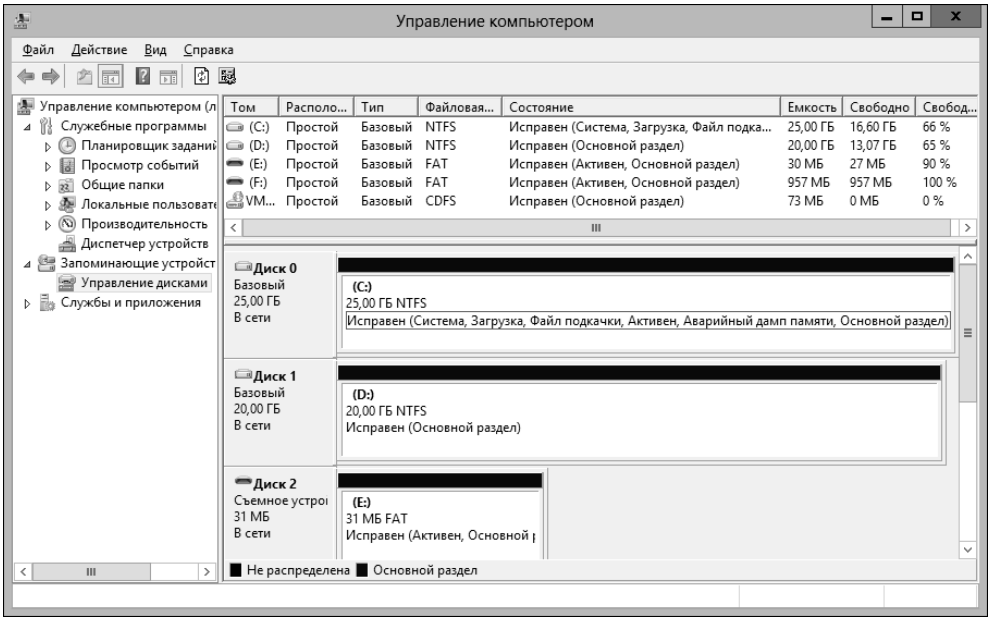


Рис. 12.2. Оснастка **Управление дисками** в консоли **Управление компьютером**

Рассмотренные представления предоставляют основные сведения о дисках компьютера. Чтобы получить более подробную информацию о локальном диске, щелкните правой кнопкой мыши на требуемом диске в виде **Список томов** и в контекстном меню выберите команду **Свойства**. Откроется диалоговое окно свойств диска (рис. 12.3).

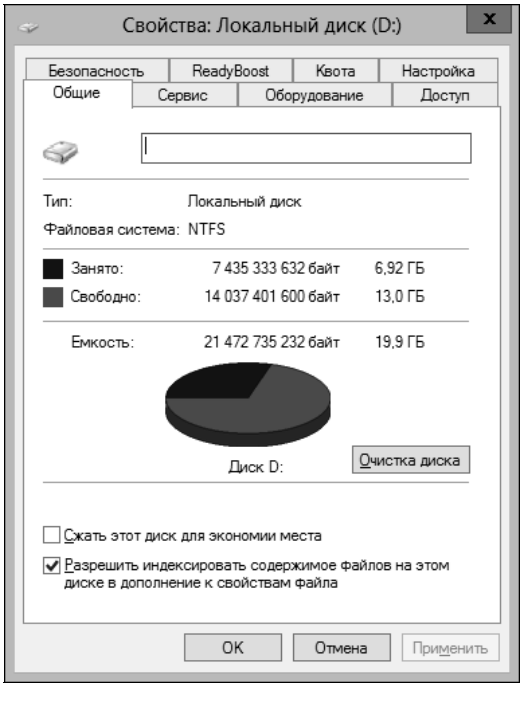


Рис. 12.3. Окно свойств диска с дополнительными сведениями о диске

Это такое же окно свойств диска, которое открывается и в Проводнике Windows. На вкладке **Настройка** (Customize) окна свойств можно выбрать шаблон, чтобы задать вид папок данного диска в панели сведений Проводника Windows.

Использование утилит FSUtil и Diskpart

Операционная система Windows 8 предоставляет несколько утилит командной строки для работы с дисками, включая следующие.

- **FSUtil.** Предназначена для использования профессиональным персоналом технического обслуживания для управления дисками на довольно низком уровне. Утилита FSUtil позволяет исследовать и работать с метаданными и другой подобной информацией, связанной с дисками, включая журналы изменения номеров USN[1], точки повторной обработки (reparse points) и жесткие связи (hard links). Также можно получить подробную информацию о секторах и кластерах, например, количество свободных или зарезервированных секторов на диске. Просмотреть список доступных команд утилиты можно, выполнив команду `fstuil`. Чтобы получить дополнительные сведения о конкретной команде, выполните команду `fsutil` *`имя_команды`* `help`. Для работы с утилитой FSUtil консоль командной строки должна быть запущенной с полномочиями администратора.
- **DiskPart.** Утилита командной строки для управления дисками, разделами и томами. Позволяет выполнять многие операции, что и средство **Управления дисками**, а также может применяться со сценариями для автоматизации процесса управления дисками. Утилита запускается командой `diskpart` в консоли командной строки, открытой с правами администратора. После запуска утилиты используется приглашение `DISKPART>`. Выполнение команды `help` выводит список команд утилиты с кратким описанием их использования.

> ***ПРИМЕЧАНИЕ***
>
> В отличие от средства **Управление дисками**, которое предоставляет удобный графический интерфейс и с которым сравнительно легко работать, утилиты FSUtil и DiskPart представляют собой сложные инструменты, предназначенные для использования опытными администраторами. Использование этих утилит подробно рассматривается в книге "Windows Command-Line Administrator's Pocket Consultant, Second Edition". Использование утилиты DiskPart также подробно рассматривается в *разд. "Пометка раздела в качестве активного" далее в этой главе*.

Улучшение производительности дисков

Операционная система Windows 8 содержит несколько функциональностей для повышения производительности дисков, включая следующие.

- **Windows ReadyBoost.** Повышает производительность системы, используя устройства флеш-памяти в качестве дополнительных устройств кэширования.
- **Windows ReadyDrive.** Повышает производительность мобильных компьютеров, оснащенных гибридными приводами.
- **Windows SuperFetch.** Повышает производительность системы, используя видоизмененный алгоритм управления памятью.

Эти возможности рассматриваются в последующих разделах.

---

[1] Update sequence number — порядковый номер обновления.

Windows ReadyBoost

Диски компьютера служат не только для хранения данных приложений и пользователей. Они также интенсивно используются операционной системой для хранения файлов подкачки и системного кэша. Так как операции записи и считывания с диска значительно медленнее, чем из физической памяти (RAM), эти операции могут создать узкое место, которое отрицательно сказывается на производительности. Средство Windows ReadyBoost предназначено для уменьшения отрицательного эффекта, связанного с операциями чтения и записи системного кэша.

Эта функциональность использует вместо жестких дисков для кэширования содержимого оперативной памяти компьютера USB-устройства флеш-памяти достаточного быстродействия, что повышает скорость произвольных чтений памяти. Так как кэшируется все содержимое кэша диска, а не только файл подкачки и системные динамические библиотеки (DLL), общая производительность компьютера повышается, поскольку скорость чтения флеш-памяти до десяти раз выше скорости чтения физических дисков.

С функциональностью Windows ReadyBoost можно применять, среди прочих, такие устройства, как флешки и карты SD и CompactFlash с интерфейсом USB 2.0 или более поздней версии. Эти устройства должны обладать достаточным быстродействием и быть размером в 256 Мбайт или больше. Для повышения производительности рекомендуется использовать USB-устройства с быстродействующей памятью. Если USB-устройство содержит как медленную, так и быстродействующую память, для повышения производительности будет использоваться только быстрая память. Для средства ReadyBoost на устройстве USB можно зарезервировать от 230 до 15 196 Мбайт флеш-памяти. Рекомендуется использовать объем флеш-памяти, равный 1—3 объемам оперативной памяти системы. Но при этом следует иметь в виду, что на момент написания этой книги можно зарезервировать самое большее 15 196 Мбайт флеш-памяти.

Флеш-память в основном используется для произвольных операций чтения, т. к. скорость последовательного ввода-вывода большинства устройств флеш-памяти медленнее, чем скорость жестких дисков. Средство ReadyBoost максимизирует производительность, автоматически передавая запросы на чтение больших последовательных массивов данных для обслуживания их жестким диском. Чтобы устройство флеш-памяти можно было удалить в любое время, все операции записи сначала выполняются на жесткий диск, а затем на устройство флеш-памяти. Таким образом, все записываемые на флеш-память данные дублируются на жестком диске, что устраняет возможность потери данных при отключении устройства флеш-памяти. Кроме этого, чтобы предотвратить возможную утерю конфиденциальной информации, все записываемые на флеш-память данные шифруются таким образом, что их можно прочитать лишь на компьютере, на котором они были записаны.

Включение и настройка ReadyBoost

Подготовка USB-устройств флеш-памяти для использования с возможностью ReadyBoost выполняется следующим образом. Когда устройство флеш-памяти подключается к USB-порту компьютера, Windows 8 проверяется быстродействие памяти устройства. Если флеш-память устройства обладает достаточным быстродействием, его можно использовать для кэширования содержимого оперативной памяти компьютера. В большинстве случаев желательно, чтобы флеш-память обладала, по крайней мере, таким быстродействием, как скорость шины компьютера.

Совет

При первом подключении устройства флеш-памяти Windows может ошибочно пометить его, как не отвечающее требованиям функциональности ReadyBoost. В таком случае можно выполнить повторную проверку устройства на соответствие этим требованиям. Для этого в Проводнике Windows щелкните правой кнопкой мыши на этом устройстве, а затем в контекстном меню выберите команду **Свойства**. В диалоговом окне свойств выберите вкладку **ReadyBoost** и нажмите на ней кнопку **Протестировать устройство**.

Далее приводится описание процедуры для включения и настройки средства ReadyBoost при первом использовании с компьютером USB-устройства флеш-памяти:

1. Вставьте устройство флеш-памяти в разъем USB 2.0 или более поздней версии интерфейса. Должно автоматически открыться диалоговое окно автозапуска (если автозапуск не был отключен в Панели управления), содержащее меню опций операций с устройством.

   При щелчке на опции **Ускорить работу системы — Windows ReadyBost** (Speed up my system — Windows ReadyBoost) откроется диалоговое окно свойств устройства с выбранной вкладкой **ReadyBoost** (рис. 12.4).

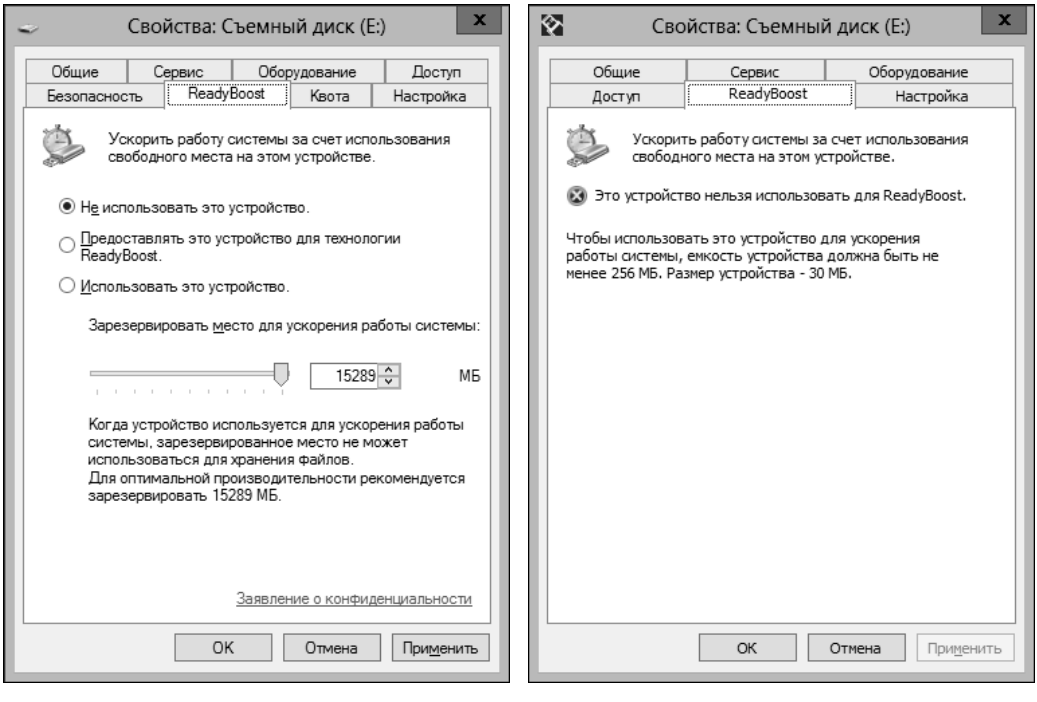


Рис. 12.4. Окно для настройки параметров средства Windows ReadyBoost

2. Выполните одно из следующих действий, а затем нажмите кнопку **OK**.
   - Чтобы система автоматически резервировала максимальный объем устройства для ReadyBoost, установите переключатель **Предоставлять это устройство для технологии ReadyBoost** (Dedicate this device to ReadyBoost). Это предотвращает использование данного устройства пользователем для каких-либо других целей и резервирует максимально возможный объем памяти устройства для использования функциональностью ReadyBoost.

- Чтобы использовать меньший, чем максимально возможный объем памяти устройства, установите переключатель **Использовать это устройство** (Use this device), а затем установите с помощью ползунка или счетчика объем памяти устройства для использования средством ReadyBoost. Если зарезервировать меньший, чем общий объем памяти устройства, оставшуюся память можно задействовать для хранения данных.

При нажатии кнопки **Применить** Windows 8 расширяет физическую память компьютера памятью устройства. Конфигурация по умолчанию позволяет системе зарезервировать весь имеющийся объем устройства флеш-памяти для функциональности Windows ReadyBoost.

ПРАКТИЧЕСКИЙ СОВЕТ

Чтобы устройство флеш-памяти можно было использовать для ReadyBoost, его скорость чтения произвольных блоков размером в 4 Кбайт должна быть, по крайней мере, 2,5 Мбит/с, а скорость записи произвольных блоков памяти размером 512 Кбайт должна быть, по крайней мере, 1,75 Мбит/с. Хотя устройство флеш-памяти, зашифрованное с помощью функциональности BitLocker To Go, можно использовать с ReadyBoost, следует иметь в виду, что процесс шифрования и расшифровывания данных на устройстве может отрицательно сказаться на производительности чтения и записи. При использовании устройства флеш-памяти, зашифрованного посредством BitLocker, рекомендуется настроить автоматическое разблокирование устройства при его подключении к компьютеру. В противном случае пользователю придется выполнять разблокирование устройства вручную.

Включить и настроить средство Windows ReadyBoost с USB-устройством флеш-памяти, которое уже подключено к системе или при автозапуске которого была отклонена возможность использовать эту функциональность, можно следующим образом:

1. Откройте Проводник Windows или консоль **Компьютер**.
2. Щелкните правой кнопкой мыши на требуемом устройстве флеш-памяти и в контекстном меню выберите команду **Свойства**.
3. На вкладке **ReadyBoost** окна свойств устройства настройте параметры функциональности, как рассматривается в шаге 2 предыдущей процедуры. Нажмите кнопку **OK**, чтобы применить настройки и закрыть окно.

Если USB-устройство флеш-памяти не отвечает требованиям ReadyBoost, включить его для использования этой функциональностью нельзя. Устройство флеш-памяти, которое полностью используется для ReadyBoost, можно удалить, не опасаясь утери данных или иного отрицательного воздействия на систему. Но с удалением устройства производительность системы возвращается к стандартному уровню, получаемому без использования устройства. Безопасно удалить устройство, используемое как для ReadyBoost, так и для хранения данных пользователя, можно следующим образом:

1. Откройте Проводник Windows или консоль **Компьютер**.
2. Щелкните правой кнопкой мыши на этом устройстве, а затем в контекстном меню выберите команду **Извлечь**. Если устройство открыто в Проводнике Windows или находящиеся на нем файлы используются программой, может потребоваться закрыть окно Проводника с устройством или закрыть программы, использующие находящиеся на нем файлы, прежде чем устройство можно будет извлечь.

Windows ReadyDrive

Средство Windows ReadyDrive повышает производительность мобильных компьютеров, оснащенных гибридными дисками. Гибридный диск представляет собой устройство, в котором данные сохраняются как во флеш-памяти, так и на жестком диске. Так как флеш-

память намного быстрее, чем жесткий диск, мобильные компьютеры под Windows 8 могут сначала записывать новые или измененные данные во флеш-память и периодически переносить их из флеш-памяти на жесткий диск. Такой подход позволяет уменьшить объем вращений жесткого диска, экономя заряд батареи.

Флеш-память на гибридных дисках можно также использовать, чтобы ускорить запуск компьютера и его вывод из режима сна или гибернации. Для этого перед завершением работы системы или перед переходом в режим сна или гибернации информация, требуемая для запуска или возобновления системы, записывается во флеш-память. Затем при запуске или возобновлении компьютера эта информация считывается из флеш-памяти.

Средство ReadyDrive не потребует включения, т. к. оно включается автоматически на мобильных компьютерах, оснащенных гибридными приводами.

Windows SuperFetch

Операционная система Windows 8 позволяет повысить производительность и улучшить время отклика, изменяя способ использования пользовательских и фоновых процессов. В Windows XP пользовательские и фоновые процессы имеют одинаковый приоритет на использование памяти. Вследствие отсутствия назначения приоритета на использование памяти между этими типами процессов часто возникают конфликты доступа к ресурсам памяти. Кроме этого, по завершению исполнения фоновые процессы часто не выгружаются из памяти. Это отрицательно сказывается на производительности, т. к. данные для пользовательских процессов загружаются в память только тогда, когда они запрашиваются. Эта проблема устранена в Windows 8, обеспечивая своевременную выгрузку фоновых процессов по завершению их исполнения и предварительную загрузку данных для пользовательских процессов.

В Windows XP операции ввода-вывода пользовательских и фоновых процессов имеют одинаковый приоритет, вследствие чего часто возникают конфликты доступа к памяти и падает уровень производительности операций записи и чтения. Этот недостаток исправлен в Windows 8 посредством реализации очередей ввода-вывода с высоким и низким приоритетом. Ввод-вывод с высоким приоритетом применяется пользовательскими процессами для операций записи и чтения с физическими дисками. А для операций записи и чтения физических дисков фоновыми процессами используется ввод-вывод с низким приоритетом.

> ***Примечание***
>
> В Windows 8 многие службы и повседневные задачи обслуживания выполняются как фоновые процессы. Например, утилита дефрагментации диска запланирована исполняться автоматически через определенные интервалы времени. Эта утилита исполняется как фоновый процесс и использует ввод-вывод с низким приоритетом.

Приоритезация ввода-вывода основана на функциональности Windows SuperFetch. Эта функциональность повышает производительность системы, используя модифицированный алгоритм управления памятью. В отличие от алгоритмов управления памятью в Windows XP и более ранних версиях Windows, SuperFetch оптимизирует использование памяти в зависимости от способа использования компьютера текущим пользователем. Для достижения такой оптимизации применяются следующие методы.

- **Дифференцирование между пользовательскими приложениями и фоновыми процессами.** Функциональность SuperFetch улучшает реагирование системы на запросы пользователя, присваивая процессам текущего пользователя более высокий приоритет, чем фоновым задачам. Так как процессы пользователя всегда имеют приоритет над фо-

новыми заданиями, последние не занимают все время процессора и система реагирует более оперативно на запросы пользователя.

- **Оптимизация памяти для пользователей после выполнения фоновых заданий.** В Windows 8 задания обслуживания используют время простоя процессора эффективнее, чем в более ранних версиях Windows. В частности, время простоя процессора используется большим количеством системных и обслуживающих процессов, таких как средства дефрагментации дисков и резервного копирования. При простое компьютера фоновые процессы исполняются обычным образом. Но по завершению исполнения фонового процесса средство SuperFetch возвращает содержимое памяти в состояние, предшествующее запуску фонового процесса. Это обеспечивает оптимизацию памяти для пользовательских процессов и оперативность реагирования компьютера на запросы пользователя.
- **Отслеживание наиболее часто используемых приложений и предвидение требований пользователя.** Функциональность SuperFetch отслеживает, какие приложения исполняются наиболее часто, а также, когда эти приложения обычно используются. Эта информация затем учитывается для предварительной загрузки приложения и его подготовки к исполнению, когда SuperFetch ожидает, что это приложение потребуется пользователю. Таким образом обеспечивается более быстрый запуск приложений и более быстрое переключение пользователей.
- **Использование ввода-вывода с разными приоритетами.** Средство SupetFetch использует запросы ввода-вывода с высоким и низким приоритетом, предоставляемые в Windows 8, для оптимизации времени чтения и записи пользовательских процессов и улучшения общей оперативности реагирования системы. Когда несколько процессов конкурирует за ввод-вывод, процессы с высоким приоритетом всегда получаются больше времени ввода-вывода, чем процессы с низким приоритетом. В результате повышается производительность пользовательских процессов и приложений, а также снижается уровень состязания за время ввода-вывода между пользовательскими и фоновыми процессами при их одновременном выполнении.

Средство SuperFetch поддерживается всеми версиями Windows 8. Администраторы должны понимать принципы работы функциональности SuperFetch и способы ее настройки. Далее приводится описание основных характеристик SuperFetch.

- Выполняется как служба, называющаяся **SuperFetch**. Служба запускается автоматически при запуске компьютера; вход службы в систему выполняется по учетной записи **Локальная система**.
- Служба использует исполняемый файл Svchost.exe с сетевыми ограничениями. Это означает, что SuperFetch имеет доступ только к локальному компьютеру, но не к локальной сети, к которой этот компьютер может быть подключен.
- Должное функционирование SuperFetch обеспечивается компонентом Filter Manager, который предоставляет информацию о файлах и файловой системе, необходимую для SuperFetch. Этот компонент устанавливается автоматически при установке операционной системы.
- SuperFetch записывает предварительно выбранные данные в папку *%SystemRoot%* Prefetch. Эти данные используются для ускорения запуска приложений. Папка Prefetch содержит несколько файлов баз данных, применяемых для отслеживания истории использования приложения и повышения его производительности. Ошибки приложений также отслеживаются и записываются в файл журнала базы данных.

Примечание

Папка Prefetch обслуживается системой и не требует удаления ее содержимого пользователем или администратором.

После внесения существенных изменений в операционную систему установки пакетов обновлений или исправлений либо после переконфигурирования приложений запуск пользовательских программ на первых порах может замедлиться. Величина такого замедления зависит от объема внесенных изменений и от объема информации по использованию памяти, которую SuperFetch должен восстановить. В некоторых случаях, например после установки нового пакета обновлений, может потребоваться несколько перезапусков в течение определенного периода времени, чтобы скорость запуска приложений вошла в норму.

Базовые и динамические диски

Не так давно все компьютеры с предустановленной системой Windows поставлялись с базовыми дисками. В настоящее время, идя навстречу пожеланиям пользователей иметь диски большего объема и повышенной надежности, производители поставляют все больше компьютеров с жесткими дисками, настроенными как динамические. Вместо одного диска объемом в 500 Гбайт новый компьютер может иметь составной диск размером в 1000 Гбайт, состоящий из двух физических дисков объемом в 500 Гбайт каждый, функционирующих как один логический диск. Одним из подходов к реализации дисков такого типа в Windows 8 является использование динамических дисков.

Факт поставки все большего количества компьютеров с динамическими дисками может заставить задуматься, не следует ли преобразовать все имеющиеся на ваших компьютерах базовые диски в динамические. В некоторых случаях такое решение может быть вызвано необходимостью стандартизации. Например, чтобы обеспечить лучшую управляемость, вы можете захотеть, чтобы все настольные компьютеры в определенном отделе имели одинаковую конфигурацию. В других случаях это решение может исходить от ИТ-руководства организации, которое считает, что преобразование базовых дисков в динамические будет частью процесса модернизации оборудования. (Иными словами, перевод компьютеров с дисков старого типа на новый.) Но прежде чем приступать к преобразованию, следует понять, в чем оно заключается, какие возможности будут поддерживаться, а какие нет.

Базовый диск представляет собой физический диск, имеющий один или несколько базовых томов, которые могут быть сконфигурированы, как основные разделы, плюс необязательный расширенный раздел, содержащий логические диски. *Основной раздел* представляет собой часть диска, к которой можно иметь прямой доступ для хранения файлов. Физический диск может содержать до четырех основных разделов. Чтобы сделать основной раздел доступным для пользователей, на нем создается файловая система. Вместо одного из четырех возможных основных разделов на физическом диске можно создать *расширенный раздел*. Иными словами, диск будет содержать три основных раздела и один расширенный. В отличие от основных разделов, обращаться напрямую к расширенному разделу нельзя. Чтобы получить доступ к расширенному разделу, на нем сначала нужно создать один или несколько *логических дисков*, к которым затем и выполняется обращение. Возможность разделять расширенные разделы на логические диски позволяет разбить физический диск на больше, чем четыре логические секции. Например, в одном расширенном разделе можно создать четыре логических диска, скажем, F, G, H и I.

Динамический диск представляет собой физический диск, содержащий один или несколько динамических томов. В отличие от базового диска, динамический диск может содержать неограниченное количество томов, каждый из которых может быть расширенным или использоваться для загрузки системы. В то время как базовые диски можно использовать с любой версией Windows, динамические диски поддерживаются только Windows 2000 и более поздними версиями Windows.

В предыдущих версиях Windows основным преимуществом динамических дисков была возможность комбинировать физические диски в *составные* (spanned), *чередующиеся* (striped) или *зеркальные* (mirrored) тома. Но Windows 8 позволяет комбинировать таким образом и базовые диски. Составной или чередующийся том представляет собой один том, который состоит из нескольких дисков и использует полностью или только часть каждого диска набора. Разница между составными и чередующимися томами заключается в способе записи на них данных. Операционная система Windows 8 видит все диски составного тома, как один раздел, и выполняет операции записи во всем разделе произвольным образом. В случае чередования дисков, Windows 8 записывает часть данных на каждый из дисков, из которых состоит том. В большинстве случаев чередование дисков ускоряет операции записи и чтения, т. к. данные считываются или записываются одновременно на несколько физических дисков.

При зеркалировании два физических диска составляют один логический отказоустойчивый том. Все данные копируются отдельно на каждый из дисков, и в случае отказа одного из них будут доступны на другом.

Осторожно!

Технически, чередующийся том представляет собой массив RAID 0, а зеркальный том — массив RAID 1. Хотя зеркальные тома являются отказоустойчивыми, ни чередующиеся, ни составные тома такими не являются, и при отказе одного из дисков тома из строя выходит весь том.

В настоящее время, когда составные, чередующиеся и зеркальные тома можно создавать, используя базовые диски, основная разница между базовыми и динамическими томами состоит в том, что динамические диски обладают расширенными возможностями обнаружения и исправления ошибок, а также возможностью модифицирования дисков без необходимости перезагружать компьютер. Наличие у динамического диска других возможностей зависит от используемой файловой системы, например exFAT или NTFS.

При форматировании жесткого диска файловой системой на диске создается структура кластеров, которые представляют собой логические группы секторов. В случае дисков 512b, файловые системы FAT, FAT32, exFAT и NTFS используют секторы размером 512 байт и допускают переменный размер кластера. Например, могут использоваться кластеры размером 4096 байт, состоящие из 8 секторов размером в 512 байт.

В табл. 12.1 приведена сводка размеров кластеров по умолчанию для файловых систем FAT16, FAT32, exFAT и NTFS. При форматировании диска под файловую систему предоставляется выбор использовать размер кластера по умолчанию или указать другой размер. В любом случае размер кластера зависит от применяемой для форматирования файловой системы.

Практический совет

Платформы Windows используют четыре типа файловых систем FAT: FAT12, FAT16, FAT32 и exFAT. Разница между файловыми системами FAT12, FAT16 и FAT32 заключается в количестве разрядов записей таблиц размещения файлов: 12, 16 и 32 соответственно. С точки зрения пользователя основная разница между этими файловыми системами состоит в теоретически возможном размере тома, который составляет 16 Мбайт, 4 Гбайт и 2 Тбайт для FAT12, FAT16 и FAT32 соответственно. Термин FAT без номера обычно может подразумевать как FAT16, так и FAT32. Расширенная файловая система FAT, или exFAT, является улучшенной версией FAT32. Хотя файловая система exFAT сохраняет преимущества легкости использования FAT32, она преодолевает барьер максимального размера файлов в 4 Гбайт и томов в 32 Гбайт, присущий FAT32. Файловая система exFAT также поддерживает размер кластера до 32 768 Кбайт. Этот формат предназначен для использования с любыми совместимыми операционными системами и устройствами, что дает ему преимущество над FAT32.

Таблица 12.1. *Размеры кластеров по умолчанию для файловых систем FAT16, FAT32, exFAT и NTFS*

Размер тома	Размер кластера			
	FAT16	**FAT32**	**exFAT**	**NTFS**
7—16 Мбайт	512 байт (как FAT12)	Не поддерживается	4 Кбайт	512 байт
17—32 Мбайт	512 байт	Не поддерживается	4 Кбайт	512 байт
33—64 Мбайт	1 Кбайт	512 байт	4 Кбайт	512 байт
65—128 Мбайт	2 Кбайт	1 Кбайт	4 Кбайт	512 байт
129—256 Мбайт	4 Кбайт	2 Кбайт	4 Кбайт	512 байт
257—512 Мбайт	8 Кбайт	4 Кбайт	32 Кбайт	512 байт
513—1024 Мбайт	16 Кбайт	4 Кбайт	32 Кбайт	1 Кбайт
1025 Мбайт — 2 Гбайт	32 Кбайт	4 Кбайт	32 Кбайт	4 Кбайт
2 —4 Гбайт	64 Кбайт	4 Кбайт	32 Кбайт	4 Кбайт
4—8 Гбайт	Не поддерживается	4 Кбайт	32 Кбайт	4 Кбайт
8—16 Гбайт	Не поддерживается	8 Кбайт	32 Кбайт	4 Кбайт
16—32 Гбайт	Не поддерживается	16 Кбайт	32 Кбайт	4 Кбайт
32 Гбайт — 2 Тбайт	Не поддерживается	*	128 Кбайт	4 Кбайт
2—16 Тбайт	Не поддерживается	*	128 Кбайт	4 Кбайт
16—32 Тбайт	Не поддерживается	*	128 Кбайт	8 КБ
32—64 Тбайт	Не поддерживается	*	128 Кбайт	16 Кбайт
64—128 Тбайт	Не поддерживается	*	128 Кбайт	32 Кбайт
128—256 Тбайт	Не поддерживается	*	128 Кбайт	64 Кбайт

* При использовании средств форматирования Windows максимальный размер тома ограничен 32 Гбайт. С помощью инструментов сторонних разработчиков можно создавать тома большего размера, чем 32 Гбайт.

Важной информацией о *кластерах* является то, что они представляют собой наименьшую единицу выделения дискового пространства. Один кластер может содержать самое большее один файл. Поэтому при сохранении файла размером в 1 Кбайт в кластер размером в 4 Кбайт, 3 Кбайт дискового пространства будут не использованы и при этом недоступны для хранения других файлов. Но таково уж устройство кластеров, и ничего с этим нельзя поделать. Если же файл не помещается в один кластер, оставшиеся данные помещаются в другой, затем следующий и т. д., пока не будет сохранен весь файл. В файловой системе FAT, например, первый кластер файла содержит указатель на второй, второй — указатель

на третий, третий — на следующий и т. д., до последнего кластера файла, который содержит маркер окончания файла EOF.

Управление физической структурой диска осуществляется подсистемой ввода-вывода диска, а логической структурой диска на уровне файлов управляет Windows. Логическая структура диска связана с базовыми или динамическими томами, созданными на диске, и с файловыми системами, под которые эти тома отформатированы. Как базовые, так и динамические тома можно форматировать под файловую систему FAT или NTFS. Эти файловые системы имеют разные структуры, и каждая обладает своими преимуществами и недостатками.

Хотя на одном компьютере можно использовать как базовые, так и динамические диски, диски, составляющие том, должны быть одного типа. Процесс преобразования базовых дисков в динамические и наоборот рассматривается в *разд. "Преобразование базового диска в динамический и наоборот" далее в этой главе*. Но не забывайте, что хотя при преобразовании базового диска в динамический данные сохраняются, это невозможно при обратном преобразовании. Для преобразования динамического диска в базовый нужно удалить все существующие разделы диска, что уничтожает находящиеся на диске данные. Наконец, динамические диски нельзя создавать на любых съемных носителях или на дисках портативных компьютеров. Ноутбуки, планшеты и вообще любые портативные компьютеры могут иметь только базовые диски.

Осторожно!

Будьте осторожны при работе с дисками портативных компьютеров. Некоторые конфигурации портативных компьютеров могут ввести средство **Управление дисками** в заблуждение, что оно может преобразовать базовый диск в динамический. Такая ситуация возможна на компьютерах, которые не поддерживают спецификацию APM[1] или интерфейс ACPI[2]. Хотя может казаться, что компьютер поддерживает динамические диски, это не так, и попытка преобразовать базовый диск в динамический на таком ноутбуке может повредить весь диск.

Примечание

Внешние жесткие диски, подключаемые посредством интерфейса FireWire, USB или eSata, в некоторых случаях можно преобразовать в динамические. Подробное описание процедуры такого преобразования приводится в статье базы знаний Microsoft 299598, "How To: Convert an IEEE 1394 Disk Drive to Dynamic Disk Drive in Windows XP[3]". Но в этой статье не уделяется должного внимания необходимым предостережениям. Преобразованный таким образом диск можно использовать только с одним компьютером. Если существует возможность будущей необходимости перемещения такого диска на другой компьютер, его не следует преобразовывать в динамический. Кроме этого, прежде чем начинать преобразование любого внешнего диска с интерфейсом USB или FireWire, следует создать резервную копию находящихся на нем данных. Если есть такая возможность, выполните преобразование на идентичном, но не критическом диске в среде разработки или тестирования, а затем протестируйте работу диска.

Использование базовых и динамических дисков

Перед использованием базовых и динамических дисков с ними выполняется несколько связанных действий, таких как инициализация новых дисков, задание диска активным или из-

[1] Advanced Power Management — усовершенствованные средства управления питанием.

[2] Advanced Configuration and Power [management] Interface — усовершенствованный интерфейс управления конфигурированием и энергопотреблением.

[3] Как: Преобразовать диск IEEE 1394 в динамический в Windows XP.

менение типа диска. Но прежде чем выполнять эти операции, нужно понять, что такое активный, загрузочный, системный диск и др.

Обозначения дисков

Базовые диски могут разбиваться на основные и расширенные разделы. Основной раздел можно использовать для запуска операционной системы. В то время как основной раздел нельзя разбить на дополнительные разделы, в расширенном разделе можно создать один или несколько логических дисков, независимых друг от друга.

Динамические диски разбиваются на тома, наиболее распространенным типом которых является простой том. *Простой том* — это том, расположенный на одном физическом диске; такой том можно использовать для запуска операционной системы. Динамические тома, с другой стороны, состоят из пространства нескольких физических дисков.

При работе с дисками любого из этих типов следует понимать значение следующих пяти специальных разделов дисков MBR.

- **Активен** (Active). Активный раздел или том представляет собой секцию диска, из которой выполняется запуск компьютера. Если на компьютере установлено несколько операционных систем, активный раздел диска должен содержать файлы запуска операционной системы. Этот раздел также должен быть основным разделом базового диска или простым томом динамического. Активный раздел обычно не помечается как таковой в средстве **Управление дисками**. В большинстве случаев это будет основной раздел или первый простой том на диске 0. Но в случае внесения изменений в конфигурацию по умолчанию метка **Активен** будет отображаться.

  Осторожно!

  Приводы дисков со съемными носителями могут быть помечены как **Активен**, но это обозначает состояние диска, и не имеет ничего общего с меткой **Активен**, обозначающей активный раздел. В частности, устройства чтения карт типа CompactFlash или других типов с интерфейсом USB или FireWire могут отображаться как **Активен**, когда в них вставлен носитель и привод находится в сети. Также важно иметь в виду, что иногда привод со съемным носителем может обозначаться как **Диск 0**. В таких случаях активный раздел следует искать на первом приводе с несъемным носителем. Например, если компьютер имеет диски **Диск 0**, **Диск 1** и **Диск 2**, из которых первым приводом с несъемным носителем является **Диск 1**, активным разделом, скорее всего, будет первый основной раздел или простой том этого диска.

- **Система** (System). Системный раздел или том, который содержит файлы, специфичные для аппаратного обеспечения данного компьютера, необходимые для загрузки операционной системы. Системный раздел или том может быть зеркальным, но не может быть частью чередующегося или составного тома. Пометка системного раздела находится в столбце **Состояние** представления **Список томов** и в виде **Графическое представление** консоли **Управление дисками**.
- **Загрузка** (Boot). Загрузочный раздел или том содержит операционную систему и ее вспомогательные файлы. Загрузочный раздел или том может быть зеркальным, но не может быть частью чередующегося или составного тома. На большинстве компьютеров системный и загрузочный раздел совмещены в одном разделе или томе. Хотя может казаться, что системный и загрузочный разделы должны называться наоборот, действующие названия используются со времени введения Windows NT и не похоже, что такое положение дел изменится. Подобно активному разделу, загрузочный раздел обычно не помечается как таковой в средстве **Управление дисками**. В большинстве случаев это будет основной раздел или первый простой том на диске `Диск 0`. Но если операционная

система установлена на другом разделе или томе, тогда метка **Загрузка** может отображаться.

- **Файл подкачки** (Page file). Этот раздел содержит файл подкачки операционной системы. Так как система может вытеснять страницы памяти на несколько дисков, в зависимости от настройки виртуальной памяти, компьютер может иметь несколько разделов или томов файла подкачки. Однако, в зависимости от настройки пакетов обновлений используемым для файла подкачки может отображаться только основной раздел. Подробную информацию о настройке и использовании файлов подкачки *см. в разд. "Настройка виртуальной памяти" главы 2*.
- **Аварийный дамп памяти** (Crash dump). В этот раздел система пытается сохранить файлы дампа в случае сбоя. Как рассматривается в *разд. "Настройка параметров восстановления" главы 2*, файлы дампа можно использовать для установления причин сбоя системы. По умолчанию файлы дампа сохраняются в папке *%SystemRoot%*, но могут записываться в любой раздел или том.

Любой компьютер имеет один активный, один системный, один загрузочный раздел или том и один раздел или том аварийного дампа памяти, при этом все разделы или тома могут быть совмещены в одном. Раздел файла подкачки может быть единственным обозначенным разделом среди нескольких разделов или томов.

Установка и инициализация новых физических дисков

Операционная система Windows 8 упрощает задачу добавления на компьютер новых физических дисков. После подключения диска согласно инструкциям его производителя нужно войти в систему и запустить средство **Управление дисками**. Если новый диск уже инициализирован, т. е. уже имеет подпись диска, что делает возможным выполнение с ним операций записи и чтения, он должен быть введен в действие автоматически при выполнении команды **Повторить проверку дисков** (Rescan disks) меню **Действие** (Action). Если же диск не был инициализирован, т. е. не имеет подписи диска, после запуска средство **Управление дисками** обнаружит его и запустит мастер инициализации и преобразования дисков (Initialize and Convert Disk Wizard).

Инициализация нового диска посредством этого мастера выполняется следующим образом:

1. Нажмите кнопку **Далее**, чтобы перейти на следующую страницу мастера. На странице **Выбор диска для инициализации** (Select Disks to Initialize) новые диски выбираются для инициализации автоматически, но если определенный диск не требуется инициализировать, нужно сбросить его флажок.
2. Нажмите кнопку **Далее**, чтобы перейти на страницу **Выбор дисков для преобразования** (Select Disks to Convert). На этой странице отображается новый диск, а также все несистемные и незагрузочные диски, которые можно преобразовать в динамические диски. Новый диск не выбран по умолчанию, и если его необходимо преобразовать, нужно установить его флажок, а затем нажать кнопку **Далее**.
3. На последней странице мастера отображаются выбранные ранее опции и действия, которые будут выполнены с каждым диском. Проверьте эту информацию и, если все правильно, нажмите кнопку **Завершить**. После этого мастер выполнит указанные действия. Если была выбрана инициализация диска, мастер поставит на нем подпись диска. Если было выбрано преобразование диска, мастер поставит на нем подпись диска, а затем преобразует его в динамический.

Для подписи и преобразования дисков не обязательно использовать мастер, т. к. все требуемые операции можно выполнить вручную в средстве **Управление дисками**. В частности, в виде **Список дисков** новый диск будет помечен красным значком со знаком восклицания, а его состояние указано как **Не проинициализирован**. Щелкните по значку диска правой кнопкой мыши и в контекстном меню выберите команду **Инициализировать диск** (Initialize Disk). Подтвердите выбранное действие (или добавьте другие диски для инициализации, если таковые имеются), а затем нажмите кнопку **OK**, чтобы начать процесс инициализации. Процедура преобразования диска в динамический рассматривается в *разд. "Преобразование базового диска в динамический и наоборот" далее в этой главе.*

Изменение типа таблицы разделов диска

Тип таблицы разделов диска можно изменять с MBR на GPT и наоборот. Эта возможность полезна в том случае, когда нужно перемещать приводы между компьютерами с разными процессорными архитектурами, или при получении новых дисков, тип которых не соответствует требуемому. Но тип таблицы разделов можно преобразовывать только на пустых дисках. Это означает, что диск должен быть новым или отформатированным. Очистить диск, конечно же, можно, удалив его разделы или тома.

Изменить тип таблицы разделов диска можно с помощью как средства **Управление дисками**, так и утилиты DiskPart. Чтобы использовать средство **Управление дисками**, запустите консоль **Управление компьютером** в окне **Администрирование** Панели управления либо выполните для этого команду `compmgmt.msc` в поле поиска панели **Приложения** или в консоли командной строки. В консоли **Управление компьютером** разверните узел **Запоминающие устройства** (Storage) и выберите в нем узел **Управление дисками**. В панели сведений консоли отобразятся все доступные диски. В левой панели вида **Графическое представление** щелкните на требуемом диске правой кнопкой мыши и в контекстном меню выберите требуемую опцию — **Преобразовать в GPT-диск** (Convert to GPT Disk) или **Преобразовать в MBR-диск** (Convert to MBR Disk).

Чтобы использовать утилиту DiskPart, запустите ее, выполнив команду `diskpart` в консоли командной строки, открытой с полномочиями администратора. Если требуется преобразовать, например, **Диск 2**, выполните команду `select disk 2`. Выбранный диск можно преобразовать с MBR в GPT, выполнив команду `convert gpt`. Чтобы преобразовать диск GPT в MBR, нужно выполнить команду `convert mbr`.

Пометка раздела в качестве активного

Обозначение раздела обычно изменять не требуется. В частности, если на компьютере установлена только Windows 8, или Windows 8 и любая другая версия Windows, изменять активный раздел не требуется. В дисках MBR активным обычно является основной раздел или первый простой том диска **Диск 0**. Если установить Windows 8 на диск C:, а на другой раздел, например диск D:, установить Windows 2000 или более позднюю версию Windows, чтобы загрузить Windows 8 или другую операционную систему, изменять активный раздел также не требуется. Но если нужно загрузить операционную систему, иную, чем Windows, раздел, в который установлена эта операционная система, обычно нужно обозначить как активный.

Примечание

Пометить активным можно только основной раздел, но не логические диски или тома. При преобразовании базового диска, содержащего активный раздел, в динамический диск, этот раздел становится простым томом, который автоматически помечается как активный.

Пометить раздел активным можно следующим образом:

1. Запустите средство **Управление дисками**, выполнив команду `diskmgmt.msc` в поле поиска панели **Приложения**.
2. Щелкните правой кнопкой мыши на требуемом основном разделе и в контекстном меню выберите команду **Сделать раздел активным** (Mark Partition as Active).

> ***Осторожно!***
>
> Если пометить раздел как активный, средство **Управление дисками** может отказаться изменять его обозначение, в результате чего после перезапуска компьютера операционная система может не загрузиться. Единым способом обойти эту проблему, который удалось найти автору книги, будет выполнить соответствующие изменения с помощью утилиты DiskPart либо перед перезагрузкой, либо перед использованием средства **Восстановление запуска** после неудачного запуска.

В листинге 12.1 приведен пример сеанса утилиты DiskPart по установке активного раздела.

Листинг 12.1. Пометка раздела активным посредством утилиты DiskPart

```
C:>diskpart

Microsoft DiskPart версии 6.2.8250
C) Корпорация Майкрософт (Microsoft Corporation) 1999-2012.
На компьютере: ENCPC85

DISKPART> select disk 0
Выбран диск 0.

DISKPART> list partition
  Раздел  ###   Тип              Размер  Смещение
  ------------ ---------------- ------- --------
  Раздел   1    Основной         151 Gб  31 Кб

DISKPART> select partition 1
Выбран раздел 1.

DISKPART> active
DISKPART: Раздел помечен как активный

DISKPART> exit
```

Как можно видеть в листинге 12.1, при запуске утилиты DiskPart отображается имя утилиты, ее версия, а также имя компьютера. Затем выбирается требуемый диск и выводится список его разделов. В данном примере выбран **Диск 0**, отображен список его разделов и выбран раздел 1. После выбора раздела диска с ним можно работать. В данном случае, просто выполняем команду `active`, чтобы сделать раздел активным. Выполнив все требуемые действия, закрываем утилиту DiskPart, выполнив команду `exit`.

> ***Примечание***
>
> Хотя в данном примере используется **Диск 0**, на вашей системе, возможно, нужно будет работать с другим диском. Вывести список доступных дисков, чтобы определить требуемый, можно, выполнив в утилите DiskPart команду `list disk`.

Преобразование базового диска в динамический и наоборот

Самым легким способом преобразовать базовой диск в динамический или наоборот можно с помощью средства **Управление дисками**. При преобразовании базового диска в динамический его разделы автоматически преобразуются в тома. В частности, все основные разделы и логические диски в расширенном разделе становятся простыми томами. Все невыделенное пространство в расширенном разделе помечается соответственно. Тома динамического диска нельзя преобразовать обратно в разделы. Чтобы преобразовать динамический диск в базовый, нужно удалить все его тома. Удаление томов также безвозвратно удаляет всю содержащуюся в них информацию.

Прежде чем приступать к преобразованию базового диска в динамический, необходимо удостовериться в том, что компьютер не требуется загружать предшествующей версией Windows. Кроме этого, в конце диска необходимо иметь 1 Мбайт свободного пространства. Хотя средство **Управление дисками** резервирует это свободное пространство при создании разделов и томов, средства управления дисками других операционных систем могут этого не делать, в результате чего преобразование завершится неудачно. Важно также иметь в виду следующие ограничения:

- преобразование съемных носителей в динамические диски невозможно. Приводы со съемными носителями можно настроить только как базовые диски с основными разделами;
- можно преобразовывать несистемные незагрузочные разделы диска, которые являются частью составного или чередующегося тома. Эти тома становятся динамическими томами такого же типа. Но при этом нужно преобразовать вместе все приводы набора.

Преобразование базового диска в динамический выполняется следующим образом:

1. В виде **Список дисков** или в левой панели вида **Графическое представление** консоли **Управление дисками** щелкните правой кнопкой мыши на требуемом базовом диске и в контекстном меню выберите команду **Преобразовать в динамический диск** (Convert to dynamic disk).
2. В открывшемся диалоговом окне **Преобразование в динамические диски** установите флажок диска, который требуется преобразовать (рис. 12.5).
3. Если диск не содержит отформатированных томов, нажатие кнопки **OK** выполняет преобразование диска, и следующие шаги выполнять не нужно. Если преобразуемый диск содержит отформатированные тома, нажатие кнопки **OK** открывает диалоговое окно **Диски для преобразования** (Disks to convert).

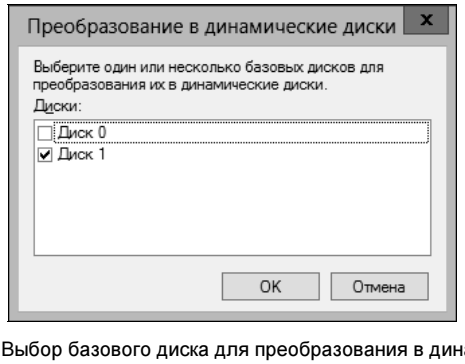


Рис. 12.5. Выбор базового диска для преобразования в динамический

4. Это окно содержит список преобразуемых дисков, чтобы можно было подтвердить их преобразование. Если диск отвечает требованиям для преобразования, в столбце **Будет преобразован** (Will convert) должно быть значение **Да**. Чтобы просмотреть информацию о разделах преобразовываемого диска, нажмите кнопку **Сведения** (Details). Удостоверившись в правильности всех данных, нажмите кнопку **ОК**, чтобы закрыть окно сведений о разделах.
5. Чтобы начать преобразование, нажмите кнопку **Преобразовать**. Появится окно с предупреждением, что после преобразования невозможно будет загружать предыдущие версии Windows с томов преобразуемого диска. Нажмите кнопку **Да**, чтобы продолжить процесс преобразования.
6. Далее выводится предупреждение об отключении файловых систем дисков. Это означает, что они будут временно недоступными. Нажмите кнопку **Да**, чтобы продолжить процесс преобразования. Если преобразуемый диск содержит загрузочный или системный раздел либо раздел, который используется в данный момент, компьютер потребуется перезагрузить, о чем будет извещено в следующем окне.

Преобразование динамического диска в базовый выполняется следующим образом:

1. Чтобы динамический диск можно было преобразовать в базовый, нужно удалить все его тома. Так как удаление томов также безвозвратно удаляет находящиеся на них данные, если эти данные требуется сохранить, для удаляемых томов следует создать резервные копии, а затем сверить эти копии с соответствующими томами, и только потом приступать к удалению томов. Удаление последнего тома автоматически преобразует динамический диск в базовый, на котором, если необходимо, можно опять создавать разделы и логические диски.
2. Чтобы преобразовать динамический диск, не содержащий томов, щелкните на нем правой кнопкой мыши в консоли **Управление дисками** и в контекстном меню выберите команду **Преобразовать в базовый диск** (Convert to basic disk).

Работа с дисками, разделами и томами

Прежде чем физический диск можно использовать для хранения на нем данных, его нужно подготовить, установив тип диска, разбив его при необходимости на разделы, присвоив букву и отформатировав его разделы и тома.

После разбиения диска на разделы или тома каждому разделу или тому нужно присвоить указатель, который может быть буквой или путем. Буквы диска позволяют получить доступ к файловым системам разделов физического диска. В общем, дискам можно присваивать буквы (латинского алфавита) от A до Z. Но буква A исторически зарезервирована для присвоения приводу гибких дисков системы. Кроме этого, если система оснащена другим приводом гибких дисков или другим приводом со съемным носителем, буква B присваивается этому приводу. При отсутствии таких приводов буква B не используется. Буква C обычно присваивается первому разделу диска 0, а буква D — первому приводу оптических дисков (CD/DVD). Таким образом, на большинстве систем для присвоения дискам доступны буквы от E до Z.

Если этих букв недостаточно, диски можно обозначать как папку NTFS на существующем локальном диске, указав путь к ней. Например, разделы или тома можно подключить как папки C:\Docs1, C:\Docs2 и C:\Docs3. Подключать к папкам можно как базовые, так и динамические диски. Единым условием является то, что это должны быть пустые папки на локальных дисках формата NTFS.

Форматирование раздела или тома задает для него файловую систему и создает на нем соответствующие файловые структуры. По большому счету, раздел или том можно форматировать как FAT, FAT32 или NTFS. Но использование каждой из этих файловых систем подлежит определенным ограничениям и условиям.

Файловая система FAT, которая также называется FAT16, является 16-разрядной файловой системой, предназначенной для использования с томами размером до 4 Гбайт. Файловая система FAT использует загрузочный сектор, в котором сохраняется информация о типе диска, первом и последнем секторах и активном разделе. Эта система берет свое название из таблицы размещения файлов[1], которая используется для отслеживания размещения кластеров файлов и папок. Система использует две таких таблицы — одну основную и вторую запасную. Запасная таблица применяется для восстановления основной таблицы в случае ее повреждения. Файловая система FAT также может помечать кластеры (секции диска, содержащие данные), как неиспользуемые, используемые, поврежденные или зарезервированные. Все это способствует довольно высокой степени надежности этой файловой системы. Система FAT лучше всего проявляет себя с томами размеров до 2 Гбайт; максимальный размер файлов, допускаемый этой системой, составляет 2 Гбайт. Эту систему также можно использовать для гибких и съемных дисков.

Файловая система FAT32 представляет собой 32-разрядную версию системы FAT16, обладающую некоторыми дополнительными возможностями и свойствами. Подобно FAT16, FAT32 использует основную и запасную таблицы размещения файлов. Эта система может помечать кластеры, как неиспользуемые, используемые, поврежденные или зарезервированные, и также ее можно использовать для гибких и съемных дисков. Файловая система FAT32 поддерживает минимальный размер тома в 33 Мбайт, максимальный — в 32 Гбайт, а максимальный размер файлов в 4 Гбайт.

Расширенная файловая система exFAT является улучшенной, 64-разрядной версией FAT. Для сохранения скорости доступа и других преимуществ FAT систему exFAT следует использовать с томами размером больше 32 Гбайт. Операционная система Windows 8 поддерживает файловую систему exFAT как на внутренних, так и на внешних томах.

> ***Примечание***
>
> Ограничение файловой системой FAT32 максимального размера файлов к 4 Гбайт присуще Windows 2000 и более поздним версиям Windows. Некоторые более ранние версии Windows, а также другие операционные системы могут создавать в FAT32 тома большего размера.

Файловая система NTFS существенно отличается от FAT. В частности, для хранения информации о файлах и папках эта система вместо таблицы размещения файлов использует реляционную базу данных. Эта база данных называется *главной файловой таблицей* (или таблицей MFT[2]) и содержит запись для каждого файла и каждой папки тома, а также дополнительную информацию, используемую для содержания тома. В целом, благодаря использованию таблицы MFT, файловая система NTFS является более надежной и восстанавливаемой, чем FAT16 или FAT32. Файловую систему NTFS можно восстанавливать после ошибок диска с большей легкостью, чем FAT16 или FAT32; кроме этого, эта система испытывает меньшее число ошибок диска.

Файловая система exFAT использует транзакции для улучшения надежности и восстанавливаемости и обладает некоторыми, но не всеми, аспектами надежности системы NTFS. Как NTFS, так и exFAT поддерживают тома максимального размера в 256 Тбайт для дисков

[1] File Allocation Table — FAT.

[2] Master File Table.

стандартных форматов, а максимальный размер файла ограничивается только размером тома.

Хотя ни NTFS, ни exFAT нельзя использовать для гибких дисков, их можно использовать для приводов со съемными носителями. Кроме этого, в отличие от FAT16 и FAT32, которые обладают ограниченными возможностями обеспечения безопасности (в частности, позволяя только помечать файл как только для чтения, скрытый или системный), система exFAT поддерживает основные функциональности контроля доступа. Но только система NTFS обладает расширенными функциональностями обеспечения безопасности, которые позволяют использовать разрешения для установки определенного уровня доступа к ним, и только NTFS поддерживает другие расширенные возможности, такие как сжатие и шифрование дисков и дисковые квоты.

Примечание

Существует несколько версий файловой системы NTFS. Версия NTFS 5 была впервые доступна с Windows 2000, а версия NTFS 5.1 — с Windows XP. Так как большинство современных компьютеров использует NTFS 5 или более позднюю версию, основное внимание в этой книге уделяется этим версиям. Кроме этого, при обновлении системы к более поздней версии Windows предоставляется возможность преобразовать существующие тома NTFS к более поздней версии этой файловой системы в процессе установки. В большинстве случаев следует воспользоваться этой возможностью, т. к. это обеспечивает поддержку самых последних функциональностей этой файловой системы. Узнать текущую версию NTFS тома можно, выполнив в консоли командной строки, открытой от имени администратора, следующую команду:

```
fsutil fsinfo ntfsinfo c:
```

где `c:` обозначает требуемый диск. Но если в результате исполнения этой команды показана версия NTFS 3.1, в действительности это версия NTFS 5.1.

Разбивка дисков на разделы и подготовка их к использованию

Основным инструментом для разбивки дисков на разделы и подготовки их к использованию является средство **Управление дисками**. С его помощью диски можно разбивать на разделы, присваивать разделам буквы, а также форматировать разделы и тома. Дополняют это средство утилита командной строки DiskPart и команда `Format`.

Создание разделов, логических дисков и простых томов

Для упрощения работы со средством **Управление дисками** в нем используется один и тот же набор диалоговых окон и мастеров как для работы с разделами, так и для работы с томами. Первые три тома базового диска автоматически создаются как основные разделы. При создании четвертого тома на базовом диске оставшееся свободное пространство диска автоматически преобразуется в расширенный раздел, а создаваемый том указанного размера создается как логический диск в этом разделе. Все последующие тома в оставшемся на диске месте создаются как логические диски в расширенном разделе.

Примечание

Как отмечалось ранее, диск MBR может иметь только четыре основных раздела. Но если создать четвертый основной раздел, дальнейшее разбиение диска будет невозможным, поэтому Windows 8 автоматически и создает четвертый раздел расширенным. Наличие расширенного раздела позволяет продолжить разбиение диска, создавая в расширенном разделе логические диски.

С помощью средства **Управление дисками** разделы, логические диски и простые тома создаются следующим образом:

1. В виде **Графическое представление** средства **Управление дисками** щелкните правой кнопкой мыши на нераспределенном или свободном пространстве диска и в контекстном меню выберите команду **Новый простой том** (New simple volume). Запустится мастер создания простого тома (New Simple Volume Wizard). Ознакомьтесь с инструкциями на странице приветствия мастера и нажмите кнопку **Далее**.
2. На странице **Указание размера тома** (Specify Volume Size) (рис. 12.6) отображается минимальный и максимальный допустимый размер создаваемого тома в мегабайтах и предоставляется возможность задать размер нового тома в этих пределах. Укажите требуемый размер для создаваемого простого тома в соответствующем поле, а затем нажмите кнопку **Далее**.

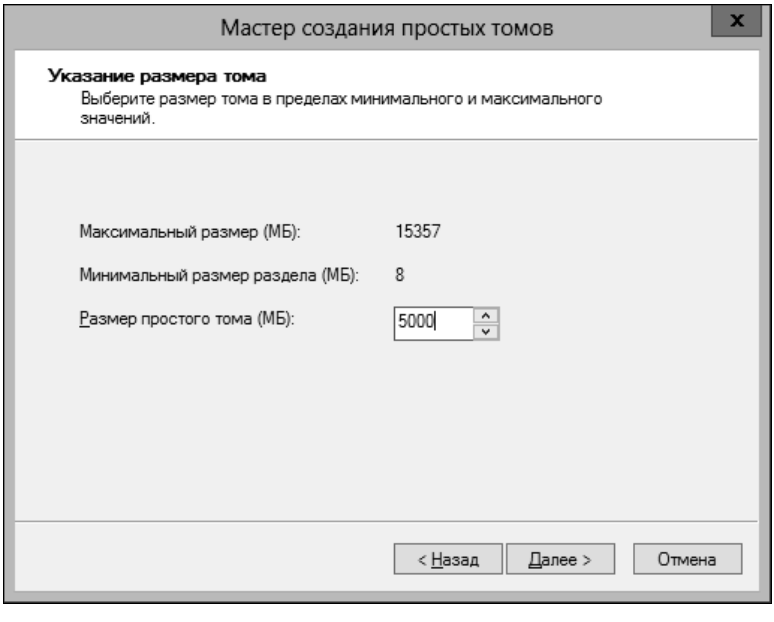


Рис. 12.6. Установка размера нового простого тома

3. На странице **Назначение буквы диска или пути** (Assign Drive Letter or Path) (рис. 12.7) присвойте создаваемому тому букву диска или подключите к пустой папке NTFS на локальном диске, указав путь к ней, и нажмите кнопку **Далее**.

   Значения доступных опций следующие.

   - **Назначить букву диска** (Assign the following drive letter). Выберите в предоставленном списке букву, которую надо присвоить диску. По умолчанию Windows 8 предлагает самую последнюю доступную букву и исключает из списка буквы зарезервированных приводов, а также буквы, уже присвоенные локальным или сетевым дискам.
   - **Подключить том как пустую NTFS-папку** (Mount in the following empty NTFS folder). Эта опция полезна, когда по каким-либо причинам диск нельзя или нежелательно обозначать буквой. Путь к существующей папке можно ввести в поле или же выполнить поиск требуемой папки, нажав кнопку **Обзор**.

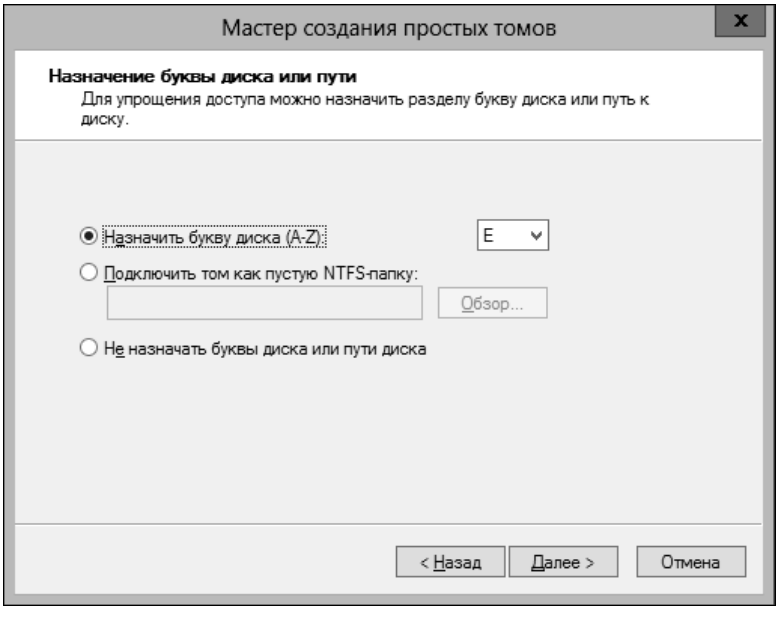


Рис. 12.7. Присвоение указателя диска

- **Не назначать буквы диска или пути диска** (Do not assign a drive letter or drive path). Эта опция полезна, когда по каким-либо причинам обозначение диска нежелательно выполнять в данный момент. Обозначить диск буквой или подключить его к папке можно будет в дальнейшем.

Примечание

Присваивать томам букву или подключать к папке не обязательно. Просто необозначенный никаким образом том считается неподключенным и, по большому счету, является бесполезным. Неподключенный том можно подключить, присвоив ему букву или путь к папке. Дополнительную информацию по этому вопросу *см. в разд. "Присвоение, изменение и удаление буквы или пути диска" далее в этой главе*.

4. На следующей странице мастера, **Форматирование раздела** (Format Partition) (рис. 12.8), можно выбрать файловую систему для форматирования раздела и ее дополнительные параметры.

   Если раздел нужно отформатировать, установите переключатель **Форматировать этот том следующим образом** (Format this volume with the following settings) и настройте следующие параметры.

   - **Файловая система** (File system). Выбор файловой системы: FAT, FAT32 или NTFS. В большинстве случаев по умолчанию выбрана NTFS. Файловые системы FAT и FAT32 можно в дальнейшем преобразовать в NTFS с помощью утилиты Convert, но обратное преобразование невозможно.
   - **Размер кластера** (Allocation unit size). Выбор размера кластера для файловой системы. Кластер представляет собой базовую единицу выделения дискового пространства. Размер кластера по умолчанию зависит от выбранной файловой системы и размера тома и по умолчанию устанавливается динамически перед форматированием. Значение по умолчанию можно заменить другим, более подходящим значением. Например, при работе в основном с большим количеством файлов небольшого раз-

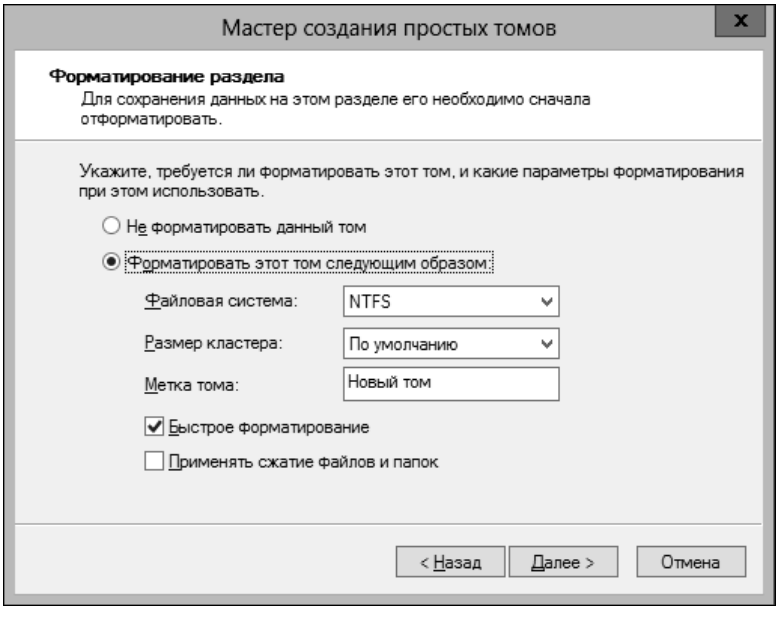


Рис. 12.8. Выбор файловой системы раздела и дополнительных параметров для нее

мера желательно использовать меньший размер кластера, например 512 или 1024 байта. Таким образом, файлы будут занимать меньше дискового пространства.

- **Метка тома** (Volume label). Текстовое имя раздела; по умолчанию установлено как **Новый том** (New Volume). Тому можно присвоить любое имя в дальнейшем. Для этого нужно щелкнуть правой кнопкой мыши на значке диска в Проводнике Windows, в контекстном меню выбрать команду **Свойства** и ввести новое имя тома в текстовое поле на вкладке **Общие**.
- **Быстрое форматирование** (Perform a quick format). Установка этого флажка задает быстрое форматирование раздела, без проверки на наличие в нем ошибок. В случае разделов больших размеров эта опция может сэкономить несколько минут. Но обычно желательно выполнить проверку на наличие ошибок. В таком случае средство **Управление дисками** пометит поврежденные секторы раздела и заблокирует их.
- **Применять сжатие файлов и папок** (Enable file and folder compression). Установка этого флажка включает функциональность автоматического сжатия данных тома. Эта возможность доступна только для файловой системы NTFS. В этой файловой системе сжатие прозрачно для пользователей и доступ к сжатым файлам осуществляется, как и к обычным файлам. Дополнительную информацию по сжатию дисков, файлов и папок *см. в разд. "Сжатие дисков и данных" далее в этой главе.*

5. Нажмите кнопку **Далее**, а на следующей странице — кнопку **Готово**.

Создание составных и чередующихся томов

Объединение или чередование дисков позволяет создать том, охватывающий несколько физических дисков. При работе с дисками этих типов следует иметь в виду следующее.

♦ Составной том использует свободное пространство нескольких дисков одинакового типа. Нераспределенное пространство на двух или больше дисках одного и того же типа

можно использовать, чтобы создать составной том. Составной том не обеспечивает отказоустойчивости и обладает посредственными характеристиками производительности чтения и записи. Данные записываются на весь составной том в произвольном порядке. В случае отказа одного диска из набора тома выходит из строя весь том и теряются все находящиеся на нем данные.

- Чередующийся том использует свободное пространство нескольких дисков и распределяет записываемые данные по всем дискам тома. В большинстве случаев чередование дисков ускоряет операции записи и чтения, т. к. данные считываются или записываются одновременно на несколько физических дисков. Например, в случае чередующегося тома, состоящего из набора трех дисков, данные одного файла будут одновременно записываться блоками по 64 Кбайт на диск 1, диск 2, диск 3, диск 1, диск 2 и т. д. по кругу. Подобно составному тому, чередующийся том не обеспечивает отказоустойчивость и при сбое одного из дисков набора из строя выходит весь том, с соответствующей потерей всех содержащихся на нем данных. Этот метод организации дисков называется RAID-0.
- С чередующимся томом, состоящим из набора трех или больше отдельных дисков, можно применять контроль по четности. В таком случае при отказе одного из дисков набора тома данные всего тома можно восстановить по данным и информации контроля четности на остальных дисках набора. Этот подход называется RAID-5 и обеспечивает отказоустойчивость при меньших накладных расходах и лучшей производительностью чтения, чем зеркалирование дисков.

Примечание

Составной или чередующийся том нельзя создать с одним физическим приводом. Также обратите внимание на то, что простые и составные тома можно расширять, чтобы увеличить их размер. Но тома RAID-0 и RAID-5 расширять нельзя. Поэтому при создании тома RAID-0 или RAID-5 следует удостовериться в том, что задаваемый размер будет достаточным для ваших целей. В противном случае, чтобы увеличить размер чередующегося тома, его придется удалить и создать повторно. Кроме этого, загрузочный и системный диски не должны входить в набор RAID-0 или RAID-5. Не используйте RAID-0 или RAID-5 с этими томами.

Дополнительная информация

Чтобы обеспечить отказоустойчивость тома RAID-5, на каждый из дисков набора тома вместе с блоками данных записывается информация контроля по четности. В случае отказа одного из дисков набора чередующегося тома, его данные можно восстановить по данным и информации контроля по четности других дисков. Но при одновременном отказе двух дисков оставшейся информации будет недостаточно для восстановления данных тома, и ее нужно будет восстанавливать с резервной копии.

Создать составной или чередующийся том с помощью средства **Управление дисками** можно следующим образом:

1. В виде **Графическое представление** средства **Управление дисками** щелкните правой кнопкой мыши по нераспределенному или свободному пространству диска и в контекстном меню выберите требуемую опцию: **Создать составной том** (New Spanned Volume), **Создать чередующийся том** (New Striped Volume), **Создать том RAID-5** (New RAID-5 Volume). Ознакомьтесь с инструкциями на странице приветствия мастера и нажмите кнопку **Далее**. Имейте в виду, что хотя Windows 8 поддерживает создание составных и чередующихся томов из базовых дисков, некоторые базовые диски для этой цели не подходят.
2. На странице **Выбор дисков** мастера выберите диски, которые будут входить в состав тома, и укажите для каждого диска размер выделяемого на нем пространства. Все диски должны быть одного типа, т. е. либо все базовые, либо все динамические.

Диски, которые можно добавить в том, указаны в левой панели **Доступные** (Available). Выберите в этом списке требуемый диск и нажмите кнопку **Добавить**, чтобы поместить его в панель **Выбраны** (Selected). Ошибочно добавленный диск можно удалить из списка **Выбраны**, указав его и нажав кнопку **Удалить**.

Для каждого диска в поле **Выберите размер выделяемого пространства** (Select the amount of space in MB) укажите пространство, которое следует выделить на нем для тома. Обратите внимание, что в поле **Максимальное доступное пространство** (Maximum) указано все свободное пространство на выбранном диске, а в поле **Общий размер тома** (Total volume size) — все пространство тома, равное сумме выделенных пространств на каждом диске.

Совет

Задать одинаковое выделяемое пространство на всех выбранных дисках можно следующим способом. Выберите все диски в поле **Выбраны**, нажав и удерживая клавишу <Shift> и щелкнув на первом, а затем на последнем диске в списке. Теперь при указании выделяемого пространства этот размер устанавливается для всех выбранных дисков.

3. Указав и настроив диски для составного или чередующегося тома, нажмите кнопку **Далее**.
4. Выполните шаги 3—5 процедуры предыдущего раздела, *"Создание разделов, логических дисков и простых томов"*.

Расширение и сжатие томов

Для загрузки операционной системы Windows 8 не используются файлы Ntldr и Boot.ini. Вместо них применяется предзагрузочная среда, в которой для управления запуском системы и загрузки выбранного приложения для загрузки операционной системы используется *диспетчер загрузки Windows* (Windows Boot Manager). Он также освобождает Windows от зависимости от MS-DOS, позволяя использовать диски недоступными ранее способами. В частности, Windows 8 позволяет расширять и сжимать базовые и динамические тома с помощью средства **Управление дисками** или утилиты DiskPart. Чередующиеся тома расширять и сжимать нельзя.

При расширении тома к нему добавляется нераспределенное пространство. В случае составных томов на динамических дисках это пространство может браться из любого доступного динамического диска, а не только из тех, из которых том был изначально создан. Это позволяет объединить нераспределенное пространство нескольких динамических дисков и использовать это объединенное пространство для расширения пространства существующего тома.

Осторожно!

Прежде чем приступать к расширению тома, нужно быть осведомленным о нескольких ограничениях в этом отношении. Прежде всего, можно расширять только простые и составные тома, которые отформатированы под файловую систему NTFS. Чередующиеся тома расширять нельзя. Неотформатированные тома или отформатированные под файловую систему FAT, FAT32 или exFAT тома расширять нельзя. Кроме этого, нельзя расширять системные или загрузочные тома независимо от их конфигурации.

Сжать базовый, простой или составной том можно следующим образом:

1. В средстве **Управление дисками** щелкните правой кнопкой мыши на требуемом томе и в контекстном меню выберите команду **Сжать том** (Shrink volume). Эта опция будет доступна только в том случае, если том отвечает всем вышеизложенным требованиям.

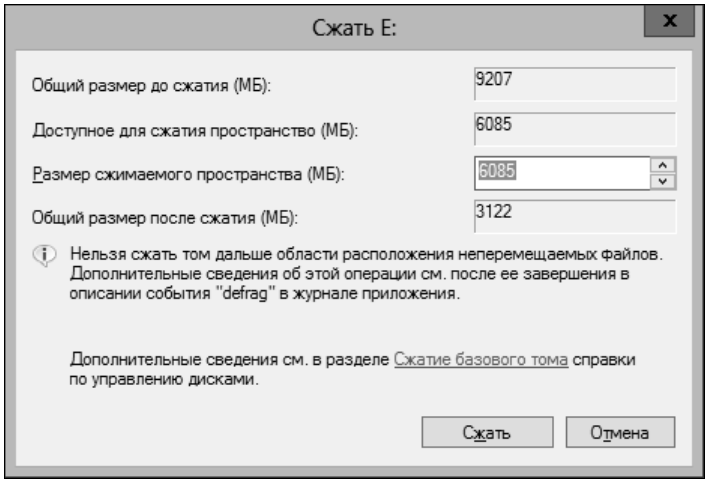


Рис. 12.9. Диалоговое окно для сжатия тома

2. В диалоговом окне сжатия тома (рис. 12.9) укажите размер, на который нужно сократить объем тома.

   Диалоговое окно сжатия тома содержит следующую информацию, которая может быть полезной при задании объема сокращаемого пространства тома.

   - **Общий размер до сжатия (МБ)** (Total size before shrink in MB). Общий исходный размер отформатированного тома в мегабайтах.
   - **Доступное для сжатия пространство (МБ)** (Size of available shrink space in MB). Максимальное пространство, на которое можно сократить размер тома. Это не общее пространство тома, а пространство, которое можно удалить из него, за вычетом пространства, зарезервированного для главной файловой таблицы, снимков тома, файлов подкачки и временных файлов.
   - **Размер сжимаемого пространства (МБ)** (Enter the amount of space to shrink in MB). Размер пространства, которое будет удалено с тома. По умолчанию исходное значение этого параметра равно всему доступному для удаления с тома пространству. Но для оптимальной работы привода нужно обеспечить, чтобы после сжатия том имел, по крайней мере, 10% свободного пространства от общего нового размера тома.
   - **Общий размер после сжатия (МБ)** (Total size after shrink in MB). Общий конечный размер отформатированного тома в мегабайтах.

3. Указав размер удаляемого из тома пространства, нажмите кнопку **OK**, чтобы выполнить сжатие и закрыть окно.

Расширить базовый, простой или составной том можно следующим образом:

1. В средстве **Управление дисками** щелкните правой кнопкой мыши на требуемом томе и в контекстном меню выберите команду **Расширить том** (Shrink volume). Эта опция будет доступна только в том случае, если том отвечает всем требованиям, изложенным в замечании "Осторожно!" перед процедурой сжатия тома.
2. Ознакомьтесь с инструкциями и информацией на странице приветствия мастера расширения тома, а затем нажмите кнопку **Далее**.
3. На странице выбора дисков укажите диск или диски, с которых можно добавить пространство на расширяемый том. На этой странице автоматически выбираются все диски

со свободным пространством, которые входят в состав тома. По умолчанию все оставшееся невыделенное пространство на этих дисках будет добавлено в расширяемый том.

4. Кроме свободного пространства дисков, составляющего том, в него можно добавить невыделенное пространство с других дисков. Делается это следующим образом:
   - выберите в списке **Доступны** требуемый диск и нажмите кнопку **Добавить**, чтобы поместить его в панель **Выбраны**;
   - для каждого диска в списке **Выбраны** в поле **Выберите размер выделяемого пространства** укажите пространство, которое следует выделить на нем для расширяемого тома.
5. Нажмите кнопку **Далее**, подтвердите указанные действия, а затем нажмите кнопку **Готово**.

Форматирование разделов и томов

При форматировании раздела или тома на нем создается файловая система для хранения данных; при этом процесс форматирования безвозвратно удаляет все данные в соответствующей части физического диска. В данном случае имеет место форматирование высшего уровня, которое создает файловую систему, а не форматирование низкого уровня, которое инициализирует диск. (Новые диски инициализируются при подключении, если они уже не были инициализированы производителем.) Чтобы выполнить форматирование раздела или тома, щелкните правой кнопкой мыши на требуемом элементе в средстве **Управление дисками** и в контекстном меню выберите команду **Форматировать**. Откроется диалоговое окно **Форматирование** (рис. 12.10). Если сравнить это окно с окном на рис. 12.8, можно видеть, что оба окна имеют практически одинаковые опции.

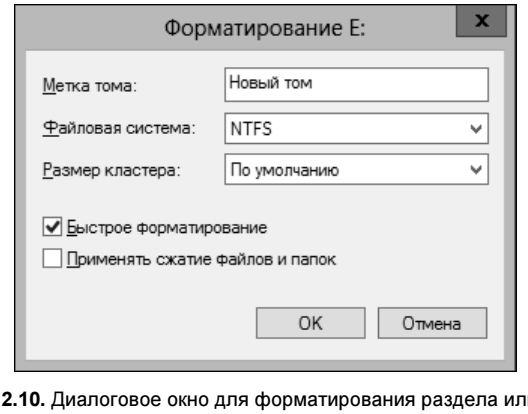


Рис. 12.10. Диалоговое окно для форматирования раздела или тома

Задав требуемые опции форматирования, нажмите кнопку **OK**. Так как форматирование уничтожает все данные на затронутом разделе, средство **Управление дисками** предоставляет последнюю возможность удостовериться в правильности выполняемого действия и, если необходимо, отменить его. Чтобы начать процесс форматирования, нажмите кнопку **OK** в этом окне предупреждения. В столбце **Состояние** данного раздела отображается параметр **Форматирование** и, если не была выбрана опция быстрого форматирования, процент выполнения. По завершению форматирования для диска отображаются все параметры о его состоянии.

Присвоение, изменение и удаление буквы или пути диска

Каждому основному разделу, тому или логическому диску компьютера можно присвоить одну букву диска и один или несколько путей к пустой NTFS-папке. Присвоенная буква диска и/или пути к папке остаются неизменными при каждом запуске компьютера. За исключением загрузочных и системных разделов или томов, букву диска и его пути к папке можно изменить в любое время. Так, за исключением загрузочных и системных разделов или томов, букву диска и его пути к папке можно удалить в любое время.

Управление буквами дисков и их подключениями к папкам выполняется с помощью средства **Управление дисками**. Для этого в виде **Список томов** или **Графическое представление** щелкните правой кнопкой мыши на требуемом разделе или томе и в контекстном меню выберите команду **Изменить букву диска или путь к диску** (Change drive letter and paths). Откроется диалоговое окно **Изменение буквы диска или путей** (рис. 12.11).

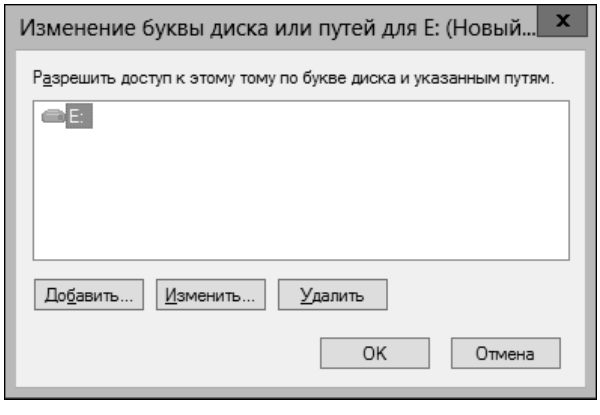


Рис. 12.11. Диалоговое окно для управления буквой и путями диска

В этом окне можно выполнять следующие настройки.

- **Добавить путь к папке.** Нажмите кнопку **Add**, установите переключатель **Подключить том как пустую NTFS-папку** (если диску присвоена буква, этот переключатель будет уже установлен), а затем введите путь к пустой папке NTFS. Можно также нажать кнопку **Обзор** и или указать существующую папку либо создать новую.
- **Удалить путь к папке.** Выберите в списке требуемый путь, нажмите кнопку **Удалить**, а затем подтвердите удаление, нажав кнопку **Да** в окне запроса на подтверждение удаления.
- **Присвоить диску букву.** Букву диску можно присвоить, только если он еще не имеет буквы. Нажмите кнопку **Добавить**, установите переключатель **Назначить букву диска** и в раскрывающемся списке выберите одну из доступных букв.
- **Изменить букву диска.** Выберите текущую букву диска и нажмите кнопку **Изменить**. В следующем окне установите переключатель **Назначить букву диска** и в ракрывающемся списке выберите одну из доступных букв.
- **Удалить букву диска.** Выберите в списке текущую букву диска, нажмите кнопку **Удалить**, а затем подтвердите удаление, нажав кнопку **Да** в окне запроса на подтверждение удаления.

Примечание

При попытке изменить букву используемого в настоящий момент диска (например, на диске может быть открыта папка или документ) Windows 8 выводит предупреждающее сообщение, что программы, использующие эту букву диска, могут перестать работать после ее смены. В таком случае нужно закрыть программы, которые используют данный диск, а затем попытаться снова изменить букву или же разрешить принудительное изменение буквы, нажав кнопку **Да** в окне предупреждения.

Практический совет

Если буква, которую вы хотите присвоить диску, отсутствует в раскрывающемся списке, это означает, что она зарезервирована для других целей. Иногда эту проблему можно решить временной заменой букв дисков. Например, если буква D используется приводом CD/DVD, а буква E — локальным жестким диском, может быть желательным поменять эти буквы местами — D для жесткого диска, а E для привода CD/DVD. Для этого нужно удалить букву привода CD/DVD, чтобы освободить ее, а затем присвоить ее локальному жесткому диску, заменив ею его прежнюю букву E. Это освобождает букву E, которую теперь можно присвоить приводу CD/DVD. Но при этом следует иметь в виду, что изменение буквы диска может иметь последствия. Например, путь к приложению, хранящийся в реестре, может содержать букву диска. После смены буквы диска этот путь будет недействительным, и приложение перестанет запускаться. Также изменение буквы диска повлияет на ярлыки к файлам и программам на затрагиваемом диске, и их нужно будет откорректировать или создать заново.

Присвоение, изменение и удаление метки тома

Метка тома представляет собой краткое текстовое описание раздела или тома. Метка тома отображается при просмотре диска в разных утилитах Windows 8, например в Проводнике Windows и консоли **Компьютер**, предоставляя дополнительную информацию о содержимом диска.

Примечание

В файловой системе FAT и FAT32 метка тома может содержать до 11 символов и включать пробелы. В файловой системе NTFS длина метки тома может быть до 32 символов. Также метка тома в NTFS может содержать некоторые специальные символы, в том числе * / \ [ ] : ; | = , . + " ? < >, в то время как в FAT и FAT32 эти символы запрещены.

Метку тома можно присваивать, изменять и удалять в средстве **Управление дисками** или с помощью консоли **Компьютер**. Процедура использования для этой цели средства **Управление дисками** следующая:

1. Откройте консоль **Управление компьютером**, разверните в ней узел **Запоминающие устройства** и выберите в нем узел **Управление дисками**.
2. В виде **Список томов** щелкните правой кнопкой мыши по значку требуемого диска и в контекстном меню выберите команду **Свойства**.
3. На вкладке **Общие** окна свойств диска удалите из текстового поля текущую метку тома и, если требуется, введите новую. Нажмите кнопку **OK**.

Процедура использования для этой цели консоли **Компьютер** следующая:

1. Щелкните по значку Проводника Windows на панели задач, а затем щелкните по значку **Компьютер** в левой панели Проводника.
2. Щелкните правой кнопкой мыши по значку требуемого диска и в контекстном меню выберите команду **Свойства**.
3. На вкладке **Общие** окна свойств диска удалите из текстового поля текущую метку тома и, если требуется, введите новую. Нажмите кнопку **OK**, чтобы сохранить настройку и закрыть окно.

Удаление разделов, томов и логических дисков

Чтобы изменить конфигурацию диска, чье пространство полностью выделено, может потребоваться удалить существующие на нем разделы, логические диски или тома. Так как такое удаление необратимо и влечет за собой удаление находящихся на этой части диска данных, прежде чем удалять раздел, логический диск или том, всегда следует создать и проверить резервную копию важных файлов и папок. Также следует быть осторожным при удалении составных или чередующихся томов. Удаление одного из дисков набора такого тома удаляет весь набор дисков, означая необратимое удаление всего тома и хранящихся на нем данных.

Осторожно!

Удаление раздела, логического диска или раздела является радикальным шагом, который нельзя отменить. Это действие удаляет связанную файловую систему и все данные, хранящиеся в этой файловой системе, также безвозвратно удаляются.

Примечание

С целью защиты целостности системы не разрешается удаление системного или загрузочного раздела. Но Windows 8 позволяет удалять активные разделы или тома, которые не являются системными или загрузочными. Поэтому всегда проверяйте, что удаляемый раздел или том не содержит важных данных.

Удалять основной раздел, том или логический диск можно следующим образом:

1. В средстве **Управление дисками** щелкните правой кнопкой мыши по требуемому разделу, тому или логическому диску и в контекстном меню выберите команду **Проводник** (Explore). В Проводнике Windows переместите все данные с удаляемого раздела на другой раздел или проверьте существующую резервную копию раздела, чтобы обеспечить сохранность данных.
2. В средстве **Управление дисками** снова щелкните правой кнопкой мыши по требуемому разделу, тому или логическому диску и в контекстном меню выберите требуемую опцию — **Удалить раздел**, **Удалить том** или **Удалить логический диск**.
3. В окне запроса подтверждения нажмите кнопку **Да**, чтобы подтвердить удаление выбранного элемента.

Удаление расширенного раздела слегка отличается от удаления основного раздела или логического диска. Чтобы удалить расширенный раздел, сначала нужно удалить все его логические диски, следуя вышеописанной процедуре. После этого можно выбрать собственно область расширенного раздела и удалить его.

Преобразование файловой системы тома в NTFS

Операционная система Windows 8 предоставляет утилиту командной строки для преобразования файловой системы FAT или FAT32 в NTFS. Утилита называется Convert; ее исполняемый файл, convert.exe, находится в папке *%SystemRoot%*\System32. При выполнении преобразования посредством этого инструмента файловая структура раздела сохраняется, и потеря данных не происходит.

Осторожно!

Операционная система Windows 8 не предоставляет никаких средств для преобразования файловой системы NTFS в FAT или FAT32. Единственным способом выполнить такое преобразование будет удалить требуемый раздел, используя описанную в предыдущем разделе процедуру, а затем создать новый раздел, указав для него файловую систему FAT или FAT32. Также обратите внимание на то обстоятельство, что утилита Convert не преобразует формат exFAT в NTFS.

Команда для преобразования файловой системы тома имеет следующий формат:

```
convert том /FS:NTFS
```

где *том* обозначает букву диска с двоеточием, путь к папке подключения диска или имя тома. Например, для преобразования в NTFS диска D: применяется следующая команда:

```
convert D: /FS:NTFS
```

Полный синтаксис команды `convert` выглядит так:

```
convert том /FS:NTFS [/V] [/X] [/CvtArea:имя_файла] [/NoSecurity]
```

Параметры и переключатели команды имеют следующее значение:

- *том* — том для преобразования, должен содержать полный указатель диска (буква диска с двоеточием). Можно также указать путь к папке подключения диска или имя тома;
- `/FS:NTFS` — задает преобразование файловой системы указанного тома в NTFS. Это единственный выбор файловой системы;
- `/V` — вывод подробных сведений в процессе преобразования;
- `/X` — принудительное отключение тома перед преобразованием (если необходимо);
- `/CvtArea:`*имя_файла* — задает непрерывный файл в корневом каталоге для резервирования места для системных файлов NTFS, хранящихся в таблице MFT. Если имя файла не указано, утилита Convert по умолчанию резервирует для этой цели 12,5% от общего размера тома или раздела. Это способствует предотвращению фрагментации таблицы MFT;
- `/NoSecurity` — устанавливает для всех файлов и папок параметры доступа NTFS, разрешающие доступ к ним членам группы Все (Everyone). Таким образом, доступ предоставляется любому пользователю, который имеет локальный или удаленный доступ к системе.

Прежде чем начинать преобразование, утилита Convert проверяет наличие достаточного свободного места на диске для выполнения этой операции. В общем, утилите требуется блок свободного пространства диска, составляющий около 25% от общего объема диска. Например, для преобразования диска размером в 100 Гбайт утилите требуется на нем 25 Гбайт свободного места. При недостатке свободного места преобразование не выполняется и выводится сообщение о необходимости освободить место на диске. При наличии достаточного свободного места утилита начинает процесс преобразования, который может занять несколько минут (чем больше диск, тем дольше). Не пытайтесь использовать файлы или приложения, находящиеся на диске, пока выполняется преобразование.

Примечание

Прежде чем выполнять преобразование диска с помощью утилиты Convert, проверьте, не является ли затрагиваемый раздел активным загрузочным или системным разделом. Активный загрузочный раздел дисков MBR можно преобразовывать в NTFS, но для этого системе требуется получить исключительный доступ к этому разделу, что возможно только при загрузке системы. Поэтому при попытке преобразовать активный загрузочный раздел в NTFS выводится запрос запланировать преобразование на следующую загрузку системы. Нажав кнопку **Да**, можно перезагрузить систему, чтобы начать процесс преобразования. Часто для завершения преобразования требуется несколько раз перезагрузить систему. Не паникуйте, и дайте системе возможность продолжить преобразование.

Практический совет

Можно улучшить производительность преобразованного тома, зарезервировав на нем место для таблицы MFT, используя в команде `convert` параметр `/CvtArea`. Этот подход способствует предотвращению фрагментации таблицы MFT. Каким образом? Со временем таблица MFT может

превысить объем диска, выделяемый ею при преобразовании в NTFS по умолчанию. В таком случае операционной системе требуется расширить таблицу MFT в другие области диска. Хотя утилита дефрагментации дисков Windows 8 может также дефрагментировать таблицу MFT, она не может переместить первую часть таблицы, а вероятность наличия свободного места после первой части очень незначительная, т. к. это место будет заполнено данными файлов.

Чтобы способствовать предотвращению фрагментации таблицы MFT в некоторых случаях, рекомендуется зарезервировать для нее при преобразовании раздела в NTFS больше места, чем выделяемые по умолчанию 12,5% от общего размера раздела или тома. Например, желательно увеличить объем места для таблицы MFT в том случае, если раздел будет использоваться для хранения большого числа файлов небольшого или среднего размера, а не несколько больших файлов. Задать требуемый для резервирования объем можно с помощью утилиты FSUtil, создав файл-заглушку размером, равным объему, который требуется зарезервировать для таблицы MFT. Имя этого файла-заглушки затем указывается в параметре `/CvtArea` утилиты Convert.

В следующем примере создается файл-заглушка temp.txt размером в 1,5 Гбайт:

```
fsutil file createnew c:\temp.txt 1500000000
```

А здесь этот файл используется для резервирования места для таблицы MFT при преобразовании диска `C:` в NTFS:

```
convert c: /fs:ntfs /cvtarea:temp.txt
```

Обратите внимание, что файл-заглушка создается в разделе или томе, который нужно преобразовать в NTFS. В процессе преобразования занимаемое файлом место записывается метаданными NTFS, а оставшееся место резервируется для будущего использования таблицей MFT.

Восстановление простого, составного или чередующегося тома

Диагностирование и восстановление основных разделов и простых томов является довольно легкой задачей, т. к. имеется дело всего лишь с одним физическим диском. С другой стороны, составные и чередующиеся тома могут состоять из нескольких дисков. В случае чередующихся томов, с которыми не применяется контроль по четности, выход из строя одного диска выводит из строя весь том. Состояние неработоспособного диска может указываться как **Отсутствует** (Missing), **Неудачно** (Failed), **В сети (ошибки)** (Online (Erorrs)), **Вне сети** (Offline) или **Не читается** (Unreadable).

Состояние **Отсутствует** (и иногда **Вне сети**) отображается для отключенных приводов или приводов с выключенным питанием. Если приводы входят в состав внешнего устройства хранения, проверьте, что это устройство запитано надлежащим образом. Переподключение устройства или включение питания должно сделать привод доступным. После этого в средстве **Управление дисками** необходимо выполнить повторное сканирование, чтобы обновить состояние проблемного привода. Для этого щелкните на значке требуемого привода правой кнопкой мыши и в контекстном меню выберите команду **Повторить проверку дисков**. По завершению сканирования щелкните на значке привода правой кнопкой мыши и в контекстном меню выберите команду **Активировать повторно** (Reactivate).

Состояние **Отказавший**, **В сети (ошибки)** или **Не читается** отображается для дисков, испытывающих проблемы ввода-вывода. Как и ранее, попытайтесь выполнить повторное сканирование для обнаружения диска, а затем выполнить повторную активацию. Если привод не возвратится в состояние **Исправен**, может потребоваться заменить его.

Совет

Иногда, чтобы возвратить диск в состояние **В сети**, может потребоваться перезагрузить компьютер. Если и это не решает проблему, проверьте исправность диска, его контроллера и кабелей подключения. Также проверьте правильность подключения привода и наличие на нем питания.

Регенерация чередующегося тома с контролем по четности

В случае сбоя одного диска тома RAID-5 (т. е. чередующегося тома с контролем по четности), том можно восстановить по данным, содержащимся на его других дисках. Состояние вышедшего из строя диска набора RAID-5 обозначается как **Отсутствует**, **Вне сети** или **В сети (ошибки)**, а всего тома как **Отказавшая избыточность** (Failed Redundancy).

Диски RAID-5 поддаются восстановлению, но только в том случае, если все диски набора одного типа — или MBR или GPT. Для восстановления все диски набора RAID-5 должны быть возвращены в состояние **В сети**. Состояние набора с проблемным приводом должно отображаться как **Отказавшая избыточность**. Корректирующее действие зависит от состояния проблемного привода.

- Если состояние отображается как **Отсутствует** или **Вне сети**, проверьте, что на привод подается питание и он подключен должным образом. Затем откройте средство **Управление дисками**, щелкните правой кнопкой мыши по значку неисправного тома и в контекстном меню выберите команду **Реактивировать том** (Reactivate Volume). Состояние диска должно изменяться на **Регенерация** (Regenerating), а затем на **Исправен** (Healthy). Если статус привода не возвращается в **Исправен**, щелкните на значке тома правой кнопкой мыши и в контекстном меню выберите команду **Восстановить четность** (Regenerate Parity).
- Если статус привода отображается как **В сети (ошибки)**, щелкните правой кнопкой мыши на значке проблемного тома и в контекстном меню выберите команду **Реактивировать том**. Состояние диска должно измениться на **Регенерация**, а затем на **Исправен**. Если статус привода не возвращается в **Исправен**, щелкните на значке тома правой кнопкой мыши и в контекстном меню выберите команду **Восстановить четность**.
- Если состояние проблемного привода отображается как **Не читается**, может потребоваться повторить сканирование приводов системы, выбрав в меню **Действие** средства **Управление дисками** команду **Повторить проверку дисков**. Если состояние привода не меняется, попробуйте перезагрузить компьютер.
- Если привод не возвращается в состояние **В сети**, нужно исправить поврежденную область набора RAID-5. В средстве **Управление дисками** щелкните правой кнопкой мыши на значке неисправного тома и в контекстном меню выберите команду **Удалить том** (Remove Volume). Далее для набора RAID-5 нужно выбрать нераспределенное пространство на отдельном динамическом диске. Размер этого пространства должен быть, по крайней мере, равным размеру восстанавливаемой области, и пространство должно находиться на приводе, не входящем в число уже используемых приводов набора RAID-5. В случае недостаточного свободного дискового пространства команда **Восстановить том** (Repair Volume) будет недоступна, и нужно будет освободить место, удалив другие тома, или же заменить проблемный привод.

Рекомендации

Если возможно, перед выполнением процедуры восстановления следует создать резервную копию данных. Таким образом, в случае проблем с восстановлением, данные не будут утеряны.

Зеркалирование дисков

Зеркалирование дисков заключается в создании набора избыточных данных с использованием двух томов одинакового размера на отдельных приводах. Информация записывается одновременно на оба тома, и в случае сбоя одного из дисков будет доступна на другом.

Хотя зеркалирование дисков обеспечивает отказоустойчивость, его основным недостатком является нерациональное использование дискового пространства, т. к. из всего доступного пространства практически используется только половина. Например, чтобы создать зеркальный том размером в 500 Гбайт, требуются два привода, каждый размером в 500 Гбайт. Таким образом, для хранения 500 Гбайт информации используется 1000 Гбайт дискового пространства.

Создание зеркальных томов

Зеркальный том можно создать таким образом:

1. В виде **Графическое представление** средства **Управление дисками** щелкните правой кнопкой мыши на нераспределенном пространстве диска и в контекстном меню выберите команду **Создать зеркальный том** (New Mirrored Volume). Запустится мастер создания зеркального тома. Ознакомьтесь с инструкциями на странице приветствия мастера и нажмите кнопку **Далее**.
2. Создайте том, следуя инструкциям, изложенным в *разд. "Создание составных и чередующихся томов" ранее в этой главе*. Основная разница состоит в том, что в данном случае создается два тома одинакового размера, которые должны находиться на разных дисках. Поэтому, пока в поле **Выбраны** не будут добавлены два диска, перейти к следующему шагу будет невозможно.
3. Подобно другим методам RAID, зеркалирование прозрачно для пользователей. В Проводнике Windows пользователи видят зеркальный том, как один диск, к которому они могут обращаться и использовать, как любой другой диск.

> ***Примечание***
>
> Статус нормального зеркального тома отображается как **Исправен**. В процессе создания зеркального тома его состояние отображается как **Ресинхронизация** (Resynching), что служит индикатором создания зеркального тома.

Вместо создания нового зеркального тома с нуля можно к существующему простому тому добавить в качестве зеркала другой том, создав таким образом зеркальный том. Для этого исходный том должен быть основным разделом или простым томом, а добавляемый привод иметь нераспределенное пространство, равное или большее, чем размер первого тома.

Чтобы добавить зеркало к существующему простому тому, выполните следующие шаги:

1. Щелкните правой кнопкой мыши на значке основного раздела или простого тома, к которому требуется добавить зеркало, и в контекстном меню выберите команду **Добавить зеркало** (Add Mirror).
2. В списке **Диски** открывшегося диалогового окна **Добавить зеркальный том** (Add Mirror) выберите диск, который нужно добавить, а затем нажмите кнопку **Добавить зеркальный том**. Будет запущен процесс создания зеркального тома. В средстве **Управление дисками** состояние обоих дисков создаваемого зеркального тома отображается как **Ресинхронизация**. Добавляемый диск отмечается значком желтого треугольника с восклицательным знаком.

Разделение зеркального тома

Иногда может потребоваться разделить зеркальный том на составляющие его простые тома. Например, может возникнуть срочная надобность в дисковом пространстве, одним из способов удовлетворения которой будет временно одолжить один из дисков зеркального тома.

Также, если один из дисков зеркального тома выйдет из строя, том будет работать, но рано или поздно зеркальность нужно будет восстанавливать, для чего зеркальный том нужно разбить на составляющие, а затем восстановить его. Хотя разделение зеркального тома не удаляет данные набора, прежде чем выполнять эту процедуру, всегда следует создать резервную копию данных тома. Таким образом, в случае возможных проблем данные не будут утеряны.

Чтобы разделить зеркальный том, выполните следующие шаги:

1. В средстве **Управление дисками** щелкните правой кнопкой мыши по значку одного из дисков зеркального тома и в контекстном меню выберите команду **Разделить зеркальный том** (Break Mirrored Volume).
2. В окне запроса подтвердите свое намерение разбить зеркальный том, нажав кнопку **Да**. Если том используется, выводится соответствующее предупреждение. Также нажмите кнопку **Да** в этом окне предупреждения, чтобы продолжить разделение зеркального тома.

   После этого Windows 8 разделит зеркальный том, создав два независимых диска. (При удалении одного из дисков зеркального тома разделять том не требуется, т. к. Windows выполняет разделение, как часть процесса удаления диска.)

Удаление диска из зеркального тома

Один из дисков зеркального тома можно удалить из набора. Выполнение этой операции удаляет все данные на удаляемом диске и помечает используемое им пространство как нераспределенное.

Удалить один из дисков зеркального набора можно таким образом:

1. В средстве **Управление дисками** щелкните правой кнопкой мыши на значке одного из дисков зеркального тома и в контекстном меню выберите команду **Удалить зеркало** (Remove Mirror).
2. В списке **Диски** открывшегося диалогового окна **Удалить зеркало** выберите диск, который нужно удалить из зеркального тома.
3. Подтвердите свое намерение удалить диск в окне предупреждения, нажав кнопку **Да**. Зеркало будет удалено со всеми хранящимися на нем данными.

Перенос динамического диска на новую систему

Важным достоинством динамических дисков является возможность с легкостью перемещать их с одного компьютера на другой. Например, после настройки системы на одном компьютере может оказаться, что один из жестких дисков будет лучше использован на другом компьютере. Но прежде чем перемещать диски, нужно выполнить следующее:

1. Откройте консоль средства **Управление дисками** на компьютере, где находятся диски, подлежащие перемещению, и проверьте, что их состояние отображается как **Исправен**. В противном случае, прежде чем перемещать диски, нужно исправить все проблемы с ними.

   Осторожно!

   Рассматриваемый метод нельзя применять для перемещения дисков, на которых используется шифрование BitLocker. Версии Windows 8 Enterprise и Ultimate предоставляют функциональность

шифрования дисков BitLocker, которая помещает приводы в защищенную оболочку, в результате чего при попытке получения доступа к содержимому снятого с компьютера диска доступ к данным диска блокируется. Эту блокировку может снять только администратор компьютера. Дополнительную информацию по вопросу функциональности шифрования дисков BitLocker *см. в главе 11*.

2. Проверьте подсистемы жестких дисков на исходном компьютере и на компьютере назначения. Эти подсистемы должны быть одинаковыми на обоих компьютерах. В противном случае код Plug and Play на системном диске с исходного компьютера будет отличаться от кода, ожидаемого компьютером назначения. В результате компьютер назначения не сможет загрузить правильные драйверы и загрузка может завершиться сбоем.
3. Проверьте, не являются ли перемещаемые динамические диски частью составного или чередующегося тома. Если являются, то нужно запомнить, какие диски входят в состав какого тома, и планировать перемещение всех дисков набора тома. Если переместить только часть дисков набора, нужно знать, каковы будут последствия этого действия. В случае составных или чередующихся томов перемещение только части набора делает связанные диски недоступными как на исходном компьютере, так и на компьютере назначения.

Когда все будет готово для перемещения дисков, выполните следующие шаги:

1. На исходном компьютере откройте консоль **Управление компьютером**. В левой панели консоли щелкните по ссылке **Диспетчер устройств**. В списке устройств в панели сведений разверните узел **Дисковые устройства** (Disk Drives). Этот узел содержит список всех физических приводов жестких дисков, установленных на компьютере. Щелкните правой кнопкой мыши на каждом диске, который требуется переместить, и в контекстном меню выберите команду **Удалить** (Uninstall). В случае проблем с определением, какие диски подлежат перемещению, щелкните на каждом диске правой кнопкой мыши и в контекстном меню выберите команду **Свойства**. В диалоговом окне свойств выберите вкладку **Тома** и нажмите на ней кнопку **Заполнить**. В панели **Тома** отобразятся тома данного диска.
2. Выполнив эти процедуры, можно перемещать динамические диски. Если диски поддерживают "горячую" замену и эта возможность поддерживается на обоих компьютерах, снимите диски с исходного компьютера и установите их на компьютер назначения. В противном случае выключите оба компьютера, а уже затем снимите диски с исходного компьютера и установите их на компьютер назначения. Установив диски, снова запустите оба компьютера.
3. На компьютере назначения откройте средство **Управление дисками** и в меню **Действие** выберите опцию **Повторить проверку дисков**. По завершению сканирования дисков щелкните правой кнопкой мыши по значку диска, обозначенного **Инородный** (Foreign), и в контекстном меню выберите команду **Импортировать** (Import). Выполните эту операцию для всех перемещенных дисков. Теперь эти диски и их тома будут доступны на компьютере назначения.

Примечание

Буквы томов динамических дисков, перенесенных на другой компьютер, должны оставаться теми же, какими они были на исходном компьютере. Если на компьютере назначения буква перенесенного диска уже используется, ему присваивается следующая свободная буква. Если перенесенный динамический том не имел буквы на исходном компьютере, после переноса буква ему также не присваивается. Кроме этого, если автоматическое подключение дисков отключено, после переноса дисков их нужно подключить и присвоить буквы вручную.

Диагностирование общих проблем с дисками

Операционная система Windows 8 интенсивно использует приводы жестких дисков как при запуске компьютера, так и в процессе его штатной работы. Производительность операционной системы и приложений можно значительно повысить, оптимизировав жесткие диски компьютера. Для оптимизации диска следует уделить особое внимание использованию дискового пространства, ошибкам диска и фрагментации диска. Также желательно включить сжатие данных, чтобы уменьшить занимаемое файлами данных пространство и освободить дополнительное пространство для хранения данных.

> ***Примечание***
>
> Средства обслуживания дисков, такие как **Очистка диска** (Disk Cleanup), **Проверка диска** (Check Disk) и **Дефрагментация диска** (Disk Defragmenter), используют возможности назначения приоритетов ресурсам, предоставляемые в Windows 8, как рассматривается в *разд. "Windows SuperFetch" ранее в этой главе*. Это позволяет данным инструментам исполняться в фоновом режиме, используя время простоя системы. В результате производительность пользовательских процессов постоянно находится на хорошем уровне даже при выполняющихся заданиях обслуживания.

Нужно всегда внимательно следить за использованием пространства на всех дисках системы. Когда диски начинают заполняться, их производительность и производительность операционной системы в целом может понижаться, особенно при нехватке дискового пространства для хранения виртуальной памяти или временных файлов. Один из способов освободить дисковое пространство — это удалить ненужные файлы и сжать старые файлы с помощью утилиты **Очистка диска**. Инструкции по использованию этой утилиты *см. в разд. "Использование утилиты Очистка диска" главы 2*. Вместо того чтобы постоянно напоминать пользователям использовать утилиту очистки диска, можно запланировать регулярное автоматическое выполнение этой утилиты, как рассматривается в *разд. "Планирование задач обслуживания" главы 10*.

С помощью утилиты **Управление дисками** можно определить состояние дисков и их разделов или томов. Состояние диска отображается в виде **Графическое представление** внизу под номером диска в значке диска и в виде **Список дисков** в столбце **Состояние**. Состояние разделов или томов диска отображается в виде **Графическое представление** справа от значка содержащего их диска и в столбце **Состояние** вида **Список томов**.

В табл. 12.2 приведен список сообщений состояния дисков и соответствующие описания и рекомендуемые действия по устранению неполадок.

Таблица 12.2. *Сообщения состояния дисков, их значения и рекомендуемые действия по решению проблем*

Состояние	Описание	Решение
В сети (Online)	Нормальное состояние диска. Диск не имеет никаких проблем и к нему есть доступ	Диск не имеет никаких известных проблем. Не требуется предпринимать никаких корректирующих действий
В сети (ошибки) (Online (Errors))	На диске обнаружены ошибки ввода-вывода	Временные ошибки можно попытаться исправить, щелкнув по значку диска правой кнопкой мыши и выбрав в контекстном меню команду **Реактивировать диск** (Reactivate Disk). Если это не даст результата, возможно, что диск поврежден физически, и может потребоваться выполнить всестороннюю проверку диска

Таблица 12.2 *(окончание)*

Состояние	Описание	Решение
Вне сети (Offline)	Диск недоступен и, возможно, поврежден. Если состояние диска меняется на **Отсутствует** (Missing), это означает, что система не может найти или определить его	Проверьте диск, его контроллер и кабели на наличие проблем. Также проверьте правильность подключения привода и наличие на нем питания. Попытайтесь "реанимировать" диск, выполнив команду **Реактивировать диск**
Инородный (Foreign)	Диск был перенесен с другого компьютера, но еще не был импортирован. Возвращенный в действие проблемный диск может иногда обозначаться как **Инородный**	Щелкните на значке диска правой кнопкой мыши и в контекстном меню выберите команду **Импорт чужих дисков** (Import foreign disks), чтобы добавить диск в систему
Не читается (Unreadable)	Диск недоступен в настоящее время, что может случиться в процессе сканирования системы на наличие дисков	Это состояние может отображаться для устройств чтения карт памяти FireWire или USB в случае неотформатированной или неправильно отформатированной карты. Также этот статус может отображаться при извлеченной из устройства чтения карты. В иных случаях диск может быть поврежден или иметь ошибки ввода-вывода. Выполните команду **Повторить проверку дисков** из меню **Действие**, чтобы попытаться исправить проблему. Можно также попробовать перезагрузить систему
Неопознан (Unrecognized)	Диск неизвестного типа и не может использоваться в системе. Этот статус может отображаться для диска системы, отличной от Windows	Если диск из другой операционной системы, не предпринимайте никаких корректирующих действий. Использовать этот диск на компьютере не получится
Не проинициализирован (Not Initialized)	Диск не имеет действительной подписи. Этот статус может отображаться для диска иной системы, чем Windows	Если диск из другой операционной системы, не предпринимайте никаких корректирующих действий. Использовать этот диск на компьютере не получится. В ином случае щелкните по значку диска правой кнопкой мыши и в контекстном меню выберите команду **Инициализировать диск** (Initialize Disk)
Нет носителя (No Media)	В приводе CD/DVD или другом приводе со съемным носителем отсутствует носитель. Это состояние отображается только для приводов CD/DVD или других приводов со съемным носителем	Вставьте носитель в привод. В случае устройств чтения карт памяти FireWire или USB этот статус обычно, но не всегда, отображается при отсутствии в устройстве карточки

В табл. 12.3 представлен список сообщений состояния томов, соответствующие описания и рекомендуемые действия по устранению неполадок.

Таблица 12.3. *Сообщения состояния томов, их значения и рекомендуемые действия по решению проблем*

Состояние	Описание	Решение
Неполные данные (Data incomplete)	Отсутствует один или несколько дисков составного тома на дисках, перенесенных с другого компьютера	Возможно, вы забыли добавить один из дисков составного тома при переносе его на другой компьютер. Добавьте недостающий диск или диски, а затем одновременно импортируйте все диски
Нет избыточности данных (Data not redundant)	Отсутствует один из дисков зеркального тома, перенесенного с другого компьютера	Возможно, вы забыли добавить один из дисков зеркального тома при переносе его на другой компьютер. Добавьте недостающий диск, а затем одновременно импортируйте все диски
Неудачно (Failed)	Ошибка диска. Диск недоступен или поврежден	Проверьте, что связанный диск подключен, и, если необходимо, щелкните по значку диска правой кнопкой мыши и в контекстном меню выберите команду **Реактивировать диск**. Щелкните на значке тома правой кнопкой мыши и в контекстном меню выберите команду **Реактивировать том**. Также рекомендуется проверить исправность физического подключения диска
Отказавшая избыточность (Failed Redundancy)	Не синхронизированы диски зеркального тома или тома RAID-5	Можно попытаться выполнить синхронизацию дисков, щелкнув по значку проблемного тома правой кнопкой мыши и выполнив команду контекстного меню **Реактивировать том**
Форматирование (Formatting)	Временное состояние при форматировании тома	Ход процесса форматирования отображается выводом процента завершения (если не была выбрана опция быстрого форматирования)
Исправен (Healthy)	Нормальный статус полностью работоспособного тома	Никаких известных проблем с томом не обнаружено. Соответственно, предпринимать каких-либо корректирующих действий не требуется
Исправен (Под угрозой) (Healthy (At Risk))	Система испытывает проблемы с чтением или записью физического диска, на котором расположен том. Это состояние обычно отображается при обнаружении ошибок операционной системой	Щелкните по значку связанного диска правой кнопкой мыши и в контекстном меню выберите команду **Реактивировать диск**. Если это не исправит проблему или это состояние отображается периодически, возможно, что диск разрушается. В таком случае следует создать резервную копию всех данных на диске
Исправен (Неизвестный раздел) (Healthy (Unknown Partition))	Windows не может определить раздел. Это состояние может отображаться для разделов, созданных в другой операционной системе, или для разделов производителя компьютера, используемых для хранения системных файлов	Никаких корректирующих действий предпринимать не требуется
Инициализация (Initializing)	Временное состояние при инициализации диска	Состояние диска должно измениться в течение короткого времени (обычно нескольких секунд)

Таблица 12.3 *(окончание)*

Состояние	Описание	Решение
Ресинхронизация (Resynching)	Временное состояние при ресинхронизации зеркального набора	Ход процесса указывается процентом завершения операции. После завершения инициализации состояние тома должно возвратиться в **Исправен**
Устаревшие данные (Stale Data)	Данные на отказоустойчивых инородных дисках не синхронизированы	Повторите сканирование дисков компьютера и снова проверьте статус. Теперь должен отображаться новый статус, например, **Отказавшая избыточность**
Неизвестно (Unknown)	Нет доступа к тому. Возможной причиной может быть поврежденный загрузочный сектор	Том может быть инфицирован вирусом загрузочного сектора. Проверьте том, используя антивирусную программу с актуальными базами данных. Если вирусы не обнаружены, загрузите компьютер с установочного диска Windows 8 и исправьте главную загрузочную запись, используя команду консоли восстановления fixmbr

Исправление ошибок и искажений данных дисков

Операционная система Windows 8 содержит усовершенствования, которые позволяют сократить объем ручного обслуживания дисков. Наиболее важными из этих усовершенствований являются следующие:

- транзакционная NTFS;
- самовосстанавливающаяся NTFS.

Транзакционная NTFS (transactional NTFS) позволяет выполнять файловые операции на томе NTFS в транзакционном режиме. Это означает, что программы могут сгруппировать в транзакцию наборы операций с файлами или реестром, чтобы обеспечить успешное выполнение их всех, а в случае неудачного выполнения одной из них — невыполнение их всех. В процессе выполнения транзакции осуществляемые в ней изменения невидимы вне транзакции. Изменения фиксируются и записываются на диск в полном составе только в случае успешного завершения транзакции. В случае неуспешного или неполного выполнения транзакции происходит откат всех выполненных в ней изменений, чтобы восстановить файловую систему к состоянию, в котором она находилась до начала транзакции.

Координация транзакций, которые охватывают несколько томов, выполняется диспетчером KTM[1]. Диспетчер KTM поддерживает независимое восстановление томов в случае сбоя транзакции. Локальный диспетчер ресурсов тома содержит отдельный журнал транзакций и отвечает за разделение потоков транзакций и потоков, выполняющих файловые операции.

При традиционном подходе для исправления ошибок и искажений томов NTFS диска используется средство **Проверка диска**. Так как использование этой программы может ограничить доступность операционной системы, в Windows 8 применяется самовосстанавливающаяся NTFS, чтобы обеспечить целостность файловой системы, не прибегая к использованию отдельных инструментов технической поддержки для исправления проблем. Большая часть процесса самовосстановления включается и выполняется автоматически, вследствие чего выполнять ручные работы по обслуживанию томов может потребоваться

[1] Kernel Transaction Manager — диспетчер транзакций ядра.

только тогда, когда операционная система не может справиться с этим самостоятельно. В таких случаях Windows 8 выдает соответствующее уведомление о проблеме, также предоставляя возможные решения по ее устранению.

Самовосстанавливающаяся NTFS обладает многими преимуществами над использованием утилиты **Проверка диска**, включая следующие.

- Утилите **Проверка диска** требуется исключительный доступ к томам. Это означает, что системный и загрузочный тома можно проверить только при загрузке операционной системы. В отличие от этой утилиты, при использовании самовосстанавливающейся NTFS файловая система всегда остается доступной, и (в большинстве случаев) для выполнения исправлений ее не требуется выводить из рабочего режима.
- В случае искажений тома самовосстанавливающаяся NTFS пытается сохранить как можно больший объем данных и уменьшает количество неуспешных запросов подключения файловой системы, которые были возможны с предыдущими версиями Windows, если в томе были ошибки или искажения. При перезапуске самовосстанавливающаяся NTFS сразу же выполняет исправление тома, чтобы его можно было подключить.
- Самовосстанавливающаяся NTFS извещает об изменениях, выполненных в томе в процессе исправления, посредством существующих механизмов утилиты chkdsk.exe, уведомлений каталогов и записей в журнале USN. Эта возможность также позволяет санкционированным пользователям отслеживать операции исправления посредством сообщений `Verification`, `Waiting For Repair Completion` и `Progress Status`.
- Самовосстанавливающаяся NTFS может восстановить том, если загрузочный сектор читается, но не определяется, как том NTFS. В таком случае необходимо отключить том и исправить загрузочный сектор, используя соответствующий инструмент, после чего предоставить самовосстанавливающейся NTFS начать процесс восстановления.

Хотя самовосстанавливающаяся NTFS является замечательнейшим усовершенствованием, иногда желательно проверить целостность диска вручную. В таких случаях проверку и при необходимости исправление проблем томов FAT, FAT32, exFAT и NTFS можно выполнить с помощью утилиты **Проверка диска** (исполняемый файл chkdsk.exe). Хотя эта утилита способна проверить наличие и исправить многие типы ошибок, она в основном выполняет поиск искажений в файловой системе и ее связанных метаданных. Для проблем иного типа полезность утилиты **Проверка диска** довольно ограничена.

Проверка диска на наличие ошибок

Как часть автоматического обслуживания, Windows 8 выполняет профилактическое сканирование томов NTFS компьютера. Подобно другим задачам автоматического обслуживания, сканирование выполняется в 3:00 посредством утилиты **Проверка диска** при условии, что компьютер простаивает и работает от сети. При других обстоятельствах сканирование дисков запускается при следующей работе компьютера от сети и простаивающей операционной системе. Это расписание можно исправить, изменив время запуска автоматического обслуживания *(см. разд. "Настройка автоматической справки и поддержки" главы 9)*. Хотя запуск автоматического обслуживания активирует сканирование дисков, процесс вызова и управления утилитой **Проверка диска** обрабатывается отдельным заданием. В библиотеке планировщика заданий это задание, называющееся **ProactiveScan**, находится в узле **Microsoft\Windows\Chkdsk**; подробные сведения о выполнении этого задания можно просмотреть на его вкладке **Журнал** (History).

Проверку целостности дисков с помощью утилиты **Проверка диска** также можно периодически выполнять вручную. Утилита **Проверка диска** может обнаруживать и исправлять

различные распространенные ошибки на дисках FAT16, FAT32, exFAT и NTFS. Одним из способов, используемых утилитой для обнаружения ошибок, является сравнение битовой карты тома с секторами диска, выделенными файлам в файловой системе. Но утилита не может исправить искаженные данные в файлах, структура которых выглядит неповрежденной. Утилиту **Проверка диска** можно запустить в командной строке или с помощью графического интерфейса.

В Windows 8 утилита **Проверка диска** автоматически выполняет усовершенствованное сканирование и исправление, вместо старого варианта сканирования, используемого в предыдущих версиях Windows. Теперь утилита выполняет проверку томов NTFS на наличие ошибок, не отключая их. Информацию об обнаруженных искажениях утилита записывает в системный файл $corrupt. Если данный том в настоящее время используется, обнаруженные ошибки можно исправить, временно отключив том. Но отключение тома для выполнения исправлений делает недействительными все открытые дескрипторы файлов. Поэтому исправления загрузочного или системного томов выполняется при следующем запуске компьютера.

Сохранение информации об ошибках позволяет Windows оперативно исправлять тома, пока они находятся в отключенном состоянии, а также разрешает использовать диск при его сканировании. Обычно исправление отключенного диска занимает всего лишь несколько секунд по сравнению с несколькими часами, требующимися для исправления томов очень большого размера с использованием старых методов сканирования и исправления.

Но расширенные возможности сканирования и исправления не поддерживаются томами FAT, FAT32 и exFAT. При проверке таких томов посредством утилиты **Проверка диска** Windows 8 использует старую версию сканирования и исправления. Это обычно означает необходимость отключения тома и невозможность его использования, пока выполняется сканирование и исправление.

Выполнение утилиты *Проверка диска* из командной строки

Утилиту **Проверка диска** можно выполнять в консоли командной строки, запущенной от имени администратора, или из других инструментов. Запуск утилиты с командной строки выполняется таким образом:

```
chkdsk /scan C:
```

Утилита выполняет проверку диска и возвращает сообщение о результатах проверки. Но если при запуске не указаны другие параметры, утилита не исправляет обнаруженные ошибки. Чтобы исправить ошибки, например, на диске `C:`, утилиту нужно запустить следующим образом:

```
chkdsk /spotfix C:
```

Для исправления ошибок утилите требуется исключительный доступ к тому. Каким образом этот доступ предоставляется, зависит от типа тома.

- Для несистемного тома выводится запрос выполнить принудительное отключение тома. Чтобы отключить том и начать процесс исправления, введите `Y`; в противном случае введите `N`, чтобы отменить отключение. Если отменить отключение, выводится другой запрос: надо ли запланировать исправление тома при следующем запуске компьютера? Опять, чтобы запланировать исправление, введите `Y`, а для отмены введите `N`.
- Для системных томов выводится только второй запрос: надо ли запланировать исправление тома при следующем запуске компьютера? В таком случае, чтобы запланировать исправление, введите `Y`, а для отмены введите `N`.

Утилиту **Проверка диска** нельзя запустить одновременно с параметрами `/scan` и `/spotfix`, т. к. задания сканирования и исправления теперь являются отдельными заданиями.

Полный синтаксис команды запуска утилиты **Проверка диска** выглядит так:

```
CHKDSK [том[[путь]имя_файла]] [/F] [/V] [/R] [/X] [/I] [/C] [/B]
  [/L[:size]] [/scan] [/forceofflinefix] [/perf] [/spotfix]
  [/sdcleanup] [/offlinescanandfix]
```

Параметры и переключатели команды имеют следующее значение:

- *том* — задает том, с которым нужно работать;
- *путь*/*имя_файла* — задает файлы, которые следует проверить на фрагментацию (только для томов FAT);
- `/B` — задает повторную проверку поврежденных кластеров тома (только для томов NTFS; подразумевает переключатель `/R`);
- `/C` — задает пропуск проверки циклов в структуре папок (только для томов NTFS);
- `/F` — задает исправление ошибок диска, используя старый метод — сканирование и исправление ошибок на отключенном диске;
- `/I` — задает минимальную проверку записей индекса (только для томов NTFS);
- `/L:`*size* — задает размер файла журнала (только для томов NTFS);
- `/R` — задает определение поврежденных секторов и восстановление читаемой информации (подразумевает переключатель `/F`);
- `/V` — задает вывод полного пути и имени каждого файла проверяемого тома (только для томов FAT), а также вывод сообщений об очистке (только для томов NTFS);
- `/X` — задает принудительное отключение тома, если необходимо (подразумевает переключатель `/F`).

Управлять расширенными возможностями утилиты **Проверка диска** в Windows 8 для томов NTFS можно с помощью следующих опций:

- `/forceofflinefix` — должна использоваться с опцией `/scan`. Задает пропуск выполнения исправлений на подключенном диске и составляет список ошибок для исправления на отключенном диске;
- `/scan` — задает сканирование подключенного тома; это режим работы по умолчанию. Обнаруженные в процессе сканирования ошибки записываются в системный файл $corrupt;
- `/perf` — задает максимальную скорость сканирования, используя дополнительные системные ресурсы;
- `/spotfix` — разрешает исправление определенных типов ошибок на подключенном диске (режим работы по умолчанию);
- `/sdcleanup` — задает удаление ненужных данных дескрипторов безопасности. Подразумевает переключатель `/F` (для сканирования и исправления старого типа);
- `/offlinescanandfix` — задает сканирование и исправление ошибок на отключенном томе.

Интерактивное выполнение утилиты *Проверка диска*

С утилитой **Проверка диска** можно также работать в интерактивном режиме из консоли **Управление компьютером**. В частности, проверка дисков на локальном компьютере выполняется следующим образом:

1. В консоли **Управление компьютером** разверните узел **Запоминающие устройства** и выберите в нем узел **Управление дисками**. В виде **Список томов** или **Графическое представление** щелкните правой кнопкой мыши по значку любого диска и в контекстном меню выберите команду **Свойства**.
2. На вкладке **Сервис** (Tools) окна свойств нажмите кнопку **Проверить** (Check). Откроется диалоговое окно **Проверка ошибок** (рис. 12.12). Для томов NTFS это окно содержит ссылку **Проверить диск** (Scan drive), а для томов FAT — ссылку **Проверить и восстановить диск** (Scan and repair drive).

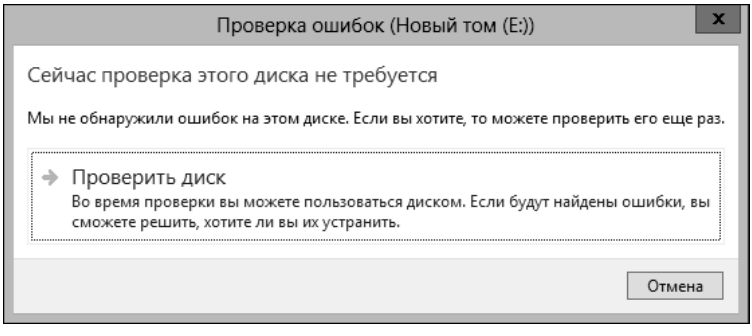


Рис. 12.12. Диалоговое окно для проверки дисков

3. Щелкните по соответствующей ссылке, чтобы запустить процесс проверки диска. Если Windows не обнаружит ошибок на диске, появится соответствующее сообщение. Если же проверка обнаружит ошибки, предоставляются дополнительные опции. Как и при работе с утилитой из командной строки, эти опции зависят от типа проверяемого тома (системный или несистемный) и его файловой системы (NTFS или FAT).

Дефрагментация дисков

При любом добавлении или удалении файлов с диска данные на диске могут фрагментироваться. Когда происходит фрагментация диска, файлы большого размера нельзя записать в один блок последовательных кластеров диска. В результате этого операционная система вынуждена записывать файлы в несколько блоков кластеров меньшего размера, размещенных в разных частях диска. Считывание таких файлов с диска занимает больше времени, чем файлов, записанных в один непрерывный блок кластеров. Чтобы понизить объем фрагментации, Windows 8 автоматически выполняет дефрагментацию диска, как часть автоматического обслуживания. Подобно проверке диска на ошибки, процесс вызова и управления оптимизацией диска осуществляется отдельным заданием. В библиотеке планировщика заданий это задание, называющееся **Scheduled Defrag**, находится в узле **Microsoft\Windows\Defrag**; подробные сведения о выполнении этого задания можно просмотреть на его вкладке **Журнал**.

Автоматический анализ и оптимизация дисков может выполняться на подключенных дисках при условии, что компьютер работает от сети и операционная система простаивает. По умолчанию оптимизация дисков происходит еженедельно, а не каждый день. Обычно оптимизацию дисков компьютера требуется выполнять только периодически, и раз в неделю будет достаточно в большинстве случаев. Но обратите внимание на то, что анализ и оптимизация несистемных дисков выполняется быстро, а оптимизация подключенных системных дисков может занять значительно больше времени. В результате этого на некоторых

компьютерах анализ и оптимизация системных томов очень больших объемов может быть выполнена не полностью, особенно если компьютер выключен, когда должно выполняться обслуживание, и активно используется, когда включен.

Дефрагментацию диска можно выполнить вручную следующим образом:

1. В консоли **Управление компьютером** разверните узел **Запоминающие устройства** и выберите в нем узел **Управление дисками**. Щелкните правой кнопкой мыши по значку любого диска и в контекстном меню выберите команду **Свойства**.
2. На вкладке **Сервис** окна свойств нажмите кнопку **Оптимизировать** (Optimize). В открывшемся диалоговом окне **Оптимизация дисков** (Optimize Drives) щелкните правой кнопкой мыши по требуемому диску и в контекстном меню выберите команду **Анализировать**. Средство оптимизации дисков проанализирует диск на необходимость дефрагментации. Если будет обнаружено, что диск нужно дефрагментировать, рекомендуется выполнить эту операцию.
3. В столбце **Текущее состояние** (Current Status) отображается состояние каждого диска и процент его фрагментации при последней проверке. Чтобы оптимизировать диск, выберите его в списке и нажмите кнопку **Оптимизировать**.

> ***Примечание***
>
> В зависимости от размера диска дефрагментация может занять несколько часов. Но этот процесс можно остановить в любой момент, нажав кнопку **Стоп**.

Хотя в предыдущих версиях Windows оптимизацию можно было выполнять в конкретное время определенного дня, Windows 8 делает это в рамках автоматизированного обслуживания. По умолчанию анализ дисков (и оптимизация, если необходимо) выполняется приблизительно раз в неделю. Можно задать приблизительное время запуска процедуры анализа и оптимизации, установив время запуска автоматического обслуживания. Кроме этого, если задание анализа и оптимизации пропущено три раза подряд, Windows 8 выводит соответствующее уведомление. Оптимизация всех внутренних и некоторых внешних приводов жестких дисков выполняется автоматически по регулярному расписанию и при подключении к компьютеру новых дисков.

Настройка и управление выполнением автоматизированной дефрагментации осуществляется следующим образом:

1. В консоли **Управление компьютером** разверните узел **Запоминающие устройства** и выберите в нем узел **Управление дисками**. Щелкните правой кнопкой мыши по значку какого-либо диска и в контекстном меню выберите команду **Свойства**.

   На вкладке **Сервис** окна свойств нажмите кнопку **Оптимизировать**. Откроется диалоговое окно **Оптимизация дисков** (рис. 12.13).
2. Чтобы изменить настройки оптимизации, нажмите кнопку **Изменить параметры** (Change settings). Откроется диалоговое окно **Оптимизация дисков** (Optimize Drives) (рис. 12.14). Чтобы отменить автоматическое выполнение дефрагментации, снимите флажок **Выполнять по расписанию** (Run on a schedule), а чтобы включить — установите его.
3. По умолчанию в раскрывающемся списке **Периодичность** задано еженедельное автоматическое выполнение анализа и, если необходимо, оптимизации дисков. Вместо этого можно задать другое расписание — ежедневно или ежемесячно. Чтобы не выводилось сообщение о пропущенных заданиях оптимизации, снимите флажок **Уведомлять в случае пропуска...** (Notify me if...).

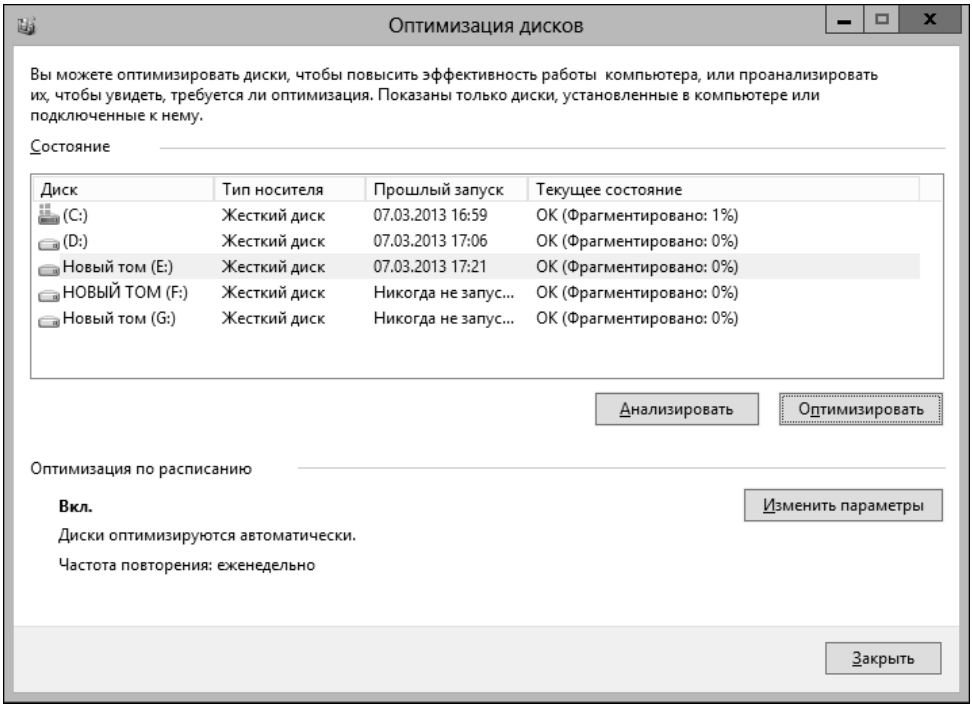


Рис. 12.13. Диалоговое окно для оптимизации производительности дисков

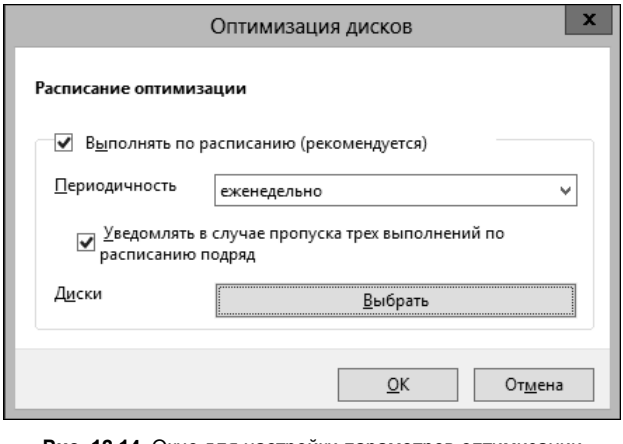


Рис. 12.14. Окно для настройки параметров оптимизации

4. Чтобы задать диски для дефрагментации, нажмите кнопку **Выбрать** и выберите диски. По умолчанию дефрагментация выполняется на всех установленных и подключенных к компьютеру дисках, а также на всех новых дисках, добавляемых к компьютеру. Установите флажки для дисков, которые необходимо дефрагментировать автоматически, и снимите флажки тех дисков, для которых это не требуется. Нажмите кнопку **OK**, чтобы сохранить и применить выполненные настройки.
5. Нажмите кнопку **OK**, а затем **Закрыть**, что закрыть все диалоговые окна, связанные с настройкой дефрагментации.

Примечание

Операционная система Windows 8 автоматически выполняет дефрагментацию на основе циклического выбора. При этом подходе, когда запланированный сеанс дефрагментации останавливается, а затем запускается снова, система автоматически выбирает для обработки следующий том в очереди, требующий дефрагментации.

Ресинхронизация и восстановление зеркального тома

Операционная система Windows 8 автоматически синхронизирует зеркальные тома на дисках. Тем не менее данные на дисках зеркального тома могут утратить синхронизацию. Например, если один из приводов тома отключится, данные будут записываться только на подключенный привод.

Зеркальные тома поддаются ресинхронизации и восстановлению, но только в том случае, если все диски набора одного типа — или MBR, или GPT. Оба диска зеркального тома должны быть подключены. Статус тома с проблемой синхронизации по причине сбоя одного из дисков должен отображаться как **Отказавшая избыточность**. Корректирующее действие зависит от состояния проблемного привода.

- Если состояние отображается как **Отсутствует** или **Вне сети**, проверьте, что на привод подается питание и он подключен должным образом. Затем откройте средство **Управление дисками**, щелкните правой кнопкой мыши по значку неисправного тома и в контекстном меню выберите команду **Реактивировать том**. Состояние тома должно измениться на **Регенерация**, а затем на **Исправен**. Если том не возвратится в состояние **Исправен**, щелкните на нем правой кнопкой мыши и в контекстном меню выберите команду **Ресинхронизация зеркала** (Resynchronize Mirror).
- Если статус привода отображается как **В сети (ошибки)**, щелкните правой кнопкой мыши на значке проблемного тома и в контекстном меню выберите команду **Реактивировать том**. Состояние тома должно измениться на **Регенерация**, а затем на **Исправен**. Если том не возвратится в состояние **Исправен**, щелкните на нем правой кнопкой мыши и в контекстном меню выберите команду **Ресинхронизация зеркала**.
- Если состояние одного из дисков тома отображается как **Не читается**, может потребоваться повторить сканирование приводов системы, выбрав в меню **Действие** средства **Управление дисками** команду **Повторить проверку дисков**. Если состояние привода не меняется, попробуйте перезагрузить компьютер.
- Если диск все равно не подключается, щелкните правой кнопкой мыши на значке проблемного тома, в контекстном меню выберите команду **Удалить зеркало** и укажите для удаления проблемный диск. Далее щелкните правой кнопкой мыши на значке оставшегося диска тома и в контекстном меню выберите команду **Добавить зеркало**. Теперь нужно добавить к тому зеркальный диск на другом приводе, имеющем нераспределенное пространство, равное или большее, чем размер первого диска зеркального тома. Если такого пространства нет, его нужно создать, удалив другие тома или же добавив новый привод.

Восстановление зеркального системного тома для загрузки компьютера

Сбой одного из дисков зеркального тома может препятствовать загрузке компьютера. Обычно это происходит при сбое основного диска зеркального системного или загрузочного тома или обоих.

При создании зеркального системного тома операционная система должна добавить запись в диспетчер загрузки системы, которая позволяет выполнить загрузку со вторичного диска зеркального тома. Наличие такой записи в файле диспетчера загрузки облегчает решение проблемы сбоя основного диска зеркального тома, так как все, что для этого требуется, — это выбрать данную запись с целью выполнить загрузку со вторичного диска зеркального тома. Если при создании зеркального загрузочного тома такая запись не была создана (ее наличие можно проверить, выполнив команду `bcdedit` в консоли командной строки, запущенной от имени администратора), ее можно создать самому с помощью редактора хранилища BCD (bcdedit.exe).

Теперь, если система не загружается с основного системного диска зеркального тома, перезагрузите компьютер и выберите опцию **Boot Mirror — Secondary Plex** для диска, с которого нужно загрузить операционную систему. Система должна загрузиться без проблем. Загрузив систему со вторичного диска зеркального тома, можно запланировать необходимое обслуживание для восстановления зеркала. Процедура для этого следующая:

1. Выключите компьютер, замените проблемный диск, а затем снова запустите компьютер.
2. Разделите зеркальный том, а затем восстановите его с новым диском, который обычно будет называться **Диск 0**. Для этого щелкните правой кнопкой мыши на значке оставшегося диска исходного зеркального тома и в контекстном меню выберите команду **Добавить зеркало**.
3. В списке **Диски** открывшегося диалогового окна **Добавить зеркальный том** (Add Mirror) выберите диск, который нужно добавить, а затем нажмите кнопку **Добавить зеркальный том**. Будет запущен процесс создания зеркального тома. В средстве **Управление дисками** состояние обоих дисков создаваемого зеркального тома отображается как **Ресинхронизация**. Добавляемый диск обозначается значком желтого треугольника с восклицательным знаком.
4. Чтобы сделать новый диск основным диском зеркального тома, снова разделите зеркальный том на два отдельных диска. Проверьте, чтобы замененному диску в бывшем зеркальном томе была присвоена буква, которая была присвоена всему зеркальному тому. В противном случае присвойте требуемую букву вручную.
5. Теперь щелкните правой кнопкой мыши на значке этого диска, в контекстном меню выберите команду **Добавить зеркало** и укажите второй диск разделенного зеркального тома.
6. Проверьте в загрузочной конфигурации, что новый диск зеркального тома используется в качестве основного загрузочного диска. В противном случае отредактируйте загрузочную конфигурацию соответствующим образом вручную.

Внешние устройства хранения данных

Внешние устройства хранения данных можно форматировать под FAT, FAT32, exFAT и NTFS. Внешние устройства хранения данных можно подключать к разъемам портов ввода-вывода компьютера вместо установки их внутри системного блока. Это делает установку внешних устройств хранения данных более легкой, чем установка большинства фиксированных приводов жестких дисков. Большинство внешних устройств хранения данных подключается посредством интерфейса USB, eSATA или FireWire. В случае устройств с интерфейсом USB или FireWire скорость передачи данных и общая производительность устройства с точки зрения пользователя в основном зависит от версии интерфейса.

В настоящее время используется несколько версий интерфейса USB и FireWire. Версия USB 2.0 является промышленным стандартом, но при этом происходит всеобщий переход на версию USB 3.0. Существуют два класса устройств USB 2.0: полноскоростные[1] со скоростью передачи данных до 12 Мбит/с и высокоскоростные[2] со скоростью до 480 Мбит/с. Но хотя высокоскоростной интерфейс USB 2.0 поддерживает максимальную скорость передачи данных в 480 Мбит/с, постоянная скорость обычно составляет от 10 до 30 Мбит/с. Фактическая постоянная скорость передачи зависит от многих факторов, включая тип устройства, тип передаваемых данных и мощности процессора компьютера. Каждый USB-контроллер компьютера обладает фиксированной пропускной способностью, которая разделяется между всеми подключенными к нему устройствами. Скорость передачи данных будет существенно ниже, если USB-порт компьютера имеет более раннюю версию, чем версия подключенного к нему устройства. Например, если подключить устройство USB 2.0 к порту USB 1.0 или наоборот, будет использоваться значительно более низкая скорость передачи USB 1.0.

Порты USB 1.0, 1.1 и 2.0 выглядят одинаково. Но большинство портов USB 3.0 имеют специальную окраску, чтобы отличить их от портов более ранних версий. Тем не менее лучше определить версию портов USB компьютера по технической документации компьютера или его системной платы. Мониторы последних выпусков также оснащаются портами USB 2.0 для подключения устройств. При подключении USB-устройств к такому монитору он играет роль USB-концентратора. Все устройства, подключенные к USB-концентратору любого типа, разделяют его общую пропускную способность, определяемую скоростью USB-порта компьютера, к которой он подключен.

Стандарт высокопроизводительного подключения FireWire (IEEE 1394) использует одноранговую архитектуру, в которой периферийные устройства согласовывают использование шины, чтобы определить, какое устройство может управлять передачей данных наилучшим образом. В настоящее время используется несколько версий интерфейса FireWire. Версия FireWire 400 (IEEE 1394a) поддерживает максимальную постоянную скорость передачи данных до 400 Мбит/с. Версия IEEE 1394b поддерживает скорость в 400 (S400), 800 (S800) и 1600 Мбит/с (S1600). Как и в случае с устройствами USB, если подключить устройство IEEE 1394b к порту IEEE 1394a или наоборот, будет использоваться значительно более низкая скорость передачи версии FireWire 400.

Также как и для USB-устройств, постоянная скорость передачи данных портов IEEE 1394a и IEEE 1394b будет значительно ниже, чем возможная максимальная скорость. Кабели и разъемы IEEE 1394a и IEEE 1394b имеют разные формы, чтобы не перепутать их, если знать в чем заключается разница между ними. Разъемы и кабели FireWire 400 выглядят точно так же, как и для ранних версий FireWire, которые были реализованы до окончательного принятия спецификаций IEEE 1394a и IEEE 1394b. Кабели и разъемы FireWire с четырьмя контактами не имеют питания шины. Кабели и разъемы для FireWire 400 имеют шесть контактов, а для FireWire 800 и FireWire 1600 — девять контактов.

Устройства хранения, обладающие сетевыми возможностями, можно напрямую подключать к сети через кабель Ethernet. Многие из таких устройств поддерживают скорость передачи данных в 1 Гбит/с (или 1000 Мбит/с). Также все более доступными становятся устройства, поддерживающие скорость передачи до 10 Гбит/с.

Прежде чем приобретать внешнее устройство хранения данных, следует рассмотреть, какие интерфейсы поддерживаются компьютером и какие используются устройством. Некоторые

---

[1] full speed.

[2] high speed.

устройства оснащены двойным интерфейсом USB 2.0 и FireWire 400, или даже тройным, поддерживающим кроме первых двух еще и FireWire 800. Такие устройства предоставляют больший выбор способов их подключения.

Управление внешними устройствами хранения выполняется в консоли **Компьютер** или **Управление дисками**. Для этого нужно щелкнуть на значке требуемого устройства правой кнопкой мыши и в контекстном меню выбрать одну из следующих команд:

- **Открыть** — для просмотра содержимого диска в Проводнике Windows;
- **Форматировать** — для форматирования съемного диска *(см. разд. "Форматирование разделов и томов" ранее в этой главе)*. Съемные диски обычно имеют один раздел;
- **Свойства** — для просмотра или настройки свойств устройства. На вкладке **Общие** окна свойств устройства можно присвоить метку тома *(см. разд. "Присвоение, изменение и удаление метки тома" ранее в этой главе)*.

Для съемных дисков можно настраивать представления дисков и папок. Для этого нужно открыть диалоговое окно свойств диска или папки и выбрать в нем вкладку **Настроить**. На этой вкладке можно задать тип папки, чтобы управлять отображаемыми по умолчанию сведениями. Например, можно установить тип папки по умолчанию как **Документы**, **Изображения** или **Видео**. Также можно задать рисунок и значок для папки.

Съемные диски поддерживают сетевой доступ к файлам и папкам. Настройка сетевого доступа съемных дисков выполняется точно так же, как и для обычных дисков. Можно задавать полномочия для сетевого доступа, настраивать опции кэширования для использования автономных файлов, а также ограничивать число пользователей, которые могут одновременно работать с сетевым ресурсом. Сетевой доступ можно задать как для всего съемного диска, так и для отдельных папок, содержащихся в нем. Также можно создавать несколько экземпляров сетевого ресурса.

Съемные сетевые диски отличаются от обычных сетевых NTFS-дисков в том отношении, что они не обязательно имеют базовую архитектуру обеспечения безопасности. А в случае FAT, FAT32 или exFAT, хранящиеся на них папки и файлы не имеют никаких полномочий доступа или других возможностей безопасности, кроме таких базовых флагов атрибутов, как **Только чтение** или **Скрытый**.

Оптические диски

Образы дисков CD/DVD и Blu-ray часто сохраняются в виде файлов ISO. Операционная система Windows 8 имеет встроенные возможности для работы с образами ISO, в частности, для их записи на диски CD или DVD. Также она обладает встроенными возможностями для записи данных на диски CD/DVD. Но прежде чем записывать данные на диск, следует ознакомиться с доступными типами оптических дисков и параметрами их файловых систем.

Основы записи дисков

По умолчанию, когда в пишущий привод оптических дисков вставляется пустой диск, в панели инструментов Проводника Windows отображается кнопка **Записать** (Burn). Нажатие этой кнопки запускает мастер записи на диск. Но следует иметь в виду, что устройства чтения оптических дисков для компьютеров отличаются от бытовых или автомобильных проигрывателей дисков. Обычно компьютерный привод оптических дисков может читать как диски промышленной записи, так и диски, записанные на компьютере в специальных форматах, но бытовой или автомобильный проигрыватель дисков не всегда сможет распознать диск, записанный на компьютере.

Большинство записывающих приводов поддерживает различные форматы дисков. Операционная система Windows 8 поддерживает запись данных на диски CD-R, CD+R, CD-RW, DVD-R, DVD+R, DVD-RW, DVD+RW и DVD-RAM. При этом диски DVD могут быть однослойными односторонними или двухслойными односторонними. Также Windows 8 поддерживает диски Blu-ray. Если компьютер оснащен пишущим приводом Blu-ray, может быть, вам удастся записывать диски Blu-ray.

Операционная система Window 8 поддерживает два способа записи дисков:

- в формате "mastered";
- в формате LFS.

Большинство программ Windows записывает диски, используя первый способ, и диски автоматически записываются с соответствующей файловой системой. При таком подходе выбирается группа файлов для записи на диск, и все они записываются за один сеанс. Это удобный способ для записи больших наборов файлов; кроме этого, он имеет преимущество в том, что записанные таким образом диски можно воспроизводить на любом компьютерном приводе или ином устройстве чтения дисков, который поддерживает данный тип диска.

Блоки файлов записываются на диск по сеансам. Многие программы записи дисков предоставляют возможность оставлять сеанс открытым, чтобы на диск можно было добавлять файлы позже. Когда на диск больше не планируется добавлять файлов, сеанс закрывается. Закрытие сеанса финализирует диск и делает возможным его чтение на других компьютерах и устройствах. При открытом сеансе диск можно читать на совместимом компьютерном приводе.

В противоположность, диск с файловой системой LFS работает как любой другой съемный носитель, например флешка или карта флеш-памяти. На диск можно добавлять файлы, не выполняя явной операции записывания, просто посредством копирования и вставки или методом перетаскивания. Файлы с диска также можно удалять обычным образом — выделив требуемый файл и нажав клавишу <Delete>. При этом, если диск перезаписываемый, на нем освобождается место, занимаемое удаляемым файлом. Такой диск можно извлечь из провода, а затем вставить повторно и продолжать использовать таким же образом.

Оптические диски с файловой системой LFS форматируют, используя формат UDF[1], а не стандартный формат CDFS[2]. Как правило, диски формата UDF могут читать только компьютерные приводы оптических дисков. Операционная система Windows 8 поддерживает запись на диски в нескольких версиях формата UDF, включая следующие:

- UDF 1.5 — формат, совместимый с Windows 2000 и более поздними версиями Windows. Может не поддерживаться компьютерами Apple или системой Windows 98;
- UDF 2.0 — формат, совместимый с Windows XP и более поздними версиями Windows. Может не поддерживаться компьютерами Apple, ОС Windows 98 и Windows 2000;
- UDF 2.01 — формат по умолчанию, содержащий основное обновление. В большинстве случаев рекомендуется использовать именно его. Совместимый с Windows XP и более поздними версиями Windows. Может не поддерживаться компьютерами Apple, ОС Windows 98 и Windows 2000;
- UDF 2.5 — формат, оптимизированный для Windows Vista и более поздних версий Windows. Может не поддерживаться компьютерами Apple и более ранними версиями Windows.

---

[1] Universal Disc Format — универсальный дисковый формат.

[2] CD File System — файловая система компакт-дисков.

Подключение образов ISO

Образ ISO можно подключать, создавая таким образом виртуальный диск, с которым можно работать, как с обычным физическим диском. Например, если подключить установочный образ ISO для приложения, с него можно установить данное приложение.

Подключение образа ISO в виде виртуального диска выполняется следующим образом: в Проводнике Windows щелкните правой кнопкой мыши по ISO-файлу и в контекстном меню выберите команду **Подключить** (Mount).

Запись образа ISO на диск

Образ ISO можно записать на физический диск, который затем можно использовать в приводах оптических дисков других компьютеров. Записать образ ISO на физический диск можно следующим образом:

1. Вставьте пустой диск в пишущий привод оптических дисков. Если откроется окно автозапуска, закройте его, нажав кнопку с крестиком в правом верхнем углу этого окна.
2. В Проводнике Windows щелкните на ISO-файле, который нужно записать на диск, и в контекстном меню выберите команду **Записать образ диска** (Burn disk image).
3. В поле **Устройство записи на диск** (Disc burner) следующего окна (рис. 12.15) выберите требуемый пишущий привод, а затем нажмите кнопку **Записать** (Burn).

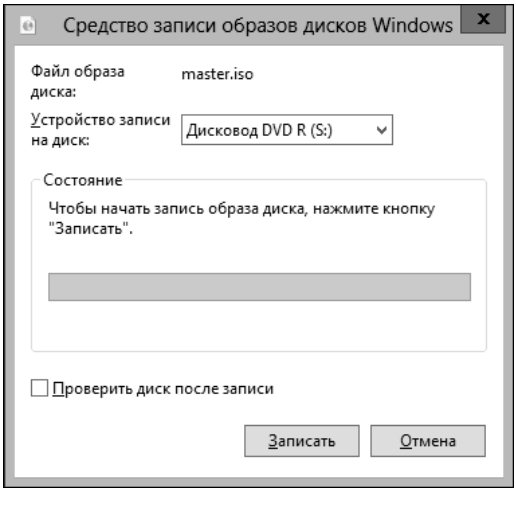


Рис. 12.15. Диалоговое окно для записи образа ISO на диск

Запись дисков типа "mastered"

Запись диска типа "mastered" выполняется следующим образом:

1. Вставьте пустой диск в пишущий привод оптических дисков. Далее, выполните одно из следующих действий.
   - Если откроется окно автозапуска, щелкните в нем, а в открывшемся меню выберите опцию **Записать файлы на диск — Проводник** (Burn files to disc — File Explorer).
   - Если окно автозапуска не откроется, откройте консоль **Компьютер**, щелкните в нем правой кнопкой мыши на значке пишущего привода и в контекстном меню выберите

команду **Открыть автозапуск** (Open AutoPlay). В меню окна автозапуска выберите опцию **Записать файлы на диск — Проводник**.

2. В поле **Название диска** (Disc title) (рис. 12.16) введите название диска. Чтобы создать диск типа "mastered", установите переключатель **С проигрывателем CD/DVD** (With a CD/DVD player). Нажмите кнопку **Далее**, после чего записываемый диск откроется в Проводнике Windows. Основная панель Проводника содержит пустой список **Подготовленные для записи на диск файлы**. Не закрывайте это окно.

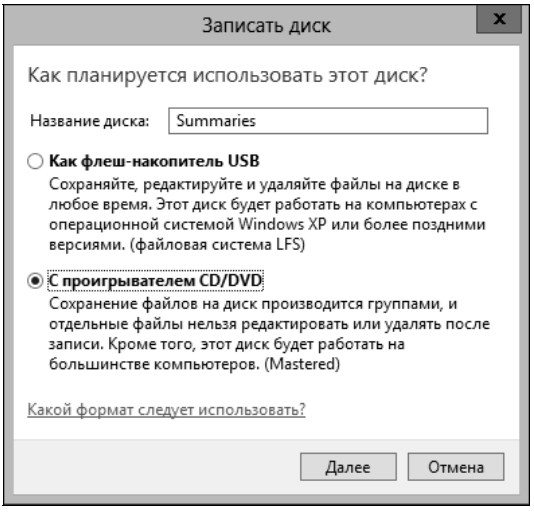


Рис. 12.16. Подготовка записи диска типа "mastered"

3. Перетащите или скопируйте в эту панель файлы, которые требуется записать на диск. Эти файлы копируются с их исходного размещения в виде временных файлов во временную папку, которая создается в личном профиле текущего пользователя. Копии файлов для записи создаются для того, чтобы все они были в одном месте, и чтобы пользователь обладал необходимыми полномочиями для доступа к ним с целью записи на диск.
4. Когда все будет готово для записи файлов, щелкните правой кнопкой мыши на пустой области панели Проводника, содержащей файлы для записи, и выберите в контекстном меню команду **Записать на диск** (Burn to disc). Откроется диалоговое окно мастера записи на диск. Введите название диска в соответствующее поле (которое может содержать название предыдущего диска) и укажите желаемую скорость записи (по умолчанию скорость записи установлена на максимальную, поддерживаемую пишущим приводом).
5. Нажмите кнопку **Далее**. Выбранные файлы будут добавлены в образ диска, а затем записаны на физический диск в приводе. По завершению записи файлов диск по умолчанию извлекается из привода, и снова открывается окно мастера записи на диск с сообщением об успешной записи файлов. Это окно также содержит предложение повторной записи выбранных файлов на другой диск. Чтобы записать файлы повторно, установите соответствующий флажок и нажмите кнопку **Готово**, после чего повторите процедуру записи сначала. В противном случае нажатие кнопки **Готово** удалит временные файлы и закроет окно мастера записи на диск.

В случае ошибки записи выводится соответствующее сообщение об ошибке, с предоставлением выбора попытаться выполнить запись на другой диск, удалить временные файлы и завершить процесс записи или же сохранить временные файлы, чтобы попытаться записать

их позже. При повторении попытки записи установите более низкую скорость записи. Хотя привод дисков может и поддерживать высокую скорость записи, эта скорость может не поддерживаться диском, на который выполняется запись.

Обычно в случае ошибки записи на диск будет записана только часть всех выбранных для записи файлов. Если сеанс записи еще открыт, можно попробовать снова записать диск. Но иногда текущий диск может быть больше не пригодным и потребуется использовать новый.

Запись дисков в формате LFS

Запись дисков в формате LFS выполняется следующим образом:

1. Вставьте пустой диск в пишущий привод оптических дисков. В окне автозапуска выберите опцию **Записать файлы на диск — Проводник**. Если окно автозапуска не откроется, щелкните в консоли **Компьютер** на значке пишущего привода, в контекстном меню выберите команду **Открыть автозапуск**, а в окне автозапуска щелкните на этой опции.
2. В поле **Название диска** открывшегося диалогового окна **Записать диск** введите требуемое название диска. Затем, чтобы создать диск типа UDF с файловой системой LFS, установите переключатель **Как флеш-накопитель USB** (Like a USB flash drive). Нажмите кнопку **Далее**. Windows создаст на диске файловую систему LFS и откроет диск в Проводнике Windows.
3. Основная панель Проводника содержит пустой список **Подготовленные для записи на диск файлы**. Не закрывайте это окно.
4. Поскольку в данном случае мы работаем с диском в оперативном режиме, списка файлов для записи как такового нет. Вместо этого файлы можно просто добавлять и удалять с оптического диска, как будто бы это был жесткий диск или флеш-накопитель. В случае перезаписываемых дисков удаление файлов с диска освобождает занимаемое ими место на диске, делая его доступным для записи других файлов. А в случае стандартных записываемых дисков удаляемые файлы просто помечаются, как удаленные, и не отображаются в Проводнике, но остаются на диске. Место, занимаемое этими файлами, не освобождается и не может быть использовано для записи других файлов.
5. Пока диск находится в приводе, Windows 8 держит сеанс записи диска открытым. При извлечении диска Windows 8 закрывает сеанс записи, чтобы диск можно было использовать на других компьютерах. Если такой диск снова вставить в пишущий дисковод, на него снова можно добавлять и удалять файлы в Проводнике Windows. При изменении содержимого диска открывается новый сеанс записи, который, как и первоначальный сеанс записи, закрывается при извлечении диска. Сеанс записи можно также закрыть вручную, щелкнув правой кнопкой мыши на значке используемого пишущего привода в консоли **Компьютер** и выбрав в контекстном меню команду **Завершить сеанс** (Close session).

Изменение значений параметров записи по умолчанию

Параметры записи по умолчанию можно изменить следующим образом:

1. Откройте консоль **Компьютер**, щелкните в ней правой кнопкой мыши на значке пишущего привода и в контекстном меню выберите команду **Свойства**.
2. Если компьютер имеет несколько пишущих приводов, на вкладке **Запись** в раскрывающемся списке **Запись на диск** (Disc burning) выберите привод, который следует использовать по умолчанию.

3. В следующем раскрывающемся списке укажите жесткий диск для хранения временных файлов.
4. Чтобы не извлекать после записи диски типа "mastered", снимите соответствующий флажок.
5. По умолчанию при извлечении дисков типа LFS Windows закрывает сеанс записи. Для настройки этого параметра нажмите кнопку **Общие параметры** (Global settings) и в открывшемся одноименном диалоговом окне задайте требуемое поведение при извлечении диска для односеансовых и многосеансовых дисков, установив или сбросив соответствующие флажки.
6. Нажмите кнопку **OK**, чтобы сохранить и применить выполненные настройки.

Управление сжатием дисков и шифрованием файлов

Для дисков с файловой системой NTFS Windows 8 предоставляет возможность сжатия дисков и шифрования хранящихся на них файлов. Сжатие диска позволяет уменьшить объем дискового пространства, требуемого для хранения файлов, а шифрование предоставляет дополнительный уровень безопасности для данных. Но эти возможности нельзя применять одновременно, т. е. можно использовать либо одну из них, либо другую, но не обе вместе. Обе эти возможности независимы от функциональности шифрования дисков BitLocker, которая зашифровывает диски на уровне тома и предотвращает несанкционированный доступ к дискам до загрузки операционной системы.

Сжатие дисков и данных

Когда для диска включена функциональность сжатия, все файлы и папки при помещении на диск автоматически сжимаются. Так как этот процесс сжатия прозрачен для пользователей, со сжатыми данными можно работать, как с обычными данными. Разница заключается в том, что на сжатом диске можно хранить больший объем информации, чем на несжатом. Обратите внимание, что в Проводнике Windows имена сжатых ресурсов отображаются синим цветом.

Практический совет

Хотя сжатие диска определенно является полезной возможностью, когда нужно сэкономить на дисковом пространстве, сжатые данные нельзя зашифровывать. Сжатие и шифрование томов NTFS являются взаимоисключающими возможностями. Эти возможности нельзя использовать одновременно. Более подробную информацию по шифрованию данных *см. в разд. "Шифрование дисков и данных" далее в этой главе*. Если попытаться сжать зашифрованные данные, Windows 8 сначала автоматически расшифрует их, и только после этого сожмет. А если попытаться зашифровать сжатые данные, Windows 8 сначала распакует их, а затем выполнит шифрование.

Сжатие дисков

Для сжатия всего содержимого диска применяется следующая процедура:

1. В Проводнике Windows или в консоли **Управление дисками** щелкните правой кнопкой мыши по значку диска и в контекстном меню выберите команду **Свойства**.
2. Установите флажок **Сжать этот диск для экономии места** (Compress contents to save disk space) и нажмите кнопку **OK**.

Сжатие файлов и папок

Кроме сжатия всего диска, Windows 8 позволяет сжимать отдельные папки и файлы. Процедура для этого следующая:

1. В Проводнике Windows щелкните правой кнопкой мыши по требуемой папке или файле и в контекстном меню выберите команду **Свойства**.
2. На вкладке **Общие** окна свойств нажмите кнопку **Другие** (Advanced). В открывшемся диалоговом окне **Дополнительные атрибуты** установите флажок **Сжимать содержимое для экономии места на диске** (Compress contents to save disk space), а затем нажмите кнопку **OK** (рис. 2.17).

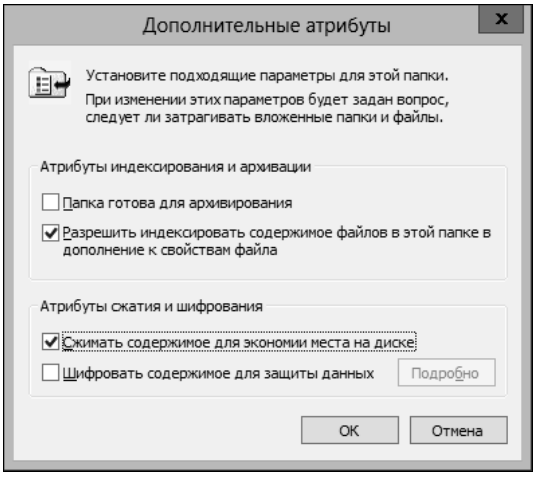


Рис. 12.17. Диалоговое окно для сжатия папок и файлов

В случае отдельного файла Windows 8 помечает файл как сжатый, а затем сжимает его. А в случае папки Windows 8 также помечает ее как сжатую, а затем просто сжимает все содержащиеся в ней файлы. Если сжимаемая папка содержит вложенные папки, Windows 8 выводит диалоговое окно, предоставляющее возможность сжать все ее вложенные папки, установив флажок **К данной папке и ко всем вложенным файлам и папкам** (Apply changes to this folder, subfolders and files). Новые файлы и папки, добавляемые в сжатую папку, также автоматически сжимаются.

Примечание

Если в сжатую папку переместить несжатый файл с другого диска, этот файл сжимается. Но если переместить файл с того же самого диска, на котором находится сжатая папка, файл не сжимается. И, как уже упоминалось, сжатые файлы нельзя шифровать.

Отмена сжатия дисков

Отменить сжатие диска можно следующим образом:

1. В Проводнике Windows или в консоли **Управление дисками** щелкните правой кнопкой мыши по значку требуемого диска и в контекстном меню выберите команду **Свойства**.
2. Снимите флажок **Сжать этот диск для экономии места** и нажмите кнопку **OK**.

Совет

Прежде чем отменять сжатие, Windows всегда проверяет доступное свободное место. Но будет хорошей практикой выполнять такую проверку и самому. Если объем свободного пространства

меньше, чем объем сжатых данных, снять сжатие может не получиться. Например, если сжатый диск имеет 70 Гбайт свободного пространства и 150 Гбайт занятого, данный объем свободного пространства явно недостаточен, чтобы снять сжатие с диска. Как правило, чтобы снять сжатие, объем свободного пространства должен быть в полтора-два раза больше, чем объем сжатых данных.

Отмена сжатия папок и файлов

Для отмены сжатия папок и файлов применяется следующая процедура:

1. В Проводнике Windows щелкните правой кнопкой мыши на требуемой папке или файле и в контекстном меню выберите команду **Свойства**.
2. На вкладке **Общие** окна свойств нажмите кнопку **Другие**. В открывшемся диалоговом окне **Дополнительные атрибуты** снимите флажок **Сжимать содержимое для экономии места на диске**. Последовательно нажмите кнопку **OK**, чтобы закрыть все окна.

В случае файлов Windows 8 отменяет сжатие файла, а в случае папок отменяет сжатие для всех файлов папки. Если папка, для которой отменяется сжатие, содержит вложенные папки, Windows 8 выводит диалоговое окно, предоставляющее возможность отменить сжатие всех ее вложенных папок, установив флажок **К данной папке и ко всем вложенным файлам и папкам**.

Совет

Операционная система Windows 8 также предоставляет средства командной строки для сжатия и отмены сжатия данных. Для сжатия применяется утилита Compact (compact.exe), а для снятия сжатия — утилита Expand (expand.exe).

Шифрование дисков и данных

Файловая система NTFS имеет много преимуществ в сравнении с другими файловыми системами, которые можно использовать в Windows 8. Одним из основных преимуществ является возможность автоматического шифрования и расшифровывания данных с помощью файловой системы EFS[1]. Шифрование данных добавляет дополнительный слой защиты для конфиденциальных данных, который предотвращает доступ к ним несанкционированных пользователей, позволяя доступ только пользователю, выполнившему шифрование. Но это преимущество также может быть и недостатком, т. к. для предоставления доступа к зашифрованным данным другим разрешенным пользователям пользователь должен отменить шифрование.

Примечание

Как упоминалось ранее, зашифрованные файлы нельзя сжимать. Возможности шифрования и сжатия являются взаимно исключающими. Одновременно можно использовать только одну из них.

Шифрование и файловая система EFS

Шифрование может применяться к папкам или отдельным файлам. Помещаемый в зашифрованную папку файл также автоматически зашифровывается. Доступ к зашифрованным файлам может иметь только зашифровавший их пользователь. Для предоставления доступа к зашифрованным файлам другим пользователям пользователь-владелец файлов должен отменить их шифрование.

[1] Encrypting File System — шифрующая файловая система.

Каждый зашифрованный файл имеет однозначный ключ шифрования. Это означает, что зашифрованный файл можно копировать, перемещать и переименовывать, как любой другой файл, и в большинстве случаев эти действия не влияют на шифрование данных. (Подробную информацию о шифровании файлов *см. в разд. "Работа с зашифрованными файлами и папками" далее в этой главе*.) Зашифровавший файл пользователь всегда имеет доступ к нему при условии, что его сертификат открытого ключа доступен на используемом компьютере. Для этого пользователя процесс шифрования и расшифровывания выполняется автоматически и прозрачно шифрующей файловой системой EFS. Настройки по умолчанию файловой системы EFS позволяют пользователям выполнять шифрование, не требуя специального разрешения. Файлы зашифровывают, используя открытый и закрытый ключи, которые файловая система EFS генерирует автоматически для каждого пользователя.

Сертификаты шифрования сохраняются среди данных в профилях пользователей. Если пользователь работает на нескольких компьютерах и хочет применять шифрование, администратор должен настроить для такого пользователя перемещаемый профиль. Перемещаемый профиль обеспечивает доступность данных профиля пользователя и сертификатов открытого ключа с других компьютеров. Без такой возможности пользователи не могли бы получить доступ к своим зашифрованным данным с другого компьютера.

Хотя возможность шифрования дисков BitLocker и файловая система EFS независимы друг от друга, обе они имеют встроенную систему для восстановления данных, предотвращающую потерю данных. Эта система обеспечивает восстановление данных в случае утери или удаления сертификата открытого ключа пользователя. Наиболее распространенным сценарием такой утери сертификата является ситуация, когда пользователь покидает организацию и его учетная запись удаляется. При наличии учетной записи пользователя его начальник мог бы войти по ней в систему, просмотреть файлы и сохранить важные файлы в другое место, но когда учетная запись удалена, доступ к зашифрованным томам и файлам можно получить, только отменив шифрование или переместив файлы на диск с файловой системой FAT или FAT32 (которые не поддерживают шифрующую файловую систему и шифрование BitLocker).

Чтобы получить доступ к файлам пользователя, чья учетная запись была удалена, нужно использовать агент восстановления. Агенты восстановления имеют доступ к ключу шифрования файлов, требующемуся для разблокирования данных в зашифрованных файлах. Но с целью защиты конфиденциальных данных агенты восстановления не имеют доступа к личному ключу пользователя или к информации личного ключа.

Операционная система Windows 8 разрешает шифрование томов без выделенных агентов восстановления BitLocker, но не допускает шифрование файлов без выделенных агентов восстановления файловой системы LFS. Агенты восстановления файловой системы LFS выделяются автоматически, и также автоматически генерируются необходимые сертификаты восстановления. Таким образом обеспечивается восстановление зашифрованных файлов.

Агенты восстановления настраиваются на двух уровнях.

- **Доменном.** Агент восстановления для домена настраивается автоматически при установке первого контроллера доменов Windows 8. По умолчанию агентом восстановления является администратор домена. Посредством групповой политики администраторы домена могут назначать дополнительных агентов восстановления. Администраторы домена также могут делегировать полномочия агента восстановления назначенным администраторам безопасности.
- **Локального компьютера.** Когда компьютер является членом рабочей группы или работает автономно, по умолчанию агентом восстановления является администратор локального компьютера. Также могут быть назначены дополнительные агенты восстановления.

Кроме этого, если в доменной среде вместо агентов восстановления уровня домена необходимо иметь локальных агентов восстановления, из групповой политики следует удалить политику восстановления для домена.

Агентов восстановления, в которых больше нет надобности, можно удалять. Но если удалить всех агентов восстановления для файловой системы EFS, она больше не будет зашифровывать файлы. Для функционирования файловой системы EFS необходимо наличие, по крайней мере, одного агента восстановления.

Шифрование файлов и папок

Операционная система Windows 8 позволяет зашифровывать отдельные папки и файлы на томах с файловой системой NTFS. Шифрование файлов преобразует данные в файлах в особый формат, в котором их может читать только зашифровавший их пользователь. Пользователи могут зашифровывать файлы, только если они обладают соответствующими правами доступа. При шифровании папок, папка помечается как зашифрованная, но в действительности шифруются только содержащиеся в ней файлы. Все файлы, создаваемые или вставляемые в зашифрованную папку, автоматически зашифровываются. В Проводнике Windows имена зашифрованных ресурсов отображаются зеленым цветом.

Для шифрования папки или файла применяется следующая процедура:

1. В Проводнике Windows щелкните правой кнопкой мыши на требуемой папке или файле и в контекстном меню выберите команду **Свойства**.
2. На вкладке **Общие** окна свойств нажмите кнопку **Другие** (Advanced) и в открывшемся диалоговом окне **Дополнительные атрибуты** установите флажок **Шифровать содержимое для защиты данных** (Encrypt contents to secure data). Последовательно нажмите кнопку **OK**, чтобы закрыть все окна.

> ***Примечание***
>
> Нельзя шифровать сжатые, системные файлы и файла с атрибутом **Только чтение**. При попытке зашифровать сжатые файлы, с них автоматически снимается сжатие, после чего применяется шифрование. При попытке применить шифрование к системным файлам выводится сообщение об ошибке.

В случае отдельного файла Windows 8 помечает файл как зашифрованный, а затем зашифровывает его. А в случае папки Windows 8 также помечает ее как зашифрованную, а затем шифрует все содержащиеся в ней файлы. Если шифруемая папка содержит вложенные папки, Windows 8 выводит диалоговое окно, предоставляющее возможность зашифровать все ее вложенные папки, установив флажок **К данной папке и ко всем вложенным файлам и папкам**.

> ***Примечание***
>
> При копировании, перемещении или переименовании на томах NTFS зашифрованные файлы сохраняют шифрование. Но при копировании или перемещении зашифрованного файла на том FAT, FAT32 или FAT32 файл автоматически расшифровывается. Это означает, что для копирования или перемещения зашифрованного файла необходимо обладать соответствующими правами.

Работа с зашифрованными файлами и папками

Ранее в этой главе было сказано, что зашифрованные файлы и папки можно копировать, перемещать и переименовывать, как обычные папки. Но данное утверждение было высказано с оговоркой, что это можно делать "в большинстве случаев". При выполнении таких

операций с зашифрованными файлами не должно возникать трудностей при условии, что работа выполняется на томах NTFS на одном и том же компьютере. Но при выполнении этих операций с другими файловыми системами или на других компьютерах возможны проблемы. Наиболее распространенными сценариями работы с зашифрованными файлами являются следующие.

- **Копирование файлов между томов одного и того же компьютера.** При копировании или перемещении зашифрованного файла или папки с одного тома NTFS на другой том NTFS одного и того же компьютера файлы остаются зашифрованными. Но при копировании или при перемещении зашифрованных файлов на том FAT, FAT32 или exFAT файлы расшифровываются перед перемещением, а затем перемещаются как обычные файлы, прибывая на новое место незашифрованными. Файловые системы FAT, FAT32 и exFAT не поддерживают шифрование.
- **Копирование файлов между томами разных компьютеров.** При копировании или перемещении зашифрованного файла или папки с одного тома NTFS на другой том NTFS другого компьютера файлы остаются зашифрованными при условии, что шифрование разрешено на компьютере назначения, а также компьютер назначения является доверяемым для делегирования. В противном случае файлы расшифровываются и перемещаются как обычные файлы. То же самое происходит и при копировании или перемещении зашифрованных файлов на тома FAT, FAT32 или exFAT на другом компьютере. Файловые системы FAT, FAT32 и exFAT не поддерживают шифрование.

После перемещения зашифрованных файлов следует убедиться в том, что они остались зашифрованными. Для этого щелкните правой кнопкой мыши на соответствующем файле и в контекстном меню выберите команду **Свойства**. На вкладке **Общие** окна свойств нажмите кнопку **Другие**. В окне **Дополнительные атрибуты** должен быть установлен флажок **Шифровать содержимое для защиты данных**.

Настройка политики восстановления

В доменах политики восстановления для файловой системы EFS и средства шифрования дисков BitLocker настраиваются автоматически для контроллеров домена и компьютеров членов домена. По умолчанию администраторы домена назначаются агентами восстановления EFS и BitLocker для всех компьютеров домена. В рабочих и домашних группах назначенным агентом восстановления EFS для автономного компьютера является локальный администратор. Для BitLocker в рабочих и домашних группах агент восстановления по умолчанию не назначается.

Агентов восстановления можно просматривать, назначать и удалять с помощью консоли редактора управления групповой политики. Процедура для этого следующая:

1. В редакторе управления групповыми политиками откройте для редактирования требуемый объект групповой политики.
2. Далее разверните узел **Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Политики открытого ключа** и выберите в нем папку **Шифрующая файловая система** или **Шифрование диска BitLocker**, в зависимости от типа агента восстановления, с которым требуется работать.
3. В правой панели консоли будут отображены текущие сертификаты восстановления, сгруппированные по издателю, получателю, конечному сроку действия и другим свойствам.
4. Чтобы назначить дополнительного агента восстановления LFS или BitLocker, щелкните правой кнопкой мыши по соответствующему узлу и в контекстном меню выберите

команду **Добавить агент восстановления данных** (Add Data Recovery Agent). Откроется начальная страница мастера добавления агента восстановления, с помощью которого можно выбрать ранее созданный сертификат, выданный пользователю, и обозначить его, как выделенный сертификат восстановления.

5. Нажмите кнопку **Далее** и на следующей странице мастера, **Выбор агентов восстановления** (Select Recovery Agents), нажмите кнопку **Обзор каталога** (Browse Directory). В открывшемся диалоговом окне **Найти пользователей, контакты или группы** (Find users, contacts and groups) выберите пользователя.

> ***Примечание***
>
> Чтобы можно было назначать дополнительных агентов восстановления, в домене нужно сначала создать корневой Центр сертификации (Certificate Authority). Затем с помощью оснастки **Сертификаты** надо создать личный сертификат на основе шаблона агента восстановления EFS. После этого Центр сертификации должен одобрить этот сертификат, чтобы его можно было использовать.

6. Чтобы удалить агента восстановления, в правой панели выберите сертификат требуемого агента и нажмите кнопку **Удалить**. На запрос подтвердить удаление, нажмите кнопку **Да**. Сертификат будет безвозвратно удален. Если политика восстановления EFS пустая (т. е. в ней нет других назначенных агентов восстановления), файловая система EFS будет отключена, файлы не будут шифроваться, а уже зашифрованные ресурсы не будут иметь агентов восстановления.

Предоставление доступа к зашифрованным файлам другим пользователям

По умолчанию просматривать зашифрованные файлы может только их владелец. Чтобы зашифрованный файл могли просматривать другие пользователи, файл нужно расшифровать или предоставить пользователям специальные права доступа к файлу, выполнив следующие действия:

1. В Проводнике Windows щелкните на требуемом файле или папке правой кнопкой мыши и в контекстном меню выберите команду **Свойства**.
2. На вкладке **Общие** окна свойств нажмите кнопку **Другие**, а в открывшемся окне **Дополнительные атрибуты** — кнопку **Подробно**.
3. Откроется диалоговое окно **Доступ пользователя к** (User access to), содержащее список пользователей, имеющих доступ к зашифрованному ресурсу.
4. Чтобы разрешить доступ другому пользователю, нажмите кнопку **Добавить**.
5. Если для пользователя, которому предоставляется доступ, есть сертификат, выберите имя этого пользователя в предоставленном списке и нажмите кнопку **OK**. В противном случае нажмите кнопку **Найти пользователя** (Find user), чтобы найти сертификат для пользователя.

Отмена шифрования для файлов и папок

В Проводнике Windows имена зашифрованных ресурсов отображаются зеленым цветом. Для отмены шифрования папок и файлов применяется следующая процедура:

1. В Проводнике Windows щелкните правой кнопкой мыши по требуемому ресурсу и в контекстном меню выберите команду **Свойства**.

2. На вкладке **Общие** окна свойств нажмите кнопку **Другие**. В открывшемся диалоговом окне **Дополнительные атрибуты** снимите флажок **Шифровать содержимое для защиты данных**. Последовательно нажмите кнопку **OK**, чтобы закрыть все окна.

В случае файлов Windows 8 снимает шифрование с файла и восстанавливает его исходный формат, а в случае папок — отменяет шифрование для всех файлов папки. Если папка, для которой отменяется шифрование, содержит вложенные папки, Windows 8 выводит диалоговое окно, предоставляющее возможность снять шифрование со всех ее вложенных папок, установив флажок **К данной папке и ко всем вложенным файлам и папкам**.

Совет

Для шифрования файлов операционная система Windows 8 также предоставляет утилиту командной строки Cipher (cipher.exe). Выполнение команды `cipher` без параметров выводит список всех элементов текущего каталога с указанием их состояния шифрования.

ГЛАВА 13

Управление защитой файлов и общими ресурсами

Независимо от среды использования Windows 8 — в домашней группе, рабочей группе или домене — вряд ли имеются более важные аспекты операционной системы, чем обеспечение безопасности файлов и общего доступа к файлам. Безопасность файлов и общий доступ к файлам настолько тесно взаимосвязаны, что трудно рассматривать один из этих вопросов в отрыве от другого. Обеспечение безопасности файлов обеспечивает сохранность важных данных системы посредством ограничения доступа, а предоставления общего доступа к файлам позволяет другим пользователям работать с этими файлами.

Параметры обеспечения безопасности и предоставления общего доступа к файлам

Для компьютеров с Windows 8 параметры обеспечения безопасности файлов и предоставления доступа к ним зависят от двух факторов: формата диска и параметров компьютера. Формат диска определяет уровень доступных параметров безопасности файлов. Диски можно форматировать под файловую систему FAT (FAT16, FAT32 или exFAT) или NTFS. Параметры безопасности для томов FAT и NTFS существенно разнятся.

- Контроль доступа к файлам на томах FAT очень ограничен и заключается только в возможности присваивать файлам и папкам атрибуты **Только чтение**, **Скрытый** или **Системный**. Но несмотря на возможность установки этих атрибутов, любой, у кого есть доступ к то́му FAT, может отменить или изменить эти настройки. Это означает, что файловая система FAT, по сути, не предоставляет никаких мер безопасности по доступу к файлам или их удалению. Любой пользователь может иметь полный доступ ко всем файлам без ограничений, в том числе удалять файлы.
- В противоположность, файловая система NTFS позволяет управлять доступом к файлам и папкам посредством присвоения полномочий, регламентирующих определенный уровень доступа, от полного доступа до полного запрета. Разрешения на доступ можно выдавать как отдельным пользователям, так и группам пользователей, что предоставляет всестороннее управление доступом к файлам и папкам. Например, пользователям группы **Менеджеры продаж** можно разрешить полный доступ к папке с данными клиентов, а пользователям группы **Техподдержка** полностью запретить доступ к этой папке.

Способ общего доступа к файлам определяется настройками параметров компьютера. Для протокола SMB Windows 8 поддерживает две модели общего доступа к файлам.

- **Общий доступ к стандартным папкам.** Позволяет общий доступ к любой папке компьютера, включая папки как на томах FAT, так и на томах NTFS. Для определения пользователей, имеющих доступ к общим папкам, применяются два набора разрешений: разрешения доступа *(см. разд. "Управление доступом к файлам и папкам посредством разрешений NTFS" далее в этой главе)* и разрешения доступа к общему ресурсу *(см. разд. "Общий доступ к сетевым файлам и папкам" далее в этой главе)*. Совместно права доступа и разрешения для общего ресурса позволяют управлять тем, кому предоставляется доступ к сетевым папкам, и уровнем предоставляемого доступа. Перемещать стандартные папки общего доступа не требуется.
- **Общий доступ через папку Общие (Public).** Общий доступ предоставляется к файлам, размещаемым на компьютере в папке *%SystemDrive%*\Пользователи\Общие (*%SystemDrive%*\Users\Public). Пользователи и группы, которым предоставляется доступ, а также их уровень доступа определяется правами доступа папки Общие. При помещении файлов в папку Общие этим файлам присваиваются такие же права, какие имеет эта папка, а также некоторые дополнительные права. Подробную информацию по этому вопросу *см. в разд. "Использование общих папок и настройка доступа к ним" далее в этой главе*.

> ***Примечание***
>
> В случае общего доступа к обычным папкам локальные пользователи не получают автоматического доступа ни к каким хранящимся на компьютере данным. Локальный доступ к файлам и папкам полностью управляется параметрами безопасности локального диска. Если локальный диск имеет файловую систему FAT, повысить уровень защиты файлов и папок можно, присваивая им атрибуты "Только чтение", "Скрытый" или "Архивный", но ограничить доступ к ним нельзя. В случае же локального диска, отформатированного под NTFS, доступом к папкам и файлам на нем можно управлять на уровне отдельных пользователей и групп пользователей.
>
> А доступ к ресурсам в папке Общие разрешается любому локальному пользователю, независимо от типа его учетной записи, будь то администратор или обычный пользователь. К папке Общие также может быть разрешен сетевой доступ, но в таком случае ее содержимое будет доступно любому, кто может подключиться к данному компьютеру по сети.

Операционная система Windows Server 2012 добавляет дополнительные уровни безопасности посредством использования составных удостоверений (compound identity), управления доступом на основе утверждений (claims-based access control) и централизованных политик доступа (central access policy). В Windows 8 и Windows Server 2012 файлам и папкам на томах NTFS можно присваивать элементы управления доступом на основе утверждений. В Windows Server 2012 пользователям предоставляется доступ к файлам и папкам либо непосредственно — с помощью прав доступа и разрешений для общего ресурса, либо косвенно — с помощью элементов управления доступом на основе утверждений и централизованных политик доступа.

В отличие от более ранних версий Windows, в которых одновременно можно было применять только одну из этих двух моделей общего доступа, на компьютерах под управлением Windows 8 можно одновременно применять обе модели. Основным преимуществом стандартного общего доступа является то, что пользователи могут иметь общий доступ к любой папке компьютера без необходимости перемещать файлы или папки с их текущего местонахождения. А папка Общие, с другой стороны, представляет собой публичную доску объявлений. При включенной функциональности папки Общие, все пользователи как локального компьютера, так и других компьютеров сети могут помещать в нее файлы и папки, которые могут просматриваться всеми другими пользователями как данного компьютера, так и всех компьютеров сети.

Контекстное меню для папок Проводника Windows содержит следующие две опции:

- **Включить в библиотеку** (Include in library). Создает ссылку на данную папку и ее содержимое в указанной папке библиотеки пользователя. Это позволяет пользователю

просматривать и работать с содержимым данной папки, как будто бы она является частью указанной папки библиотеки. Но при этом не следует забывать, что при обращении к такой папке через ее ссылку в библиотеке пользователь в действительности обращается к ее содержимому в исходном местонахождении папки.

- **Общий доступ** (Share with). Предоставляется общий доступ к стандартной папке указанной пользователям. В домашней группе пользователи могут предоставить общий доступ к папке только для чтения или для чтения и записи любому другому члену домашней группы. В рабочей группе или домене пользователь также имеет опцию предоставления доступа к папке другим определенным пользователям. В сетевой среде любого типа пользователь также может выбрать опцию **Прекратить общий доступ** (Stop sharing), которая отменяет общий доступ к папке.

Настройки общего доступа по умолчанию зависят от членства компьютера в сети определенного типа. При создании или подключении к домашней группе указываются типы файлов библиотеки, к которым предоставляется общий доступ, а также предоставлять ли общий доступ к принтерам и устройствам. Компьютеры, которые принадлежат к одной домашней группе, имеют автоматический доступ к файлам библиотек других компьютеров, к которым предоставлен общий доступ.

В домашней группе процедура предоставления общего доступа только для просмотра или для просмотра и изменения довольно простая:

1. В Проводнике Windows щелкните правой кнопкой мыши на требуемой папке.
2. В контекстном меню выберите команду **Общий доступ**, а во вложенном меню — команду **Домашняя группа (просмотр)** (Homegroup (view)) или **Домашняя группа (просмотр и изменение)** (Homegroup (view and edit).

Этот простой способ предоставления общего доступа к ресурсам может показаться привлекательным пользователям. Но при всей своей простоте, этот подход также предоставляет большую свободу действий с данными пользователя и обычно не рекомендуется для применения в рабочей среде. Поэтому пользователям следует настоятельно рекомендовать предоставлять доступ к своим данным не всем, а только определенным другим пользователям. В рабочих группах и доменах общий доступ можно предоставлять только конкретным пользователям.

Процедура для этого следующая:

1. В Проводнике Windows щелкните правой кнопкой мыши на требуемой папке.
2. В контекстном меню выберите команду **Общий доступ**, а во вложенном меню — команду **Отдельные люди** (Specific people). Запустится мастер **Общий доступ к файлам**. По умолчанию владельцем ресурса, к которому предоставляется общий доступ, указана локальная группа **Администраторы**, а текущему пользователю предоставлен доступ на чтение и запись.
3. Используя предоставленные в мастере общего доступа к файлам опции, выберите пользователей, которым следует предоставить общий доступ к данному ресурсу. Например, чтобы предоставить общий доступ всем локальным пользователям данного компьютера, введите в текстовое поле слово `Пользователи` (Users) и нажмите кнопку **Добавить**. Предоставление общего доступа группе **Пользователи** не равнозначно предоставлению общего доступа группе **Все** (Everyone), т. к. членами группы **Все** являются все пользователи, имеющие право доступа к данному компьютеру, а не только локальные или доменные пользователи.
4. По умолчанию предоставляется общий доступ только для чтения. Чтобы предоставить общий доступ для пользователя или группы, щелкните в списке на имени пользователя или группы и в контекстном меню выберите команду **Чтение** или **Чтение и запись**.

5. Выбрав пользователей и указав требуемый уровень общего доступа для них, нажмите кнопку **Общий доступ** (Share), а в следующем окне — кнопку **Готово**.

Отменить общий доступ к папке можно следующим образом:

1. В Проводнике Windows щелкните правой кнопкой мыши на требуемой папке.
2. В контекстном меню выберите команду **Общий доступ**, а во вложенном меню — команду **Прекратить общий доступ** (Stop sharing).
3. В мастере общего доступа к файлам выберите **Прекратить общий доступ**.

По умолчанию при первом предоставлении стандартного доступа к папке Windows создает в брандмауэре Windows исключение на общий доступ к файлам и принтерам. Это входящее исключение позволяет трафику, отправляемому по протоколу SMB другими компьютерами сети, проходить через брандмауэр Windows к общему ресурсу. Чтобы разрешить этот трафик, Windows открывает следующие порты:

- UDP-порт 137, который используется для разрешения имен NetBIOS;
- UDP-порт 138, который используется для передачи и приема дейтаграмм NetBIOS;
- TCP-порт 139, который используется для службы сеансов NetBIOS;
- динамические порты для протоколов ICMPv4 и ICMPv5 (которые используются для запросов отклика, если применимо).

Таков, вкратце, принцип работы предоставления общего доступа к стандартным папкам. Далее в этой главе будет более подробно рассмотрено предоставление общего доступа отдельным пользователям. Но прежде чем кто-либо может начать предоставлять общий доступ к чему-либо, необходимо включить на компьютере возможность общего сетевого доступа.

Параметры общего сетевого доступа служат для предоставления соответствующего уровня безопасности для каждой категории сети, к которой может подключаться компьютер. По этой причине Windows содержит отдельный сетевой профиль для каждого типа сети, используемой компьютером. В общем, большинство параметров сетевого обнаружения и общего доступа по умолчанию отключено. Настроить параметры сетевого обнаружения и общего доступа можно так:

1. В разделе **Сеть и Интернет** Панели управления щелкните по ссылке **Выбор параметров домашней группы и общего доступа к данным** (Choose homegroup and sharing options), а затем по ссылке **Изменить дополнительные параметры общего доступа** (Change advanced sharing settings).
2. Откроется страница **Изменение параметров общего доступа для различных сетевых профилей** (Change sharing options for different network profiles), содержащая отдельную панель управления с конфигурационными параметрами для каждого доступного сетевого профиля. Для работы с требуемым сетевым профилем разверните соответствующую панель, нажав кнопку в виде кружка с направленным вниз треугольником внутри него справа от панели.
3. Функциональность **Сетевое обнаружение** (Network discovery), которая доступна для частных, общедоступных и доменных сетей, позволяет компьютеру обнаруживать другие компьютеры и устройства в сети и наоборот. Эта функциональность включается или отключается установкой соответствующего переключателя.
4. Функциональность **Общий доступ к файлам и принтерам** (File and printer sharing), которая доступна для частных, общедоступных и доменных сетей, управляет общим доступом к файлам и принтерам компьютера. Включите или выключите эту функциональность, установив соответствующий переключатель.

5. В сетевом профиле **Все сети** (All Networks) функциональность **Общий доступ к общедоступным папкам** (Public folder sharing) управляет предоставлением общего доступа к файлам в папках Общие компьютера. Включите или отключите эту функциональность, установив соответствующий переключатель.
6. Функциональность **Потоковая передача мультимедиа** (Media streaming) сетевого профиля **Все сети** управляет предоставлением общего доступа к музыке, видео и изображениям на данном компьютере другим компьютерам сети, а также доступом данного компьютера к ресурсам данного типа на других компьютерах сети. Настройте эту функциональность, щелкнув по ссылке **Выберите параметры потоковой передачи мультимедиа** (Choose media streaming options) и задав в следующем окне требуемые значения параметров. Прослушивание пользователями музыки или просмотр видео и изображений с других компьютеров может отрицательно сказаться на производительности локального компьютера, поэтому желательно не задействовать эту возможность.
7. Для обеспечения безопасности передаваемых общих данных Windows применяет шифрование. По умолчанию в большинстве конфигураций установлен 128-битный уровень шифрования. Но следует проверить, что все компьютеры и устройства, которым предоставляется общий доступ, поддерживают этот уровень шифрования. В противном случае установите более низкий уровень шифрования или же обновите поддержку шифрования на других компьютерах и устройствах.
8. В рабочих и домашних группах функциональность **Общий доступ с парольной защитой** (Password protected sharing) разрешает доступ к общим ресурсам только пользователям, имеющим на локальном компьютере учетную запись с паролем. Включите или выключите эту функциональность, установив соответствующий переключатель.
9. Установив требуемые параметры, нажмите кнопку **Сохранить изменения**, чтобы сохранить их и закрыть окно настройки параметров общего доступа.

В групповой политике можно запретить присоединение компьютеров к рабочей группе, включив параметр политики **Запретить присоединение компьютера к домашней группе** (Prevent the computer from joining a homegroup). Этот параметр находится в узле **Конфигурация компьютера\Административные шаблоны\Компоненты Windows\Домашняя группа** редактора локальной групповой политики.

В групповой политике также можно накладывать ограничения на общий доступ. Ключевое ограничение на использование общего доступа устанавливается в параметре политики **Запретить пользователям в их профиле предоставлять общий доступ к файлам** (Prevent users from sharing files within their profile). Этот параметр находится в узле редактора групповой политики **Конфигурация пользователя\Административные шаблоны\Компоненты Windows\Общий сетевой доступ** и управляет предоставлением общего доступа к папкам, связанным с профилем пользователей, в основном к папке *%SystemDrive%*\Пользователи. При работе с параметром **Запретить пользователям в их профиле предоставлять общий доступ к файлам** нужно иметь в виду следующее.

- Когда этот параметр имеет значение **Не задано** (которое является значением по умолчанию), пользователям разрешается предоставлять другим пользователям сети общий доступ к файлам в папках своего профиля, при условии, что один из пользователей компьютера с правами администратора согласится на предоставление общего доступа. Чтобы согласиться на предоставление общего доступа администратору нужно только предоставить общий доступ к файлу в одной из папок своего профиля.
- Когда этот параметр включен, пользователи не смогут предоставлять общий доступ к папкам своего профиля посредством мастера общего доступа к файлам, который не будет предоставлять общий доступ к подпапкам папки *%SystemDrive%*\Пользователи.

- Когда этот параметр выключен (что может потребоваться для замены унаследованного включенного состояния), пользователям разрешается предоставлять другим пользователям сети общий доступ к файлам в папках своего профиля при условии, что один из пользователей компьютера с правами администратора согласится на предоставление общего доступа.
- Настройка параметра **Запретить пользователям в их профиле предоставлять общий доступ к файлам** в редакторе групповой политики выполняется следующим образом:
  - В редакторе управления групповыми политиками откройте для редактирования требуемый объект групповой политики. Далее разверните узел **Конфигурация пользователя\Административные шаблоны\Компоненты Windows\Общий сетевой доступ**.
  - Дважды щелкните на параметре **Запретить пользователям в их профиле предоставлять общий доступ к файлам**.
  - В открывшемся диалоговом окне установите переключатель **Включить** или **Отключить**, после чего нажмите кнопку **OK**.

Хотя подход с предоставлением общего доступа к папкам **Общие** может выглядеть привлекательным, для большинства организаций, включая малые предприятия, рекомендуется предоставлять доступ к любым данным организации посредством предоставления общего доступа к обычным папкам. Это объясняется тем простым фактом, что предоставление общего доступа к стандартным папкам обеспечивает лучшую защищенность, т. к. вместо полного доступа кому угодно к данным, что имеет место при общем доступе к папкам **Общие**, при этом подходе доступ к данным получают только пользователи, имеющие соответствующие разрешения. Повышенная безопасность является обязательным условием защиты одного из самых ценных активов организации — ее данных.

Разрешения для общего ресурса применяются только тогда, когда пользователь пытается получить доступ к файлу или папке другого компьютера по сети, а полномочия доступа применяются всегда, будь то при локальном входе пользователя в систему или при обращении к файлу или папке с удаленной системы по сети. При удаленном обращении к данным сначала применяются разрешения для общего ресурса, а затем полномочия доступа.

Полномочия доступа и разрешения для общего доступа к стандартным папкам во многих отношениям подобны оболочкам для данных. Первая оболочка — полномочия доступа к файлам — защищает данные на локальном уровне. При попытке получить доступ к данным локальным пользователем доступ предоставляется или запрещается полномочиями доступа. А вторая оболочка — права общего доступа к файлам — защищает данные при удаленном обращении к данным. Если пользователь пытается получить доступ к данным с удаленного компьютера, сначала доступ предоставляется или запрещается правами общего доступа к файлам, после чего вступают в действия полномочия доступа к файлам.

Управление доступом к файлам и папкам посредством разрешений NTFS

При попытке доступа к файлу или папке в файловой системе NTFS-система всегда проверяет полномочия пользователя (или процесса) на доступ к данному ресурсу. Разрешения NTFS довольно сложные, и чтобы разбираться, как управлять ими, необходимо понимать следующие термины.

- **Основные разрешения.** Что собой представляют основные разрешения и как они используются.

- **Разрешения на основе утверждений.** Что собой представляют утверждения пользователей и устройств и как они используются.
- **Особые разрешения.** Что собой представляют особые разрешения и как они используются.
- **Принадлежность файла.** Что означает принадлежность файла и как она используется.
- **Наследование.** Что означает наследование и как оно используется.
- **Действующие разрешения.** Как определить действующие разрешения для файлов.

Основные разрешения и их использование

В Windows 8 владелец файла или папки имеет полномочия разрешить или запретить доступ к данному ресурсу; этим правом также обладают члены группы **Администраторы** и другие санкционированные пользователи. Разрешения и запрещения применяются к пользователю или группе пользователей. Следует иметь в виду, запрещения имеют приоритет над разрешениями. В результате, если пользователь является членом двух разных групп, одной из которых предоставлены определенные права, а другой эти права запрещены, в конечном итоге данные права этому пользователю будут запрещены.

Просмотреть текущие полномочия на файл или папку для определенного пользователя или группы можно в Проводнике Windows. Для этого щелкните на требуемом ресурсе правой кнопкой мыши, в контекстном меню выберите команду **Свойства**, а в окне свойств выберите вкладку **Безопасность** (Security) (рис. 13.1).

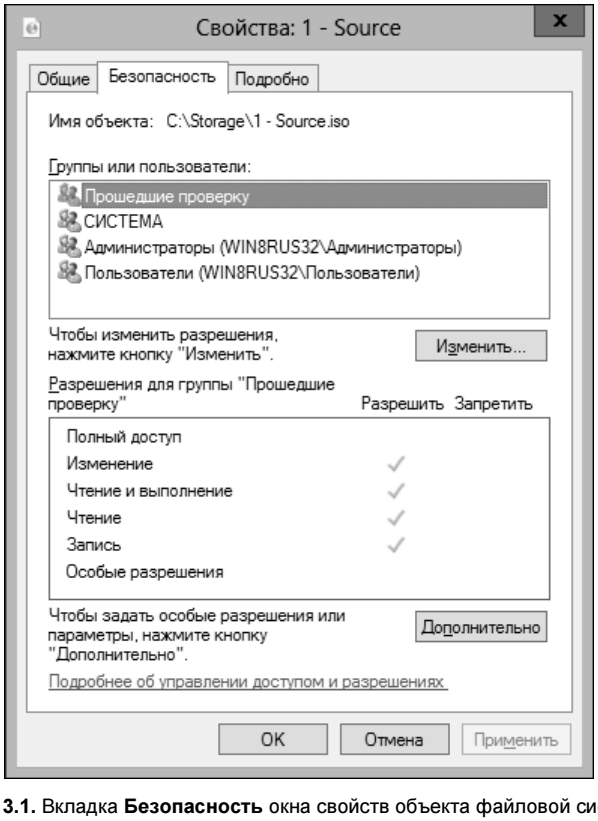


Рис. 13.1. Вкладка **Безопасность** окна свойств объекта файловой системы

Список **Группы или пользователи** содержит перечень групп и пользователей, которым предоставлены полномочия на данный ресурс, а при выборе в этом списке группы или пользователя их полномочия отображаются в нижней панели **Разрешения для** (Permissions for).

Если разрешения отображаются серым шрифтом, это означает, что они унаследованы от родительской папки (и недоступны для изменения). Тема наследования подробно рассматривается в *разд. "Применения разрешений посредством наследования" далее в этой главе.*

Установка и работа с основными разрешениями

Все разрешения хранятся в файловой системе, как часть списка ACL[1], присвоенного файлу или папке. В табл. 13.1 приведен список и краткое описание основных полномочий, шесть из которых применяются к папкам, а пять также применяются к файлам. Хотя некоторые полномочия наследуются на основе разрешений родительской папки, все разрешения определяются явно на определенном уровне иерархии файловой системы. В таблице разрешения подаются в приблизительном порядке диапазона их полномочий, от **Полный доступ**, предоставляющего наибольшие полномочия, до **Запись** и **Чтение**, предоставляющих особые полномочия.

Таблица 13.1. *Основные разрешения для файлов и папок*

Полномочие	Описание
Полный доступ (Full Control)	Пользователю или группе предоставляется полный доступ к данному ресурсу, включая полномочия на чтение, запись, изменение и удаление файлов и вложенных папок. Пользователь, обладающий правами полного доступа на файл или папку, может изменять разрешения и удалять файлы в папке, независимо от разрешений для этих файлов, а также может становиться владельцем папки или файла. Установка этого разрешения также устанавливает все другие
Изменение (Modify)	Предоставляет пользователю или группе полномочия читать, записывать, изменять или удалять файлы. Пользователь может также создавать файлы и вложенные папки, но не может становиться владельцем файлов. Установка этого разрешения также устанавливает все другие разрешения ниже его
Чтение и выполнение (Read & Execute)	Разрешает просмотр содержимого файла и папки, включая вложенные папки, а также исполнение файлов. Для папок это разрешение наследуется всеми файлами папки и ее вложенными папками. Установка этого разрешения также устанавливает разрешение **Список содержимого папки** и **Чтение**
Список содержимого папки (только для папок) (List Folder Contents)	Подобно разрешению **Чтение и выполнение**, но доступно только для папок. Разрешает просмотр содержимого папки, включая вложенные папки, а также исполнение файлов. В отличие от разрешения **Чтение и выполнение**, это разрешение наследуется вложенными папками, но не файлами папки или ее вложенных папок
Чтение (Read)	Позволяет пользователю или группе просматривать содержимое файла или папки, включая атрибуты и разрешения файла, а также синхронизировать файлы. Для исполнения сценариев требуется только разрешение чтения. Для доступа к ярлыку и его объекта требуется разрешение чтения
Запись (Write)	Разрешает пользователю или группе создавать новые файлы и записывать данные в существующие файлы, а также просматривать атрибуты и разрешения файлов и синхронизировать файлы. Предоставление пользователю прав на запись, но не на удаление файла или папки не может предотвратить удаление им содержимого файла или папки

[1] Access control list — список управления доступом.

Такими же важными, как и основные разрешения, являются пользователи и группы, которым эти разрешения присваиваются. Если пользователь или группа, которым требуется присвоить разрешения, уже находятся в списке **Группы или пользователи** на вкладке **Безопасность**, их разрешения можно изменить. Для этого нужно нажать кнопку **Изменить**, а затем установить или снять флажки требуемых разрешений или запрещений в списке **Разрешения для**. В частности, чтобы добавить разрешения на выполнение определенного действия, нужно установить его флажок в столбце **Разрешить** (Allow), а чтобы отменить разрешение — снять его флажок.

Чтобы явно запретить выполнение определенного действия, нужно установить его флажок в столбце **Запретить** (Deny). Так как запрещенные полномочия имеют приоритет над разрешенными, запрещения могут быть полезными в следующих двух сценариях.

- Если пользователь является членом группы, которой было предоставлено определенное разрешение, но использование этого разрешения нежелательно для данного пользователя, и его нельзя или нежелательно удалить из данной группы, унаследованное от группы разрешение пользователя можно переопределить, запретив ему данное полномочие.
- Если для пользователя или группы нежелательно иметь унаследованное от родительской папки разрешенное полномочие, в большинстве случаев это полномочие для данного пользователя или группы можно явно запретить.

Если список **Группы или пользователи** не содержит пользователей или групп, которым требуется присвоить разрешения, их можно добавить в этот список. Добавить пользователя или группу в список **Группы и пользователи** вкладки **Безопасность** можно следующим образом:

1. На вкладке **Безопасность** окна свойств объекта файловой системы нажмите кнопку **Изменить** (Edit).
2. В открывшемся диалоговом окне **Разрешения для** нажмите кнопку **Добавить**, в результате чего откроется диалоговое окно **Выбор: "Пользователи" или "Группы"** (Select Users or Groups) (рис. 13.2).

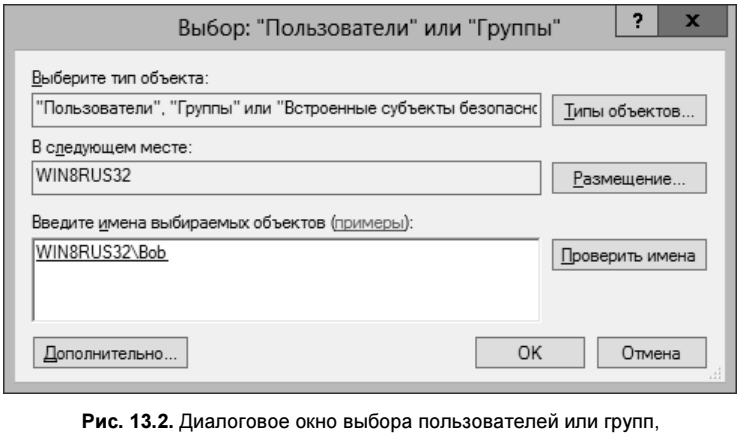


Рис. 13.2. Диалоговое окно выбора пользователей или групп, для которых требуется настроить разрешения

Примечание

В доменной среде это диалоговое окно называется **Выбор: "Пользователи", "Компьютеры", "Учетные записи"**, но имеет точно такое же назначение.

Совет

Всегда внимательно проверьте значение поля **В следующем месте** (From this location). В рабочих группах компьютеры всегда отображают здесь только локальные учетные записи и группы. В доменах содержимое этого поля меняется, а исходное значение установлено, как домен по умолчанию текущего пользователя. Если требуемый пользователь или группа находятся в другом месте, нажмите кнопку **Размещение** (Locations), чтобы отобразить список других расположений, где следует выполнить поиск требуемого пользователя, включая текущий домен, доверенные домены и другие ресурсы, к которым имеется доступ.

3. Введите имя учетной записи пользователя или группы. Вводить нужно именно имя учетной записи пользователя, а не полное имя пользователя. При вводе нескольких пользователей или групп их имена разделяются точкой с запятой.
4. Завершив ввод учетных записей, нажмите кнопку **Проверить имена**. Если для введенной учетной записи система найдет одно совпадение, список диалогового окна автоматически обновится и учетная запись будет подчеркнута. В противном случае появится другое диалоговое окно, **Имя не найдено** (Name not found). Отсутствие совпадений означает, что либо имя было введено неправильно, либо же используется не то размещение. Исправьте имя в диалоговом окне **Имя не найдено** и выполните поиск снова или же нажмите кнопку **Размещение**, чтобы выбрать новое место для поиска. Если для введенного имени система найдет несколько совпадений, которые выводятся в диалоговом окне **Найдено несколько имен** (Multiple Names Found), выберите из них требуемое имя, а затем нажмите кнопку **OK**. Данный пользователь (или группа) будет добавлен в список **Группы или пользователи**.
5. Теперь для добавленного пользователя можно настроить разрешения или запреты полномочий, выбрав его имя в верхней панели и установив или сбросив флажки требуемых разрешений или запрещений в нижней панели.

Специальные учетные записи и рекомендации по установке разрешений

При работе с основными разрешениями важно понимать не только, как они используются, но также то, как использование специальных учетных записей может быть полезным при присвоении разрешений. Наиболее часто используются такие специальные учетные записи, как **Создатель-владелец** (Creator Owner) и **Пользователи** (Users), но иногда встречаются и другие. Наиболее часто используемые специальные учетные записи и их краткое описание приведены в табл. 13.2. Специальные учетные записи автоматически являются членом какой-либо группы. Чтобы настроить разрешения для специальной учетной записи, введите в поле **Группы или пользователи** ее имя, как имя любой другой учетной записи пользователя или группы.

Таблица 13.2. *Специальные учетные записи, используемые при задании разрешений*

Специальная учетная запись	Описание
Анонимный вход (Anonymous Logon)	Охватывает всех сетевых пользователей, для которых нет учетных данных. Данная специальная учетная запись применяется, чтобы разрешить анонимный доступ к ресурсам, наподобие ресурсов, доступных на веб-сервере
Прошедшие проверку (Authenticated Users)	Охватывает пользователей и компьютеры, которые выполняют вход с указанием имени пользователя и пароля. Исключает пользователей, которые выполняют вход по учетной записи **Гость**, даже если эта учетная запись имеет пароль

Таблица 13.2 *(окончание)*

Специальная учетная запись	Описание
Создатель-владелец (Creator Owner)	Специальное обозначение учетной записи, создавшей файл или папку. Windows 8 использует эту группу для обозначения учетной записи, которая обладает максимальными правами на файл или папку
Удаленный доступ (Dialup)	Охватывает всех пользователей, которые осуществляют доступ к компьютеру через коммутированное подключение. Данная учетная запись используется, чтобы отличить таких пользователей от пользователей других типов
Все (Everyone)	Охватывает всех интерактивных, удаленных и прошедших проверку пользователей. Также включает гостей, но не анонимных пользователей
Интерактивные (Interactive)	Охватывает пользователей, выполнивших вход локально или посредством удаленного подключения к рабочему столу
Сеть (Network)	Охватывает всех пользователей, выполняющих вход в систему по сети. Эта учетная запись используется, чтобы позволить удаленным пользователям получить доступ к ресурсу, и не охватывает пользователей, выполняющих интерактивный вход в системы посредством удаленного подключения к рабочему столу
Пользователи (Users)	Охватывает только прошедших проверку и доменных пользователей. Рекомендуется использование встроенной группы **Пользователи** вместо группы **Все**

Четкое понимание этих специальных учетных записей может помочь вам в эффективной настройке разрешений для ресурсов на томах NTFS. Кроме этого, при работе с разрешениями всегда нужно иметь в виду следующие рекомендации.

- **Придерживайтесь системной иерархии.** Наследование играет важную роль в установке разрешений. По умолчанию заданные для папки разрешения применяются ко всем файлам и вложенным папкам этой папки. Имея это в виду, приступайте к настройке разрешений с корневой папки локального диска или папки профиля пользователя (которые играют роль папок высшего уровня).
- **Составьте план работы.** Не приступайте к настройке разрешений, не имея четкого плана действий. В случае рассогласования разрешения папок, возможно, необходимо найти способ начать процесс присвоения разрешений сначала, чтобы обеспечить определенную связность. В таком случае полезно настроить все требуемые разрешения в родительской папке, а затем восстановить разрешения файлов и вложенных папок этой папки, используя подход, рассматриваемый в *разд. "Восстановление наследуемых разрешений" далее в этой главе*.
- **Предоставляйте только необходимый доступ.** Важным аспектом встроенных в NTFS элементов управления доступа к файлам является требование явного назначения разрешений. Если пользователю не предоставлено разрешение и этот пользователь не является членом группы, которая имеет данное разрешение, данный пользователь не имеет этого разрешения. Все предельно просто. Это правило особенно важно иметь в виду при назначении разрешений, т. к. часто предоставить пользователю полный контроль кажется намного проще, чем обдумывать конкретные требуемые разрешения. Принцип предоставления пользователям лишь тех разрешений, которые им необходимы для выполнения их работы, называется *принципом минимальных полномочий* (principle of least privilege).
- **Используйте группы для более эффективного управления разрешениями.** Всегда, когда это возможно, пользователей следует делать членами соответствующих групп, а затем

присваивать разрешения этим группам, а не отдельным пользователям. Таким образом, разрешения новым пользователям присваиваются посредством присвоения им членства в соответствующей группе или группах. Когда же обязанности пользователя меняются, должным образом меняется его членство в группах. Например, когда Дарья начинает работать в отделе продаж, ее можно сделать членом группы SalesUS и SalesCan, чтобы она могла иметь доступ к общим данным этих групп. Если она позже перейдет из отдела продаж в отдел маркетинга, ее можно удалить из первых двух групп и сделать членом групп MarketingUS и MarketingCan. Такой подход намного эффективней, нежели редактирование разрешений для каждой папки, к которой Дарье требуется доступ.

- Используйте централизованные политики доступа для улучшения существующих средств управления доступом. На серверах домена под управлением Windows Server 2012 используйте централизованные политики доступа для точного и аккуратного определения конкретных атрибутов, которыми должны обладать пользователи и устройства, чтобы получить доступ к ресурсам.

Присвоение особых разрешений

Для точного управления разрешениями пользователей и групп в Windows 8 используются специальные разрешения. При любой работе с основными разрешениями Windows 8 негласно использует связанных специальных полномочий, которые точно определяют разрешенные действия. Далее приведен список основных разрешений и составляющие их специальные разрешения:

- **Чтение** (Read):
  - **Содержание папки / Чтение данных** (List folder / read data);
  - **Чтение атрибутов** (Read attributes);
  - **Чтение дополнительных атрибутов** (Read extended attributes);
  - **Чтение разрешений** (Read permissions);
- **Чтение и выполнение** (Read & execute) или **Список содержимого папки** (List folder contents):
  - все специальные разрешения для **Чтение**;
  - **Траверс папок / выполнение файлов** (Traverse folder / execute file);
- **Запись** (Write):
  - **Создание файлов / Запись данных** (Create files / write data);
  - **Создание папок / Дозапись данных** (Create folders / append data);
  - **Запись атрибутов** (Write attributes);
  - **Запись дополнительных атрибутов** (Write extended attributes);
- **Изменение** (Modify):
  - все специальные разрешения для **Чтение**;
  - все специальные разрешения для **Запись**;
  - **Удаление** (Delete);
- **Полный доступ** (Full control):
  - все ранее перечисленные специальные разрешения;
  - **Смена разрешений** (Change permissions);

- **Удаление подпапок и файлов** (Delete subfolders and files);
- **Смена владельца** (Take ownership).

В табл. 13.3 описано, как Windows 8 использует каждое специальное разрешение.

Таблица 13.3. *Специальные разрешения для файлов и папок и их использование в Windows 8*

Специальное разрешение	Описание
Смена разрешений	Предоставляет полномочия на изменение основных и специальных разрешений файла или папки
Создание файлов / Запись данных	Разрешение **Создание файлов** предоставляет полномочия на помещение файлов в папку. Разрешение **Запись данных** позволяет заменять данные в файле (но не добавлять новые данные в существующем файле, для чего нужно разрешение **Дозапись данных**)
Создание папок / Дозапись данных	Разрешение **Создание папок** предоставляет права на создание в папке вложенных папок, а разрешение **Дозапись данных** позволяет добавлять данные в конец существующего файла (но не заменять существующие данные файла, для чего требуется разрешение **Запись данных**)
Удаление	Позволяет удалять файл или папку. Если папка не пустая и пользователь не имеет разрешения **Удаление** для одного или нескольких ее файлов или подпапок, удаление будет невозможным, если только пользователь не имеет разрешения **Удаление подпапок и файлов**
Удаление подпапок и файлов	Предоставляет права на удаление содержимого папки. С этим разрешением можно удалять подпапки и файлы папки, даже если для них нет явного разрешения **Удаление**
Содержание папки / Чтение данных	Разрешение **Содержание папки** предоставляет право просматривать список подпапок и файлов папки, а разрешение **Чтение данных** — просматривать содержимое файла
Чтение атрибутов	Позволяет просматривать основные атрибуты файла или папки — **Только чтение**, **Скрытый**, **Системный** и **Архивный**
Чтение дополнительных атрибутов	Предоставляет полномочия на просмотр дополнительных атрибутов (которые называются *потоками данных* — data streams), связанных с файлом
Чтение разрешений	Допускает просмотр основных и специальных разрешений файла или папки
Смена владельца	Позволяет становиться владельцем файла или папки. По умолчанию администраторы всегда могут стать владельцем файла или папки, а также могут предоставлять это полномочие другим
Траверс папок / Выполнение файлов	Разрешение **Траверс папок** предоставляет прямой доступ к папке для доступа к ее подпапкам, даже при отсутствии явного разрешения на чтение содержимого папки. Разрешение **Выполнение файлов** позволяет выполнять исполняемые файлы
Запись атрибутов	Позволяет изменять основные атрибуты файла или папки — **Только чтение**, **Скрытый**, **Системный** и **Архивный**
Запись дополнительных атрибутов	Предоставляет полномочия на изменение дополнительных атрибутов (которые называются *потоками данных*), связанных с файлом

Просмотреть специальные разрешения для файла или папки можно в Проводнике Windows. Для этого щелкните правой кнопкой мыши на нужном файле или папке и в контекстном

меню выберите команду **Свойства**. В открывшемся окне свойств объекта перейдите на вкладку **Безопасность**, а на ней нажмите кнопку **Дополнительно**. В результате откроется диалоговое окно **Дополнительные параметры безопасности** (Advanced Security Settings).

В этом диалоговом окне разрешения отображаются по большому счету таким же образом, как и на вкладке **Безопасность**. Ключевая разница состоит в том, что здесь можно видеть отдельные наборы разрешения и запрещения полномочий, состояние наследования этих разрешений (и запрещений), а также ресурсы, к которым эти разрешения применяются.

Дополнительная информация

На рис. 13.3 обратите внимание, что владельцем папки является неизвестная учетная запись, которая обозначается идентификатором GUID, а не именем пользователя. В Windows 8 это обычно означает, что файл (или папка) был создан пользователем в другой операционной системе компьютера, как в случае компьютера с возможностью загрузки двух разных операционных систем.

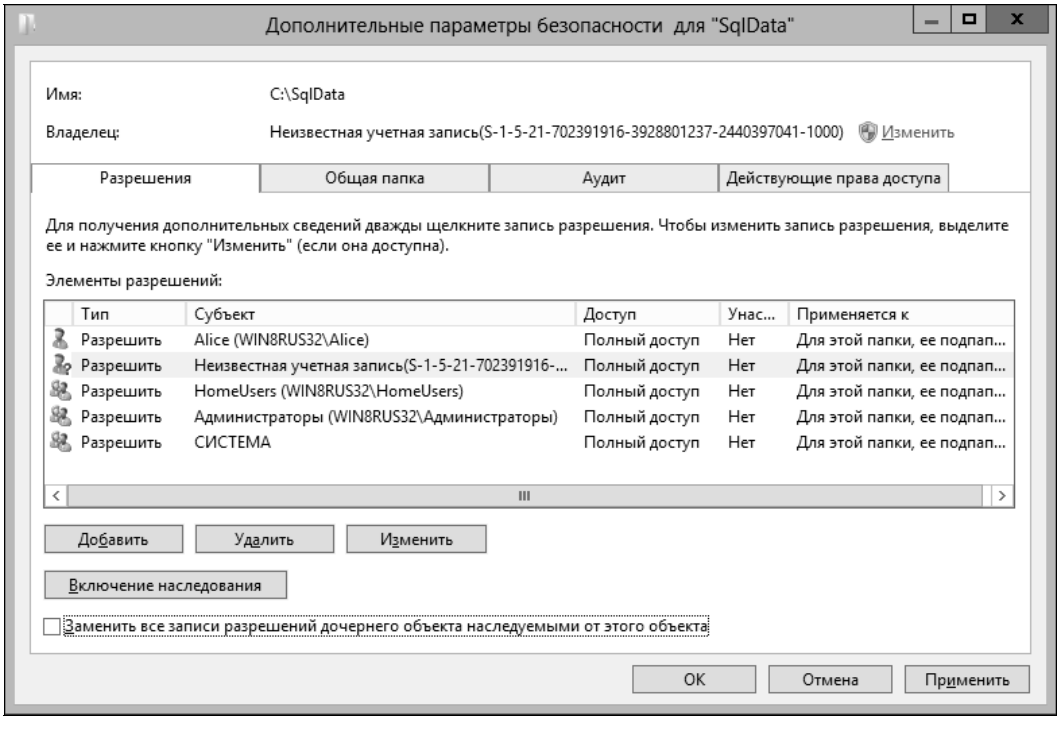


Рис. 13.3. Диалоговое окно **Дополнительные параметры безопасности** для настройки специальных разрешений

В диалоговом окне **Дополнительные параметры безопасности** специальные разрешения для участника системы безопасности можно задавать следующим образом:

1. Если пользователь или группа уже имеет набор разрешений для файла или папки, эти разрешения можно просмотреть или изменить, нажав кнопку **Изменить** (Edit), а затем перейти к шагу 6.
2. Нажмите кнопку **Добавить**, в результате чего откроется диалоговое окно **Элемент разрешения для** (Permission Entry for). Щелкните в этом окне по ссылке **Выберите субъект**

(Select a principal), в результате чего откроется диалоговое окно **Выбор: "Пользователь" или "Группа"** (Select User or Group).

3. Введите имя учетной записи пользователя или группы. Вводить нужно именно имя учетной записи пользователя, а не полное имя пользователя. Кроме этого, вводить можно только одно имя за раз.
4. Нажмите кнопку **Проверить имена**. Если для введенной учетной записи система найдет одно совпадение, список диалогового окна автоматически обновится и учетная запись будет подчеркнута. В противном случае выводится другое диалоговое окно. Отсутствие совпадений означает, что или имя было введено неправильно, или же используется не то размещение. Исправьте имя в диалоговом окне **Имя не найдено** и выполните поиск снова либо нажмите кнопку **Размещение**, чтобы выбрать новое место для поиска. Ели для введенного имени система найдет несколько совпадений, которые выводятся в диалоговом окне **Найдено несколько имен**, выберите из них требуемое имя, а затем нажмите кнопку **OK**.
5. Нажмите кнопку **OK**. Выбранный пользователь (или группа) добавится как **Субъект**, что отображается в диалоговом окне **Элемент разрешения для**.
6. По умолчанию это окно содержит список только основных разрешений. Щелчок по ссылке **Отображение дополнительных разрешений** (Show advanced permissions) выводит в панели **Разрешения** список специальных разрешений (рис. 13.4).

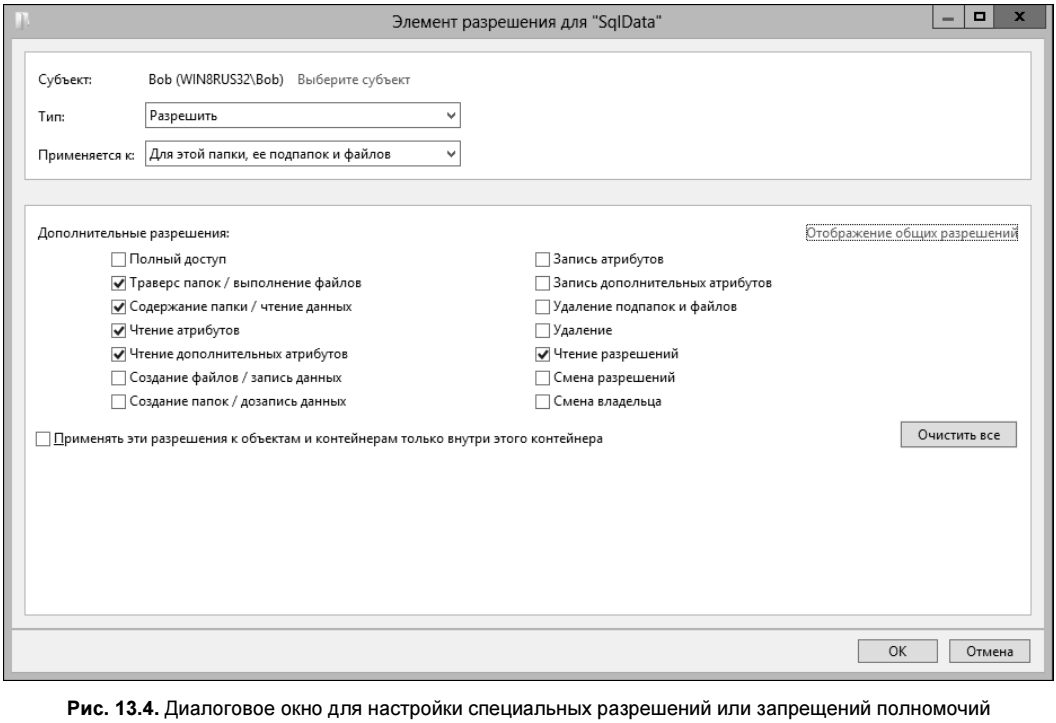


Рис. 13.4. Диалоговое окно для настройки специальных разрешений или запрещений полномочий

7. В раскрывающемся списке **Тип** выберите тип задаваемых полномочий — разрешаемые или запрещаемые — после чего установите флажки требуемых специальных полномочий. Недоступные для редактирования разрешения (отображаемые серым шрифтом) унаследованы от родительской папки.

Примечание

Специальные полномочия разрешаются и запрещаются отдельно. Поэтому, если требуется задать как разрешенные, так и запрещенные полномочия, нужно настроить разрешения полномочий, а затем повторить эту процедуру, начиная с шага 1, и настроить запрещения полномочий.

8. Если доступны опции выпадающего списка **Применяется к** (Applies to), выберите в этом списке требуемую опцию, чтобы обеспечить правильное наследование полномочий. Значения этих опций таковы:
   - **Только для этой папки** (This folder only) — полномочия применимы только для текущей папки;
   - **Для этой папки, ее подпапок и файлов** (This folder, subfolders and files) — полномочия применяются к текущей папке и всем ее подпапкам и файлам, как в текущей папке, так и в ее подпапках;
   - **Для этой папки и ее подпапок** (This folder and subfolders) — полномочия применяются к текущей папке и ко всем ее подпапкам, но не к файлам в этих папках;
   - **Для этой папки и ее файлов** (This folder and files) — полномочия применяются к текущей папке и ко всем ее файлам, но не к ее подпапкам;
   - **Только для подпапок и файлов** (Subfolders and files only) — полномочия применяются ко всем подпапкам и всем файлам в этих папках, но не к самой текущей папке;
   - **Только для папок** (Subfolders only) — полномочия применяются ко всем подпапкам текущей папке, но не к самой папке и не к файлам в этих папках;
   - **Только для файлов** (Files only) — полномочия применяются ко всем файлам текущей папки и ко всем файлам ее подпапок, но не к самой текущей папке и не ее подпапкам.
9. Завершив настройку полномочий, нажмите кнопку **OK**, чтобы применить и сохранить их.

Присвоение разрешений на основе утверждений

Для управления доступом к ресурсам элементы управления доступом на основе утверждений используют составные удостоверения. При удаленном доступе к ресурсам элементы управления доступом на основе утверждений и централизованные политики доступа используют защиту Kerberos для проверки утверждений устройств. Защита Kerberos повышает уровень доменной безопасности, разрешая присоединенным к домену клиентам и контроллерам домена взаимодействовать по безопасным, зашифрованным каналам связи.

Самым простым подходом к созданию утверждения будет определить ограничивающие доступ условия на основе групп, к которым пользователь или устройство может принадлежать или не принадлежать. Более продвинутые методы состоят в использовании прав доступа, типов утверждений и свойств ресурсов, чтобы можно было тщательно определить конкретные критерии, которые нужно удовлетворить, с целью получить доступ.

Иными словами, утверждения определяют конкретные атрибуты, которыми пользователи и устройства должны обладать, чтобы получить доступ к файлу или папке. Например, в случае основных утверждений на основе группового членства можно указать следующее.

- Пользователь (или устройство) может быть членом любой группы, указанной в утверждении. Например, устройство может быть членом группы **Engineering Computers**.
- Пользователь (или устройство) должен быть членом каждой группы, указанной в утверждении. Например, устройство должно быть членом группы **Engineering Computers** и группы **Restricted Access**.

- Пользователь (или устройство) не может быть членом какой-либо группы, указанной в утверждении. Например, устройство не может быть членом группы **Temp Computers**.
- Пользователь (или устройство) не должен быть членом никакой группы, указанной в утверждении. Например, устройство не может быть членом группы **Temp Computers** и группы **Contract Computers**.

> ***Дополнительная информация***
>
> При использовании централизованных политик доступа в службе каталогов Active Directory определяются централизованные правила доступа, которые затем применяются динамически для всех компьютеров организации. В централизованных правилах доступа используются условные выражения, которые требуют определения свойств ресурса, типов утверждений и/или групп безопасности, требуемых политикой, а также серверов, на которых данная политика должна применяться.

Прежде чем можно определять и применять условия утверждений к файлам и папкам компьютера, необходимо включить политику на основе утверждений. Для компьютеров, которые не являются членами домена, это можно сделать, включив и настроив параметр **Поддержка KDC требований, комплексной проверки подлинности и защиты Kerberos** (KDC support for claims, compound authentication and Kerberos armoring), который находится в узле **Конфигурация компьютера\Административные шаблоны\Система\Центр распространения ключей** (Computer Configuration\Administrative Templates\System\KDC). Данный параметр необходимо настроить для использования одного из следующих режимов.

- **Поддерживается.** Контроллеры доменов поддерживают утверждения, составные удостоверения и защиту Kerberos. Может осуществляться проверка подлинности компьютеров, не поддерживающих защиту Kerberos.
- **Всегда предоставлять утверждения.** То же самое, что и поддерживаемый режим, но контроллеры домена всегда возвращают утверждения для учетных записей.
- **Отклонять запросы проверки подлинности без защиты.** Защита Kerberos является обязательной. Проверка подлинности компьютеров, не поддерживающих защиту Kerberos, не может выполняться.

Чтобы обеспечить единообразное применение политики по всему домену, политику на основе утверждений необходимо включить для всех контроллеров домена. Для этого данная политика обычно включается и настраивается через объект групповой политики **Default Domain Controllers Policy** или через наивысший объект групповой политики, связанный с организационной единицей контроллеров домена.

Управление запросами утверждений и комплексной проверкой подлинности для клиентов Kerberos на компьютерах под Windows 8 и Windows Server 2012 выполняется посредством параметра политики **Поддержка клиентами Kerberos требований, комплексной проверки подлинности и защиты Kerberos** (Kerberos client support for claims, compound authentication and Kerberos armoring). Этот параметр нужно включить, чтобы совместимые клиенты Kerberos могли запрашивать утверждения и комплексную проверку подлинности для динамического контроля доступа и защиты Kerberos. Этот параметр находится в узле редактора объекта групповой политики **Конфигурация компьютера\Административные шаблоны\Система\Kerberos**.

Включив и настроив политику на основе утверждений, условия утверждений можно определить следующим образом:

1. В Проводнике Windows щелкните правой кнопкой мыши на требуемой папке или файле и в контекстном меню выберите команду **Свойства**. В открывшемся окне свойств объекта перейдите на вкладку **Безопасность**, а на ней нажмите кнопку **Дополнительно**.

В результате откроется диалоговое окно **Дополнительные параметры безопасности** (см. рис. 13.3).

2. Если пользователь уже имеет набор разрешений для данного объекта, эти разрешения можно просмотреть или редактировать. Для этого выберите необходимого пользователя, нажмите кнопку **Изменить** и перейдите к шагу 7.
3. Нажмите кнопку **Добавить**, в результате чего откроется диалоговое окно **Элемент разрешения для**. Щелкните в этом окне по ссылке **Выберите субъект**, в результате чего откроется диалоговое окно **Выбор: "Пользователь" или "Группа"**.
4. Введите имя учетной записи пользователя или группы. Вводить нужно именно имя учетной записи пользователя, а не полное имя пользователя. Кроме этого, вводить можно только одно имя за раз.
5. Нажмите кнопку **Проверить имена**. Если для введенной учетной записи система найдет одно совпадение, список диалогового окна автоматически обновится и учетная запись будет подчеркнута. В противном случае появится другое диалоговое окно. Отсутствие совпадений означает, что или имя было введено неправильно, или же используется не то размещение. Исправьте имя в диалоговом окне **Имя не найдено** и выполните поиск снова либо нажмите кнопку **Размещение**, чтобы выбрать новое место для поиска. Если для введенного имени система найдет несколько совпадений, которые выводятся в диалоговом окне **Найдено несколько имен**, выберите из них требуемое имя, а затем нажмите кнопку **OK**.
6. Нажмите кнопку **OK**. Данный пользователь или группа будут добавлены как **Субъект**. Щелкните по ссылке **Добавить условие** (Add a condition).
7. С помощью предоставленных опций определите условие или условия, которые должны быть соблюдены для предоставления доступа. Для пользователей и групп задайте основные утверждения на основе группового членства, ранее определенного утверждения или обоих. Для свойств ресурсов определите условия для значений свойств.
8. Завершив настройку условий, нажмите кнопку **OK**, чтобы применить и сохранить их.

Присвоение разрешений и владения файлам

Владелец файла или папки имеет право разрешать или запрещать доступ к данному ресурсу. Хотя члены группы **Администраторы** и другие санкционированные пользователи также имеют право разрешать или запрещать доступ, владелец имеет полномочия заблокировать пользователей, которые не являются администраторами, после этого восстановить доступ к ресурсу можно будет, если сделать администратора или члена группы операторов восстановления владельцем ресурса. Это обстоятельство делает владельца файла или папки ответственным за решения, какие полномочия разрешаются и запрещаются для данного ресурса.

Владельцем файла или папки по умолчанию является пользователь, создавший данный ресурс. Владение объектом можно принимать или передавать несколькими разными способами. Текущий владелец файла или папки может передать владение им другому пользователю или группе. Член группы **Администраторы** может стать владельцем файла или папки либо передать владение объектом другому пользователю или группе, даже если текущие разрешения объекта не предоставляют администраторам никаких полномочий. Любой пользователь, обладающий разрешением **Смена владельца** для файла или папки, может стать владельцем данного объекта, как и любой член группы **Операторы архива** (или и любой другой пользователь с полномочиями **Восстановление файлов и каталогов** (Restore files and directories)).

Присвоить владение файла или папки можно следующим образом:

1. В Проводнике Windows щелкните на требуемом объекте правой кнопкой мыши и в контекстном меню выберите команду **Свойства**.
2. На вкладке **Безопасность** окна свойств нажмите кнопку **Дополнительно**, в результате чего откроется диалоговое окно **Дополнительные параметры безопасности**, в верхней части которого имя владельца указано под именем объекта.
3. Щелкните по ссылке **Изменить** справа от имени владельца. В открывшемся диалоговом окне **Выбор: "Пользователь" или "Группа"** выберите нового владельца объекта. При смене владельца папки новому владельцу также можно присвоить владение всех подпапок и файлов этой папки, установив флажок **Заменить владельца подконтейнеров и объектов** (Replace owner of subcontainers and objects) (рис. 13.5).
4. Завершив смену владельца объекта, нажмите кнопку **OK**, чтобы сохранить настройки и закрыть диалоговое окно.

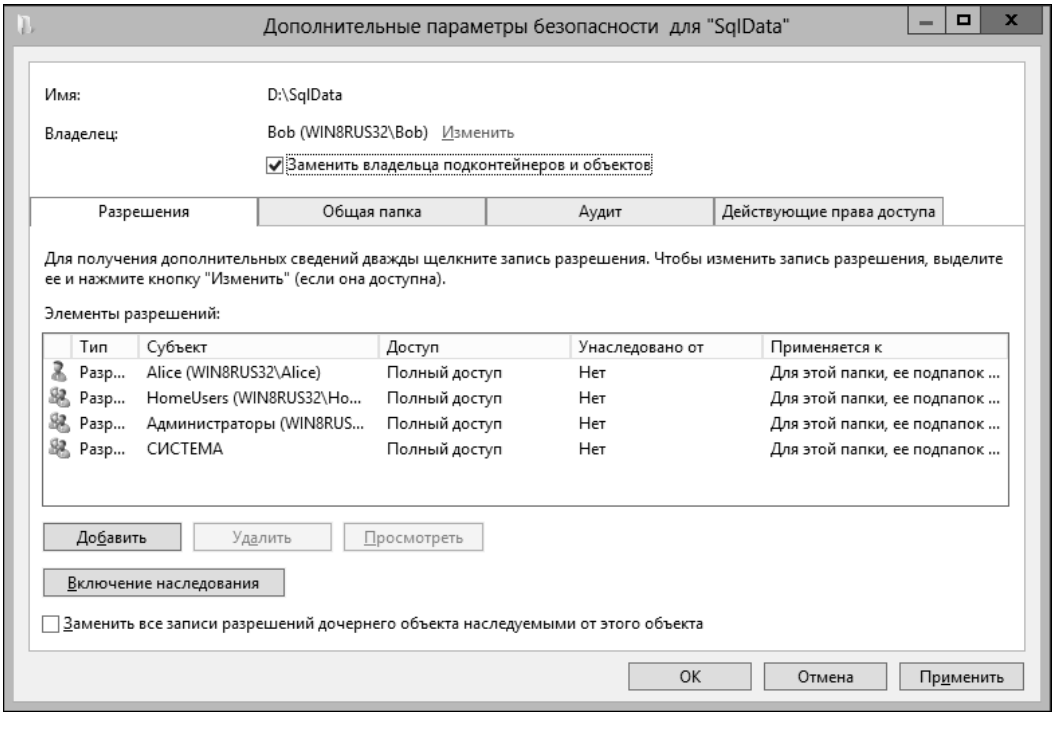


Рис. 13.5. Смена владельца папки или файла

Применения разрешений посредством наследования

В используемой в Windows иерархии файловой системы корневая папка локального диска и папка *%UserProfile%* по умолчанию являются родительскими папками всех своих вложенных папок. Любой добавленный в эти папки ресурс наследует разрешения корневой папки локального диска или папки профиля пользователя. Это поведение можно изменить, модифицировав параметры наследования папки, чтобы она больше не наследовала разрешений своей родительской папки. Эта процедура создает новую родительскую папку, и все добавляемые подпапки и файлы будут тогда наследовать разрешения этой папки.

Основы наследования

Наследование является автоматическим процессом, а наследуемые разрешения присваиваются при создании файла или папки. Если нежелательно, чтобы файл или папка наследовали разрешения родительской папки, это можно осуществить одним из следующих способов:

- прекратить наследование разрешений с родительской папки, а затем либо удалить все унаследованные разрешения, либо преобразовать их в явные разрешения;
- выбрать родительскую папку, а затем настроить разрешения для содержащихся в ней файлов и папок;
- попытаться заменить наследуемое полномочие, установив противоположное полномочие. В большинстве случаев **Запретить** преобладает над **Разрешить**.

На вкладке **Безопасность** диалогового окна свойств объекта унаследованные полномочия отображаются серым шрифтом, и их нельзя редактировать. Кроме этого, новоприсвоенные полномочия для папки распространяются на содержащиеся в ней подпапки и файлы и либо дополняют или заменяют существующие полномочия. Это распространение полномочий позволяет предоставлять или ограничивать дополнительным пользователям и группам доступ к ресурсам папки независимо от родительской папки.

Чтобы лучше понять наследование, рассмотрим примеры.

- На диске C: создается папка Data, в которой создается подпапка CurrentProjects. По умолчанию папка Data наследует полномочия папки C:\, а папка CurrentProjects в свою очередь наследует эти полномочия от папки Data. Все файлы, вставляемые или создаваемые в папках C:\, C:\Data и C:\CurrentProjects, будут иметь одинаковые полномочия — те, которые были установлены для папки C:\ или унаследованы от нее.
- На диске C: создается папка Docs, в ней — подпапка Working. Для папки Working отключается наследование с удалением полномочий, унаследованных от корневой родительской папки, C:\. Теперь все файлы, добавляемые в папку C:\Docs\Working, наследуют полномочия только папки C:\Docs, и никаких других папок.
- На диске C: создается папка Backup, в которой создается подпапка Sales. Для папки Sales добавляются полномочия, разрешающие доступ членам группы **Sales**. Все файлы, добавляемые в папку C:\Backup\Sales, наследуют полномочия для папки C:\, а также дополнительные права доступа для членов группы **Sales**.

> ***Практический совет***
>
> Многие начинающие администраторы не понимают выгоды наследования и его применения. Хотя наследование иногда может казаться приносящим больше хлопот, чем преимуществ, оно позволяет очень эффективно управлять полномочиями. Без наследования нужно было бы настраивать полномочия для каждого создаваемого файла и папки. Кроме этого, если бы потребовалось изменить полномочия в будущем, то нужно было бы делать это для всех файлов и папок. С использованием наследования все новые файлы и папки автоматически получают набор полномочий. А если возникает необходимость изменить полномочия, это можно сделать для родительской папки, в результате чего все изменения будут автоматически применены ко всем содержащимся в ней папкам и файлам. Таким способом один и тот же набор полномочий можно применить ко многим файлам и папкам, не редактируя полномочия индивидуальных файлов и папок.

Просмотр унаследованных разрешений

Для просмотра унаследованных полномочий файла или папки в Проводнике Windows щелкните на объекте правой кнопкой мыши и в контекстном меню выберите команду

Свойства. В открывшемся окне свойств объекта выберите вкладку **Безопасность**, а на ней нажмите кнопку **Дополнительно**. В результате откроется диалоговое окно **Дополнительные параметры безопасности** (см. рис. 13.3). Полномочия пользователей для данного ресурса указаны в столбце **Доступ** (Access) этого окна. Если полномочия унаследованы, в столбце **Унаследовано от** (Inherited from) указывается родительская папка. Если данное полномочие наследуется другими ресурсами, эти ресурсы перечисляются в столбце **Применяется к**.

Отключение наследования

При отключении наследования в настройках безопасности объекта этот объект прекращает наследовать полномочия от родительских папок. При отключении наследования предоставляется возможность или преобразовать унаследованные полномочия в явные полномочия объекта, что позволит редактировать их, или же удалить все унаследованные полномочия объекта.

Отключить для объекта наследование полномочий от родительской папки можно следующим образом:

1. В Проводнике Windows щелкните правой кнопкой мыши на требуемой папке или файл и выберите в контекстном меню команду **Свойства**. На вкладке **Безопасность** окна свойств объекта файловой системы нажмите кнопку **Дополнительно**. Откроется диалоговое окно **Дополнительные параметры безопасности**, в котором по умолчанию выбрана вкладка **Разрешения**.
2. Внизу этой вкладки находится кнопка, надпись на которой зависит от текущего состояния наследования. Если наследование включено, надпись будет **Отключить наследование** (Disable inheritance). Соответственно, чтобы отключить наследование, нажмите эту кнопку.
3. Откроется диалоговое окно **Блокировать наследование** (Block Inheritance), в котором предоставляются два варианта обработки текущих унаследованных полномочий объекта (рис. 13.6). Первый вариант — это преобразовать унаследованные полномочия объекта в его явные полномочия, а второй — удалить все унаследованные полномочия и применить только те, которые были явно установлены.

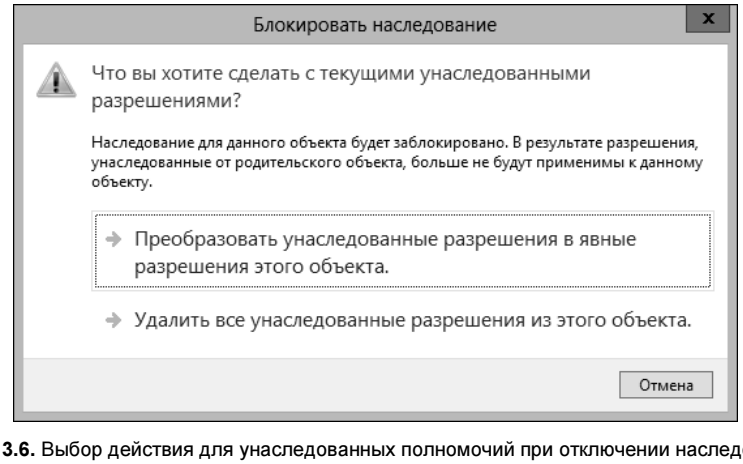


Рис. 13.6. Выбор действия для унаследованных полномочий при отключении наследования

Совет

Если отключить наследованные полномочия и при этом не присвоить никаких других, доступ к объекту будет запрещен всем пользователям, за исключением его владельца. Но при этом администраторы все еще могут стать владельцами такого ресурса. Таким образом, если администратору действительно нужно получить доступ к такому объекту, он может стать его владельцем и получить в результате неограниченный доступ.

Восстановление наследуемых разрешений

Со временем полномочия для файлов и папок могут настолько значительно отличаться от полномочий для родительской папки, что уже невозможно эффективно управлять доступом. Чтобы облегчить управление доступом к объекту, желательно предпринять решительные меры и удалить все существующие полномочия для всех содержащихся в папке объектов и заменить их полномочиями, унаследованными от родительской папки. Таким образом, полномочия, заданные для родительской папки, заменяют полномочия, установленные для каждого отдельного файла и папки данной родительской папки.

Для замены полномочий вложенных объектов полномочиями родительской папки применяется следующая процедура:

1. В Проводнике Windows щелкните правой кнопкой мыши на требуемой папке и в контекстном меню выберите команду **Свойства**. На вкладке **Безопасность** окна свойств папки нажмите кнопку **Дополнительно**.
2. На вкладке **Разрешения** открывшегося окна **Дополнительные параметры безопасности** установите флажок **Заменить все записи разрешений дочернего объекта наследуемыми от этого объекта** (Replace all child object permissions with inheritable permissions from this object), а затем нажмите кнопку **OK**.
3. Откроется окно **Безопасность Windows** (Windows Security), с предупреждением, что это действие заменит все явно определенные полномочия и включит распространения наследуемых полномочий (рис. 13.7). Нажмите кнопку **Да**, чтобы продолжить процесс.

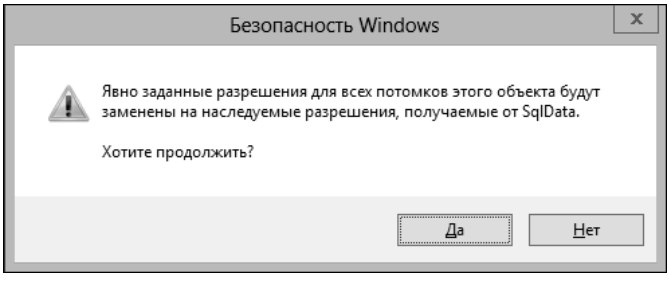


Рис. 13.7. Предупреждение о замене явных полномочий для объекта наследуемыми

Но чтобы получить полномочия от родительской папки, не обязательно удалять все существующие полномочия самого объекта. В частности, если для объекта было отключено наследование полномочий родительской папки, его можно снова включить. Процедура для этого следующая:

1. В Проводнике Windows щелкните правой кнопкой мыши на требуемой папке или файле и в контекстном меню выберите команду **Свойства**. На вкладке **Безопасность** окна свойств объекта нажмите кнопку **Дополнительно**.
2. На вкладке **Разрешения** открывшегося окна **Дополнительные параметры безопасности** нажмите кнопку **Включить наследование** (Enable inheritance), а затем кнопку **OK**.

Обратите внимание, что кнопка **Включить наследование** доступна только в том случае, если наследование в данный момент отключено.

Определение действующих полномочий и диагностирование проблем с полномочиями

Полномочия NTFS являются сложной функциональностью, управление которой может быть задачей не из легких. Иногда изменение, даже казалось бы совсем незначительное, может вызвать непреднамеренные последствия. Пользователи могут обнаружить, что им отказано в доступе к файлам, к которым они ранее имели полный доступ, или пользователи могут получить доступ к файлам, который им нельзя было предоставлять. В любом из таких сценариев причиной является какая-либо проблема с полномочиями. Наличие проблемы требует ее устранения.

Начинать диагностирование вышеописанных или других проблем с полномочиями следует с определения действующих сомнительных полномочий файлов или папок. Важность определения действующих полномочий состоит в том, что они позволяют быстро определить общий набор используемых полномочий.

Для пользователя действующие полномочия основываются на всех полномочиях, которые были предоставлены или запрещены пользователю, независимо от того, присвоены ли эти полномочия явно или же получены от групп, членом которых является пользователь. Например, если пользователь JimB является членом групп **Users**, **Sales**, **Marketing**, **SpecTeam** и **Managers**, его действующими полномочиями для файла или папки будет суммарный набор полномочий, которые были ему присвоены явно, и полномочий, присвоенных вышеперечисленным группам для данного объекта. Также, если пользователь JimB является членом группы, которой запрещено определенное полномочие для файла или папки, это полномочие для данного объекта также будет запрещено и для него, даже если другой группе, членом которой он является, это полномочие и разрешено. Это объясняется тем, что запрещение полномочий имеет приоритет над их разрешением.

То же самое справедливо и для утверждений пользователей и устройств. Если настроена политика доступа на основе утверждений и добавлено утверждение пользователя, это утверждение может препятствовать доступу. Так, доступу может препятствовать действующее утверждение устройства.

Определить действующие полномочия для пользователя или группы в отношении файла или папки можно следующим образом:

1. В Проводнике Windows щелкните правой кнопкой мыши на требуемой папке или файле и в контекстном меню выберите команду **Свойства**. В диалоговом окне свойств выберите вкладку **Безопасность** и нажмите на ней кнопку **Дополнительно**.
2. В открывшемся диалоговом окне **Дополнительные параметры безопасности** выберите вкладку **Действующие права доступа** (Effective Access). С помощью предоставленных на этой вкладке опций выберите требуемого пользователя, группу или устройство и просмотрите их действующие полномочия. При этом нужно иметь в виду следующее.
   - Если требуется определить права доступа только для определенного пользователя или группы пользователей, щелкните по ссылке **Выбрать пользователя** (Select a user), введите в следующем окне имя пользователя или группы и нажмите кнопку **OK**.
   - Если требуется определить права доступа только для определенного устройства или группы устройств, щелкните по ссылке **Выбрать устройство** (Select a device), введите в следующем окне имя устройства или группы устройств и нажмите кнопку **OK**.

- Если требуется определить права доступа для определенного пользователя или группы пользователей на конкретном устройстве или группе устройств, задайте как пользователя или группу пользователей, так и устройство или группу устройств.

3. Нажмите кнопку **Просмотреть действующие разрешения** (View effective access). В нижней панели окна будут отображены действующие полномочия для указанного пользователя или группы пользователей в формате полного набора специальных полномочий.
4. Если пользователь имеет полный доступ к выбранному ресурсу, он будет иметь все полномочия (рис. 13.8). В противном случае для пользователя будет выбрано только подмножество полномочий, и нужно тщательно изучить, обладает ли он соответствующими полномочиями. Для помощи в интерпретации действующих полномочий используйте табл. 13.3, представленную ранее в этой главе.

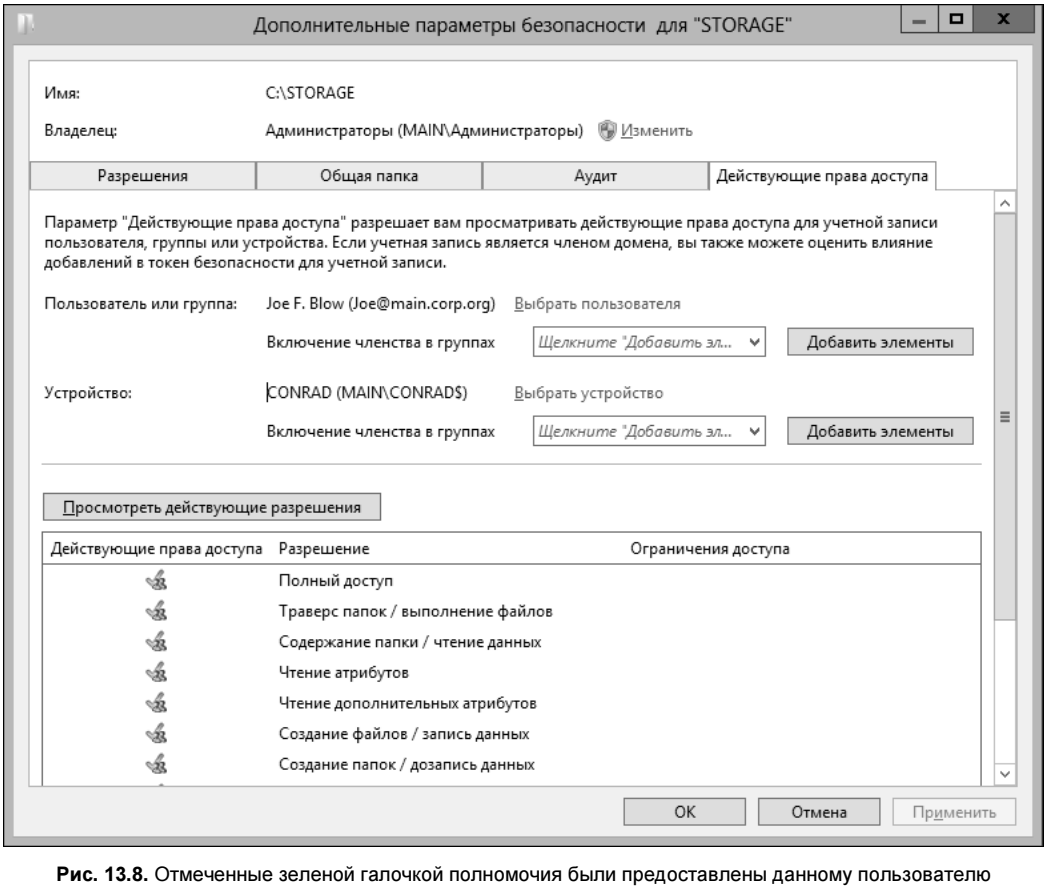


Рис. 13.8. Отмеченные зеленой галочкой полномочия были предоставлены данному пользователю

Примечание

Для просмотра действующих полномочий любого пользователя или группы необходимо обладать соответствующими правами. Также важно помнить о том, что нельзя определить действующие полномочия для неявных групп или специальных учетных записей, таких как **Прошедшие проверку** или **Все**. Кроме этого, действующие полномочия не отражают полномочия, предоставленные пользователю, как создателю-владельцу.

Предоставление общего доступа к файлам и папкам по сети

Операционная система Windows 8 поддерживает две модели предоставления общего доступа к файлам: предоставления общего доступа к папкам Общие и предоставление доступа к стандартным папкам. Эти модели, по отдельности или совместно, можно использовать в рабочих группах и доменах, но предоставление общего доступа к стандартным папкам является предпочтительным, т. к. этот подход предоставляет больший уровень безопасности, чем предоставление общего доступа к папкам Общие. Предоставление общего доступа к стандартным файлам позволяет использовать стандартный набор полномочий, чтобы разрешить или запретить первоначальный сетевой доступ к файлам и папкам. Параметры предоставления общего доступа к стандартным папкам задаются для каждого отдельного компьютера. Настройка предоставления общего доступа к данным выполняется следующим образом:

1. В разделе **Сеть и Интернет** Панели управления щелкните по ссылке **Выбор параметров домашней группы и общего доступа к данным**, а затем по ссылке **Изменить дополнительные параметры общего доступа**.
2. Откроется страница **Изменение параметров общего доступа для различных сетевых профилей**, содержащая конфигурационные параметры для каждого доступного сетевого профиля. Для работы с требуемым сетевым профилем разверните соответствующую панель, нажав кнопку в виде кружка с направленным вниз треугольником справа от панели.
3. Чтобы разрешить общий доступ к файлам и принтерам, установите переключатель **Включить общий доступ к файлам и принтерам** (Turn on file and printer sharing), а чтобы отключить общий доступ к файлам и принтерам — переключатель **Отключить общий доступ к файлам и принтерам** (Turn off file and printer sharing). Нажмите кнопку **Применить**.

Основным протоколом общего доступа к файлам по сети, используемым в компьютерах под управлением Windows, является протокол SMB. При общем доступе к папкам по сети клиент SMB выполняет операции чтения и записи файлов и запрашивает сервисы у компьютера, на котором расположена общая папка. Операционные системы Windows 8 и Windows Server 2012 поддерживают версию протокола SMB 3.0 и содержат клиента, совместимого с этой версией.

Протокол SMB 3.0 улучшает производительность во многих отношениях, особенно при использовании кластерных файловых серверов. Готовым усовершенствованием, для которого не требуется специальная настройка, является двустороннее шифрование обмениваемых по протоколу SMB данных, что устраняет необходимость использования протокола IPSec, специализированного оборудования или WAN-оптимизаторов, чтобы защитить данные от перехвата. Шифрование средствами протокола SMB можно задавать как для отдельных общих ресурсов, так и для всего сервера.

Управление доступом к общим сетевым ресурсам

При обращении пользователя по сети к обычному файлу или папке с общим доступом, для определения действий, разрешенных этому пользователю, выполнять с данным ресурсом, применяются два уровня полномочий. Первый уровень полномочий состоит из прав для доступа к общему ресурсу, которые определяют максимальный уровень доступа. Уровень

полномочий пользователя или группы никогда не может быть выше уровня полномочий, предоставляемых ему для доступа к общему ресурсу. Второй уровень полномочий состоит из прав, заданных для файлов и папок. Эти полномочия используются для дальнейшего ограничения доступа.

Существуют три вида полномочий для общего ресурса.

- **Владелец.** Пользователи, имеющие этот уровень доступа к общему ресурсу, имеют права **Полный доступ**, **Чтение** и **Смена разрешений**, а также дополнительные права по смене полномочий и владельца для файлов и папок. Уровень доступа **Владелец** к общему ресурсу предоставляет полный доступ к этому ресурсу.
- **Чтение-запись.** Пользователи с этим уровнем доступа имеют полномочия **Чтение** и **Смена разрешений**, а также дополнительные полномочия для создания файлов и папок, изменения файлов, изменения атрибутов файлов и подпапок и удаления файлов и подпапок. Этот уровень доступа позволяет читать, изменять и удалять данные ресурса, но не становиться его владельцем.
- **Чтение.** Этот уровень доступа имеет только полномочие **Чтение**. Пользователи с этим уровнем доступа к общему ресурсу могут просматривать имена файлов и папок, открывать подпапки общей папки, просматривать данные и атрибуты файла и выполнять файлы программ. Самое большое, что можно делать, имея уровень доступа **Чтение** к общему ресурсу, — это выполнять только операции чтения.

Групповые полномочия действуют следующим образом: пользователь, являющийся членом группы, которая обладает правом доступа к общему ресурсу, также имеет это право. Если пользователь является членом нескольких групп, его права доступа будут суммарными. Например, если одна группа имеет уровень доступа **Чтение**, а другая — **Чтение/Запись**, уровень доступа пользователя, являющегося членом обеих этих групп, будет **Чтение/Запись**. А если одна группа имеет уровень доступа **Чтение**, а другая **Владелец**, уровень доступа пользователя, являющегося членом обеих этих групп, будет **Владелец**.

Это поведение можно заместить, явно запретив полномочие. Запрет полномочия имеет приоритет над разрешенными полномочиями и замещает их. Если требуется, чтобы у пользователя не было определенного уровня доступа, следует в настройках прав доступа к общему ресурсу запретить его. Например, если нужно, чтобы пользователь, который является членом группы с уровнем доступа **Владелец** к общему ресурсу, имел только уровень доступа **Чтение/Запись**, в настройках общего доступа к сетевому ресурсу пользователю следует запретить доступ **Владелец**.

Предоставление общего сетевого доступа к ресурсу

Общий сетевой доступ к ресурсам можно предоставлять в рабочих группах и доменах. Чтобы предоставить общий сетевой доступ к первому ресурсу компьютера, нужно обладать правами локального администратора. После предоставления общего сетевого доступа к первому ресурсу другие пользователи могут предоставлять общий сетевой доступ к ресурсам, которыми они владеют или для которых они имеют соответствующие права доступа.

Для предоставления общего сетевого доступа к ресурсам можно использовать несколько разных инструментов.

- **Проводник Windows.** С помощью Проводника Windows общий сетевой доступ можно предоставлять к ресурсам локального компьютера.
- **Консоль Управление компьютером.** С помощью консоли **Управление компьютером** общий сетевой доступ можно открывать к ресурсам любого компьютера, который можно подключить к консоли.

- **Утилита командной строки Net Share.** Эта утилита полезна для предоставления общего сетевого доступа с помощью файлов сценариев. Чтобы получить справку о синтаксисе команды, выполните команду `net share /?`.
- **Модуль SmbShare.** Позволяет предоставлять и управлять общим сетевым доступом к ресурсам. Чтобы получить список связанных командлетов, выполните команду `get-help smbshare` в консоли Windows PowerShell.

Процесс предоставления общего сетевого доступа к ресурсу состоит из нескольких этапов. Сначала предоставляется общий доступ к папке, а затем настраивается уровень общего сетевого доступа к этому ресурсу. После этого нужно проверить и должным образом настроить полномочия доступа файловой системы. В этом разделе мы рассмотрим предоставление общего сетевого доступа к ресурсу и настройку полномочий для него с помощью Проводника Windows и консоли **Управление компьютером**. Подробные сведения о полномочиях файловой системы *см. в разд. "Управление доступом к файлам и папкам посредством разрешений NTFS" ранее в этой главе.*

Предоставление общего сетевого доступа к ресурсу и настройка уровня доступа с помощью Проводника Windows

Проводник Windows поддерживает предоставление основного и расширенного общего сетевого доступа. Основной сетевой доступ предоставляет доступ к любой папке, за исключением корневой папки диска. А расширенный сетевой доступ — к корневой папке диска, а также к любой другой папке. Сетевой доступ к корневым папкам дисков предоставляется автоматически, как к общим административным ресурсам.

Основной общий сетевой доступ к папке можно предоставить следующим образом:

1. В Проводнике Windows щелкните правой кнопкой мыши на требуемой папке и в контекстном меню выберите команду **Общий доступ**, а во вложенном меню — команду **Отдельные люди**. Откроется окно мастера **Общий доступ к файлам** (рис. 13.9).

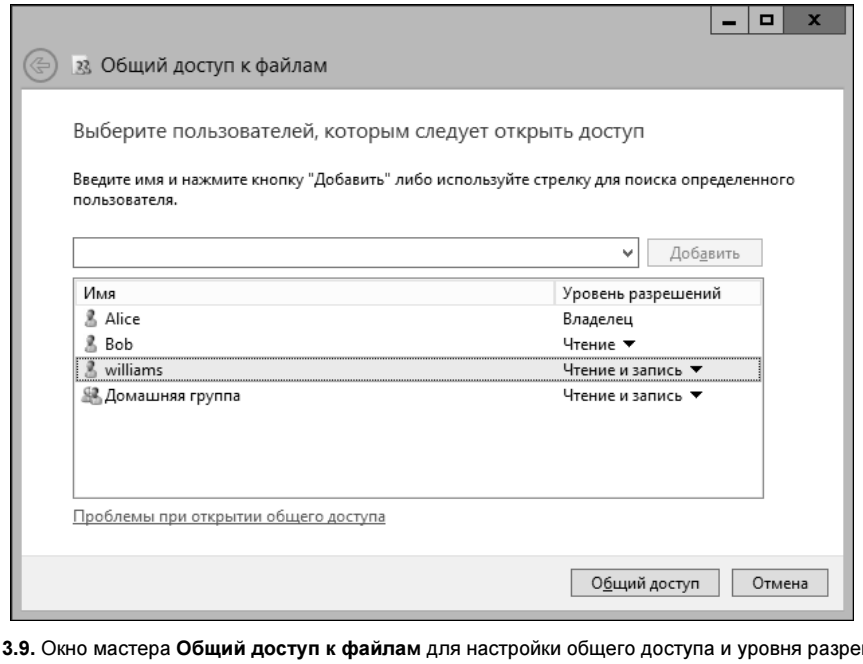


Рис. 13.9. Окно мастера **Общий доступ к файлам** для настройки общего доступа и уровня разрешений

2. В текстовое поле введите имя пользователя, которому нужно предоставить доступ, или щелкните по направленному вниз треугольнику в правой части поля, чтобы выбрать пользователя из списка. На компьютерах рабочих групп здесь всегда отображаются только локальные учетные записи и группы. На доменных компьютерах этот список, кроме локальных пользователей и групп, также содержит доменных пользователей.
3. После нажатия кнопки **Добавить** выбранные пользователи и группы добавляются в список **Имя** в нижней панели окна мастера. Для пользователей и групп в этом списке можно настроить определенный уровень доступа к данному сетевому ресурсу, щелкнув по направленному вниз треугольнику в поле **Уровень разрешений** (Permission Level) и выбрав в раскрывающемся списке требуемый уровень: **Чтение** или **Чтение и запись**.
4. Выбрав всех необходимых пользователей и задав для них требуемый уровень доступа, нажмите кнопку **Общий доступ** (Share), чтобы открыть общий доступ к ресурсу. После того как Windows 8 откроет общий доступ к ресурсу и выведет соответствующее сообщение, запомните имя общего ресурса. Это имя, по которому можно обращаться к данному общему ресурсу. Ссылку на общий ресурс можно отправить по электронной почте другим пользователям, щелкнув по ссылке **отправить по электронной почте** (e-mail), или скопировать ее в буфер обмена, щелкнув по ссылке **скопировать ссылки** (copy). Завершив настройку общего сетевого доступа, нажмите кнопку **Готово**, чтобы сохранить настройки и закрыть окно мастера.

> ***Примечание***
>
> Доступ к общему ресурсу можно получить, используя сокращенный формат его пути UNC. Например, если к папке C:\Data\Reports\Current компьютера CorpPCSS предоставить общий доступ посредством предоставления общего доступа к папке C:\Data\Reports\, пользователи других компьютеров могут получить доступ к этой папке, используя путь UNC \\CorPC85\Reports. Но для доступа к общей папке в профиле пользователя используется путь относительно папки **Пользователи** компьютера. Причиной этому является то обстоятельство, что Windows настраивает общий доступ к ресурсу относительно расположения этого ресурса в папке **Пользователи**. Например, если пользователь ДарьяМ на компьютере CustPC27 предоставит общий доступ к своей папке Документы, путь UNC к этому общему ресурсу будет \\CustPC27\Пользователи\ДарьяМ\Документы.

Расширенный общий сетевой доступ к папке предоставляется следующим образом:

1. В Проводнике Windows щелкните правой кнопкой мыши на требуемой папке или файле и в контекстном меню выберите команду **Свойства**.
2. На вкладке **Доступ** (Sharing) открывшегося окна свойств объекта нажмите кнопку **Расширенная настройка** (Advanced Sharing). В открывшемся диалоговом окне **Расширенная настройка** установите флажок **Открыть общий доступ к этой папке** (Share this folder).
3. По умолчанию Windows присваивает имя папки в качестве имени общего ресурса. Примите это имя или введите другое.
4. Далее нажмите кнопку **Разрешения** (Permissions). В открывшемся диалоговом окне **Разрешения для** настройте полномочия доступа для общего ресурса. Нажмите кнопку **OK**, чтобы закрыть окно настройки полномочий.
5. Нажмите кнопку **Кэширование**. В открывшемся диалоговом окне **Настройка автономного режима** (Offline Settings) укажите возможность и способ кэширования данных общего ресурса для автономного режима работы с ним. Нажмите кнопку **OK**, чтобы закрыть окно настройки кэширования.
6. Нажмите кнопку **OK**, а затем **Закрыть**, чтобы закрыть все диалоговые окна, связанные с настройкой расширенного сетевого доступа.

Изменение параметров или прекращение общего сетевого доступа

Чтобы прекратить общий сетевой доступ к ресурсу, выберите в его контекстном меню команду **Общий доступ**, а во вложенном меню — команду **Прекратить общий доступ**. Чтобы отредактировать полномочия доступа к общему сетевому ресурсу, выберите в его контекстном меню команду **Общий доступ**, а во вложенном меню — **Отдельные люди**. В открывшемся диалоговом окне **Общий доступ к файлам** можно изменить или полностью отменить полномочия доступа для существующих пользователей или предоставить доступ дополнительным пользователям. Чтобы отменить доступ пользователю, выберите его в списке **Имя** и в контекстном меню выберите команду **Удалить** (Remove). Завершив редактирование настроек общего сетевого доступа к ресурсу, нажмите кнопку **Общий доступ**, а в следующем окне — кнопку **Готово**.

Для редактирования расширенных настроек общего сетевого доступа откройте окно свойств требуемого ресурса, перейдите в нем на вкладку **Доступ**, а на ней нажмите кнопку **Расширенная настройка**. В открывшемся диалоговом окне **Расширенная настройка общего доступа** можно редактировать параметры общего доступа таким же образом, как и при первоначальном предоставлении расширенного общего доступа к ресурсу. Подробную информацию *см. в предыдущем разделе*.

Предоставление общего сетевого доступа к ресурсу и настройка уровня доступа с помощью консоли *Управление компьютером*

С помощью консоли **Управление компьютером** можно предоставлять общий сетевой доступ к ресурсам на любом компьютере, к которому вы имеете доступ, как администратор. Выполнение удаленного входа вместо локального на требуемый компьютер обычно позволяет сэкономить время, т. к. для этого не нужно покидать свое обычное рабочее место. Процедура для предоставления и настройки общего доступа к ресурсу с помощью консоли **Управление компьютером** следующая:

1. Запустите консоль **Управление компьютером** в окне **Администрирование** Панели управления либо выполните для этого команду `compmgmt.msc` в поле поиска панели **Приложения** или в консоли командной строки. По умолчанию консоль **Управление компьютером** подключена к локальному компьютеру и корневой узел дерева консоли помечен как **Управление компьютером (локальным)**.

   Совет

   Для предоставления общего доступа к ресурсу локального компьютера можно пропустить шаги 1—4 и запустить мастер создания общих ресурсов вручную. Для этого нужно выполнить команду `shrpubw` в консоли командной строки, открытой от имени администратора, а затем нажать кнопку **Далее** на первой странице мастера.

2. Нажмите или щелкните правой кнопкой мыши по узлу **Управление компьютером** в дереве консоли и в контекстном меню выберите команду **Подключиться к другому компьютеру**. Откроется диалоговое окно **Выбор компьютера**, в котором по умолчанию установлен переключатель **к другому компьютеру**. Введите в смежное с этим переключателем поле полное имя удаленного компьютера. Например, `engpc08.microsoft.com`, где `engpcOS` означает имя компьютера, а `microsoft.com` — имя домена. Если имя требуемого компьютера неизвестно и включена функциональность сетевого обнаружения, нажмите кнопку **Поиск** и выполните поиск требуемого компьютера.
3. Выполнив подключение к другому компьютеру, разверните в дереве консоли узел **Служебные программы\Общие папки** (System Tools\Shared Folders) и выберите в нем

подузел **Общие ресурсы** (Shares), чтобы просмотреть ресурсы с общим сетевым доступом на управляемом удаленном компьютере (рис. 13.10).

4. Запустите **Мастер создания общих ресурсов** (Create a shared folder wizard), щелкнув правой кнопкой мыши по узлу **Общие ресурсы** и выбрав в контекстном меню команду **Новый общий ресурс** (New share). Нажмите кнопку **Далее**, чтобы перейти на следующую страницу мастера, **Путь к папке** (Folder path).

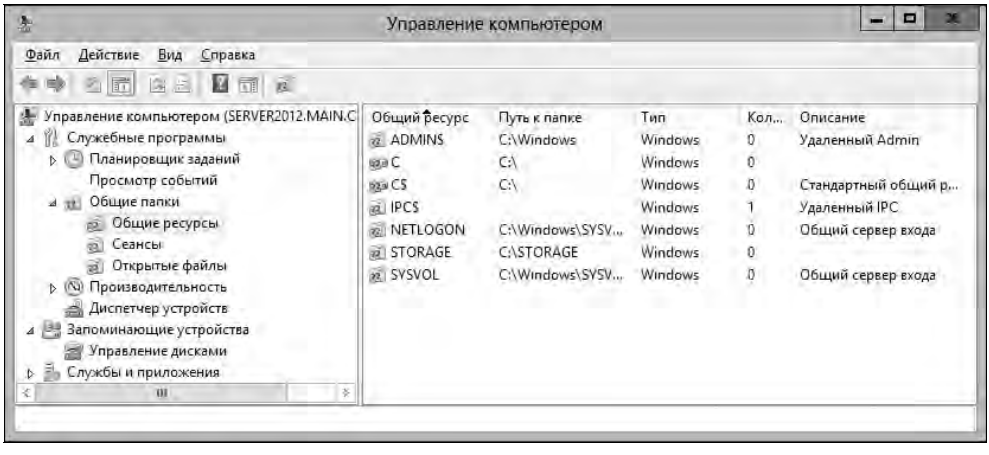


Рис. 13.10. Все ресурсы с общим сетевым доступом удаленного компьютера отображаются в узле **Общие ресурсы**

5. В поле **Путь к папке** введите полный путь к папке, к которой требуется предоставить общий доступ, например C:\Data. Если путь неизвестен, нажмите кнопку **Обзор** и с помощью окна **Обзор папок** (Browse for folder) найдите требуемую папку. В этом же окне можно создать новую папку, к которой затем можно предоставить общий доступ. Выбрав требуемую папку, нажмите кнопку **Далее**, чтобы перейти на следующую страницу мастера, **Имя, описание и параметры** (Name, Description, and Settings).
6. В текстовое поле **Общий ресурс** (Share Name) введите имя для общего ресурса. Имена общих ресурсов для каждой системы должны быть уникальными. Имя может быть длиной в 80 символов и содержать пробелы.
7. В поле **Описание** (Share Description) введите описание содержимого общего ресурса.

> ***Совет***
>
> По умолчанию использовать в автономном режиме можно только файлы и программы, указанные пользователем. Чтобы изменить настройки работы в автономном режиме, нажмите кнопку **Изменить**. В открывшемся окне **Настройка автономного режима** кроме настройки по умолчанию доступны еще две опции использования содержимого общего ресурса в автономном режиме: автоматически доступны все открывавшиеся пользователем файлы и программы или все файлы и программы общего режима недоступны в автономном режиме. Задание требуемой опции выполняется установкой соответствующего переключателя. Задав требуемый автономный режим использования содержимого общего ресурса, нажмите кнопку **OK**, чтобы сохранить настройки и закрыть окно.

8. Нажмите кнопку **Далее** для перехода на следующую страницу мастера, **Разрешения для общей папки** (Shared Folder Permissions). Здесь доступны следующие опции.
   - **У всех пользователей доступ только для чтения** (All users have read-only access). Опция по умолчанию. Всем пользователям предоставляются полномочия просматривать файлы и данные, но не создавать, изменять или удалять файлы и папки.

- **Администраторы имеют полный доступ, остальные — доступ только для чтения** (Administrators have full access; other users have read-only access). Администраторам предоставляется полный доступ к общему ресурсу, а остальным пользователям — доступ только для чтения. Администраторы могут создавать, изменять и удалять файлы и папки. Для общего ресурса на томе NTFS эта опция также предоставляет администраторам полномочия изменять разрешения и становиться владельцем файлов и папок. Все прочие пользователи могут только просматривать список файлов и их содержимое, но не создавать, изменять или удалять файлы и папки.
- **Администраторы имеют полный доступ, остальные не имеют доступа** (Administrators have full access; other users have no access). Предоставляет администраторам полный доступ к общему ресурсу и никакого доступа всем другим пользователям.
- **Настройка разрешений доступа** (Customize permissions). Предоставляет возможность настроить доступ для определенных пользователей и групп, что обычно является лучшим подходом. Установив этот переключатель, нажмите кнопку **Другой** (Customize Permissions) и в открывшемся диалоговом окне **Настройка разрешений доступа** установите требуемые полномочия.

9. Настроив разрешения доступа к общему ресурсу, нажмите кнопку **Далее**, а затем **Готово**, чтобы предоставить к папке общий доступ. На последней странице мастера нажмите кнопку **Готово**, чтобы закрыть его.

Если в будущем потребуется отменить общий доступ к этому ресурсу, щелкните на нем в папке **Общие ресурсы** консоли **Управление компьютером** и в контекстном меню выберите команду **Прекратить общий доступ**. При выводе запроса подтвердить действие, нажмите кнопку **Да**.

Предоставление общего доступа к ресурсу и управление им посредством групповой политики

Предоставить общий сетевой доступ к ресурсу можно с помощью групповой политики. Но этот подход рекомендуется использовать только в том случае, когда можно точно выбрать целевые компьютеры, чтобы общий сетевой доступ к папкам предоставлялся лишь на тех компьютерах, на которых это действительно требуется.

Создать элемент предпочтения для создания, обновления, замены или удаления папки с общим сетевым доступом можно следующим образом:

1. В редакторе управления групповыми политиками откройте для редактирования требуемый объект групповой политики. Разверните узел **Конфигурация компьютера**\ **Настройка****Конфигурация Windows** и выберите в нем подузел **Сетевые общие ресурсы** (Network Shares).
2. Щелкните на этом узле правой кнопкой мыши, в контекстном меню выберите команду **Создать**, а во вложенном меню — команду **Сетевой ресурс** (Network Share). Откроется диалоговое окно **Новые свойства общего сетевого ресурса** (New Network Share Properties).
3. В раскрывающемся списке **Действие** этого окна выберите требуемое действие — **Создать**, **Обновить**, **Заменить** или **Удалить**.
4. В текстовое поле **Имя ресурса** введите имя для общего ресурса. Имена общих ресурсов для каждой системы должны быть уникальными. Имя может быть длиной до 80 символов и содержать пробелы.

5. В поле **Путь к папке** введите полный путь к папке, к которой требуется предоставить общий доступ, например C:\Data. Если полный путь к существующей требуемой папке неизвестен, нажмите кнопку обзора файловой системы (кнопка с тремя точками справа от поля пути) и в открывшемся диалоговом окне **Выбор папки** укажите папку, к которой требуется предоставить общий сетевой доступ.

> ***Практический совет***
>
> Если в пути папки требуется использовать переменную среды, нажмите клавишу <F3>, чтобы отобразить список системных переменных. Выберите требуемую переменную, например `LogonUser`, а затем нажмите кнопку **Выбрать**. По умолчанию, прежде чем переменные применяются к компьютеру пользователя, они сопоставляются групповой политикой. Чтобы вместо этого использовать переменную в качестве подстановочного значения, которое сопоставляется на компьютере пользователя, до нажатия кнопки **Выбрать** нужно снять флажок **Сопоставить переменную** (Resolve variable).
>
> В предпочтениях групповой политики можно с легкостью отличить переменные, которые сопоставляются групповой политикой, от переменных, которые сопоставляются на компьютере пользователя. Первые имеют синтаксис *%Имя_переменной%*, например *%ProgramFiles%*, а вторые — *%<Имя_переменной>%*, например *%<ProgramFiles>%*.

6. В текстовое поле **Комментарий** (Comment) введите описание содержимого общего ресурса.
7. Операцию обновления или удаления общих ресурсов можно применить не только к отдельному ресурсу, а ко всем общим ресурсам определенного типа. В частности, можно выполнить одно из следующих действий:
   - обновить или удалить все обычные общие ресурсы (т. е. общие ресурсы, которые не являются скрытыми, административными или особыми), установив флажок **Обновить все обычные общие ресурсы** (Update all regular shares) или **Удалить все обычные общие ресурсы** (Delete all regular shares);
   - обновить или удалить все скрытые общие ресурсы, за исключением административных и специальных общих ресурсов (которые включают общие ресурсы букв дисков, ADMIN$, FAX$, IPC$ и Print$), установив флажок **Обновить все скрытые неадминистративные общие ресурсы** (Update all hidden non-administrative shares) или **Удалить все скрытые неадминистративные общие ресурсы** (Delete all hidden non-administrative shares);
   - обновить или удалить все административные общие ресурсы (которые включают только общие ресурсы букв дисков), установив флажок **Обновить все административные общие ресурсы букв дисков** (Update all administrative drive-letter shares) или **Удалить все административные общие ресурсы букв дисков** (Delete all administrative drive-letter shares).

> ***Примечание***
>
> Если требуется изменить специальные общие ресурсы, такие как ADMIN$, FAX$, IPC$ или Print$, или другие системные общие ресурсы, такие как SYSVOL или NETLOGON, для общего ресурса можно создать элемент предпочтения и присвоить ему имя специального общего ресурса.

8. Укажите количество пользователей, которые могут подключаться к общему ресурсу. Установите флажок **Максимально допустимое** (Maximum allowed), чтобы разрешить подключения максимального количества пользователей, поддерживаемого системой. Чтобы установить другое предельное количество, установите флажок **Не более** (Allow this number of users).
9. Укажите, нужно ли использовать элементы управления доступом для просмотра пользователями папок общего ресурса. Установите переключатель **Включить** (Enable), чтобы

разрешить просмотр папок общего ресурса только пользователям, имеющим полномочие **Чтение**. Чтобы разрешить просмотр папок общего ресурса всем пользователям, установите переключатель **Отключить** (Disable).

10. Для управления способом применения настройки существуют специальные опции на вкладке **Общие параметры**. Так как мы принудительно используем элемент управления, обычно параметры желательно применять при каждом обновлении групповой политики. В таком случае нужно снять флажок **Применить один раз и не применять повторно**.
11. Нажмите кнопку **OK**. При следующем обновлении групповой политики элемент предпочтений будет применен должным образом к тому объекту групповой политики, для которого он был определен.

Доступ к общим ресурсам и их использование

Когда к файлу или папке предоставлен общий сетевой доступ, пользователи могут обращаться к нему как сетевому ресурсу, или подключить его к локальному компьютеру в виде сетевого диска. Пользователи могут обращаться к подключенному сетевому диску, как будто бы это локальный диск.

Подключение к локальному компьютеру файла или папки с общим доступом в виде сетевого диска выполняется следующим образом:

1. В левой панели Проводника Windows щелкните на значке **Компьютер**, в результате чего в правой панели откроется консоль **Компьютер**.
2. По умолчанию, при открытии этой консоли в ней выбрана вкладка инструментов **Компьютер**. Выберите на ней команду **Подключить сетевой диск**, откроется диалоговое окно **Подключение сетевого диска** (Map Network Drive) (рис. 13.11).

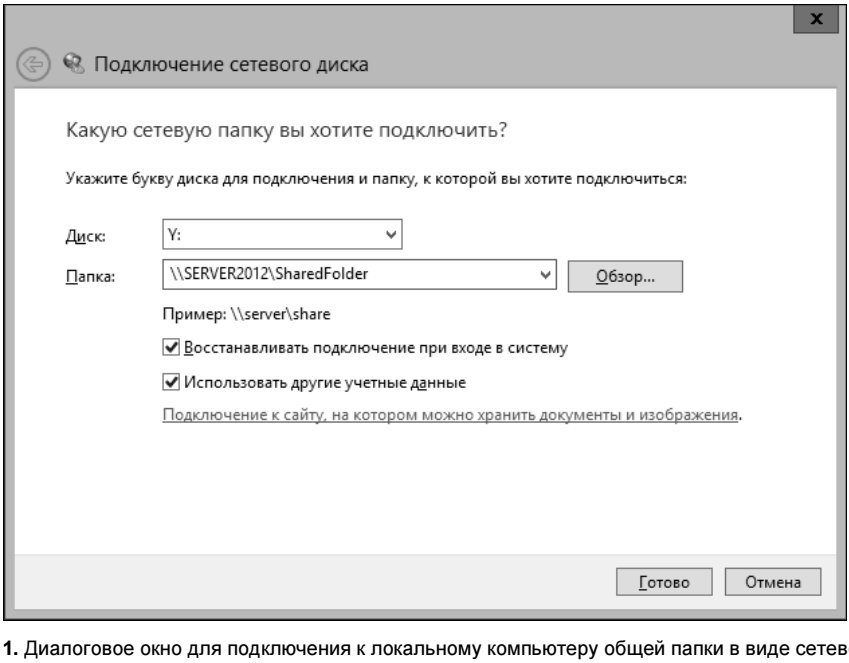


Рис. 13.11. Диалоговое окно для подключения к локальному компьютеру общей папки в виде сетевого диска

3. В раскрывающемся списке **Диск** выберите букву диска, а затем нажмите кнопку **Обзор** справа от списка **Папка**. В диалоговом окне **Обзор папок** разверните дерево сетевых папок, пока не будет найдена необходимая рабочая группа или домен.
4. Затем разверните этот узел, чтобы отобразить список его общих папок. Выберите в этом списке нужную папку и нажмите кнопку **OK**.
5. Если требуется, чтобы Windows 8 автоматически подключала общую папку при каждом входе пользователя в систему, установите флажок **Восстанавливать подключение при входе в систему** (Reconnect at logon).
6. Выполнив все настройки, нажмите кнопку **Готово**. Если пользователь, подключающий сетевой диск, не обладает должными полномочиями доступа для данного общего ресурса, установите флажок **Использовать другие учетные данные** (Connect using different credentials), а затем нажмите кнопку **Готово**. После этого откроется диалоговое окно для ввода учетных данных, по которым можно подключаться к данному сетевому диску. Введите имя пользователя в формате **Домен\Имя_пользователя** (например, `MAIN\Williams`) и пароль для данной учетной записи. Если требуется сохранить эти данные, чтобы не вводить их при каждом подключении, установите флажок **Запомнить учетные данные** (Remember my credentials).

При подключении общих папок в виде сетевого диска нужно иметь в виду, что компьютер переходит в автономный режим работы с данным ресурсом при следующих обстоятельствах:

- в случае недоступности сервера;
- в случае медленного сетевого подключения (при соответствующей настройке в групповой политике);
- когда пользователь выберет в Проводнике Windows опцию **Работать автономно** (Work offline);
- когда подключенный диск настроен на работу в режиме вне сети.

Чтобы включить этот режим, в Проводнике Windows щелкните на значке подключенного сетевого диска правой кнопкой мыши и в контекстном меню выберите команду **Всегда доступны вне сети** (Always available offline). Если требуется, Windows 8 затем запустит и выполнит настройку службы **Автономные файлы**, которая скопирует требуемые файлы и программы с сервера на локальный компьютер. Обратите внимание, что если в данный момент наблюдается низкая скорость сетевого подключения, на копирование файлов могут повлиять настройки групповой политики для медленных сетей. Задать способ использования медленного подключения с автономными файлами можно, включив и настроив параметр политики **Настроить режим медленного подключения** (Configure slow link mode), который находится в узле **Конфигурация компьютера\Административные шаблоны\Сеть\Автономные файлы** редактора управления групповыми политиками.

Режим постоянной доступности вне сети является нововведением в Windows 8 и Windows Server 2012. Когда этот режим включен, Windows 8 всегда использует подключенный сетевой диск в автономном режиме, а выбор файлов и программ, копируемых на локальный компьютер для использования в автономном режиме, определяется настройками опций кэширования на сервере. По умолчанию, только указанные пользователями файлы и программы доступны для использования в автономном режиме; чтобы использовать другую опцию кэширования, на сервере (или в групповой политике) нужно отредактировать настройки папки с общим доступом.

За содержание кэша автономных файлов и синхронизацию их изменений с сервером отвечает служба **Автономные файлы**. По умолчанию служба выполняет синхронизацию в фо-

новом режиме с интервалом в каждые два часа. Задать режим работы фоновой синхронизации автономных файлов можно, включив и настроив параметр политики **Настроить фоновую синхронизацию** (Configure background sync), который находится в узле **Конфигурация компьютера\Административные шаблоны\Сеть\Автономные файлы** редактора объекта групповой политики.

> ***Примечание***
>
> Режим постоянной доступности вне сети является нововведением в Windows 8 и Windows Server 2012. Эту функциональность могут использовать только компьютеры под Windows 8 и Windows Server 2012, работающие в доменной сетевой среде.

Чтобы отключить сетевой диск, откройте Проводник Windows и выберите в левой панели узел **Компьютер**. В разделе **Сетевое размещение** (Network location) консоли **Компьютер** щелкните правой кнопкой мыши на значке сетевого диска и в контекстном меню выберите команду **Отключить**.

На компьютерах домена настройку сетевых дисков можно выполнять с помощью элемента предпочтения групповой политики. Процедура для этого следующая:

1. В редакторе управления групповыми политиками откройте для редактирования требуемый объект групповой политики. Разверните узел **Конфигурация пользователя\Настройка\Конфигурация Window**s и выберите в нем подузел **Сопоставления дисков** (Drive Maps).
2. Щелкните по этому узлу правой кнопкой мыши, в контекстном меню выберите команду **Создать** (New), а во вложенном меню — команду **Сопоставленный диск** (Mapped Drive). Откроется диалоговое окно **Новые свойства диска** (New Drive Properties).
3. В раскрывающемся списке **Действие** этого окна выберите требуемое действие — **Создать**, **Обновить**, **Заменить** или **Удалить**.
4. В текстовое поле **Размещение** (Location) введите путь к сетевому диску в формате UNC, например \\CorpServer45\corpdatashare. Если путь неизвестен, нажмите кнопку обзора файловой системы (кнопка с тремя точками справа от поля **Размещение**) и в открывшемся диалоговом окне укажите требуемый общий ресурс.

> ***Практический совет***
>
> Если в пути общего ресурса нужно использовать переменную среды, щелкните по текстовому полю **Размещение**, а затем нажмите клавишу <F3>, чтобы отобразить список системных переменных. Выберите требуемую переменную, например `LogonUser`, а затем нажмите кнопку **Выбрать**. По умолчанию, прежде чем переменные применяются к компьютеру пользователя, они сопоставляются групповой политикой. Чтобы вместо этого использовать переменную в качестве подстановочного значения, которое сопоставляется на компьютере пользователя, до нажатия кнопки **Выбрать** нужно снять флажок **Сопоставить переменную**.
>
> В предпочтениях групповой политики можно с легкостью отличить переменные, которые сопоставляются групповой политикой, от переменных, которые сопоставляются на компьютере пользователя. Первые имеют синтаксис *%Имя_переменной%*, например *%ProgramFiles%*, а вторые — *%<Имя_переменной>%*, например *%<ProgramFiles>%*.

5. Если требуется, чтобы Windows 8 автоматически подключала общую папку в начале каждого сеанса, установите флажок **Повторное подключение** (Reconnect).
6. В текстовое поле **Подпись** (Label as) введите метку для сетевого диска.
7. В разделе **Буква диска** (Drive Letter) укажите способ присвоения буквы диска. Чтобы использовать первую свободную букву, начиная с указанной, установите переключатель **Использовать первую доступную, начиная с** (Use first available, starting at) и в раскрывающемся списке укажите требуемую букву диска. Чтобы всегда использовать опреде-

ленную букву диска, установите флажок **Использовать** (Use) и в раскрывающемся списке укажите требуемую букву диска. Если только не известно с точностью, что определенная буква диска является доступной, обычно рекомендуется использовать первую доступную букву.

8. Дополнительно можно указать учетные данные для подключения к общему сетевому ресурсу.
   - Чтобы использовать другие учетные данные, нежели данные текущего пользователя, введите требуемые данные в соответствующие поля в разделе **Подключиться как**. Пароль пользователя зашифровывается и сохраняется как часть объекта групповой политики в томе Sysvol на контроллерах домена.
   - Если нужно, чтобы текущий пользователь вводил свои учетные данные, введите текст `%<LogonUser>%` в поле **Имя пользователя** и оставьте поля пароля пустыми.

   Примечание

   Предоставление учетных данных для подключения к сетевому диску представляет угрозу безопасности, и это должно делаться только в ограниченных случаях. При использовании этого подхода следует в обязательном порядке периодически менять пароль соответствующей учетной записи пользователя, а затем обновлять пароли в элементах предпочтения, в которых используется эта учетная запись.

9. В окне свойств нового сетевого диска также предоставляются опции для скрытия или отображения подключаемого диска или всех дисков, которые применяются как к сетевым, так и к локальным дискам.
10. Для управления способом применения настройки предназначены опции на вкладке **Общие параметры**. Так как мы принудительно используем элемент управления, обычно параметры желательно применять при каждом обновлении групповой политики. В таком случае нужно снять флажок **Применить один раз и не применять повторно**.
11. Завершив настройку элемента предпочтения для сетевого диска, нажмите кнопку **OK**, чтобы сохранить настройки и закрыть окно свойств. При следующем обновлении политики элемент настройки будет применен должным образом к тому объекту групповой политики, для которого он был определен.

Доступ к общим папкам и использование их для администрирования

В Windows 8 автоматически создается несколько специальных сетевых папок, которые предназначены для использования администратором или операционной системой. Имя большинства из этих специальных общих ресурсов заканчивается символом доллара ($), что скрывает их от просмотра пользователями. Администратору иногда требуется создать свои скрытые общие папки или работать со штатными специальными общими папками.

Создание скрытой общей папки не представляет особого труда. Все, что для этого нужно сделать — это добавить знак доллара ($) в конец имени общей папки. Например, если требуется предоставить общий доступ к папке C:\Reports, но при этом не отображать ее в списке обычных общих ресурсов, этой папке нужно присвоить имя Reports$. Но скрытие общего ресурса от просмотра не запрещает доступа к нему. Управление доступом к общим ресурсам осуществляется посредством полномочий, независимо от того, скрыт ли общий ресурс или нет.

Какие именно специальные сетевые диски могут быть доступными в системе, зависит от конфигурации этой системы. Это означает, что некоторые компьютеры будут иметь больше

специальных общих папок, чем другие. В табл. 13.4 приведен список наиболее распространенных специальных и административных общих папок и их краткое описание.

Таблица 13.4. *Специальные и административные общие папки*

Имя общего ресурса	Описание
C$, D$, E$ и другие локальные диски	Специальная корневая папка диска с общим доступом. Все локальные диски, включая приводы CD/DVD, и их общие папки доступны как общие ресурсы C$, D$, E$ и т. д. Эти общие ресурсы позволяют членам групп **Администраторы** и **Операторы архива** подключаться к корневой папке локального диска для выполнения административных заданий. Например, при подключении к общему ресурсу C$ выполняется подключение к папке C:\ с полным доступом к этому локальному диску
ADMIN$	Административный общий ресурс для доступа к папке *%SystemRoot%*, содержащей файлы операционной системы. Эта общая папка предназначена для удаленного администрирования. Для администраторов, которые выполняют удаленное обслуживание систем, общая папка ADMIN$ предоставляет удобный способ быстрого доступа к папке операционной системы
IPC$	Общий административный ресурс, используемый для поддержки именованных каналов, которые применяются программами для взаимодействия между процессами. Так как именованные каналы можно перенаправлять по сети для подключения к локальным и удаленным системам, они также позволяют выполнять удаленное администрирование
PRINT$	Поддерживает общий доступ к принтерам, посредством предоставления доступа к драйверам принтера. Когда предоставляется общий доступ к принтеру, система помещает в эту общую папку драйверы принтера, чтобы другие компьютеры имели к ним доступ в случае надобности

Лучшим инструментом для работы со специальными или другими скрытыми общими ресурсами являются команда `net share` и консоль **Управление компьютером**. Вывести список всех общих ресурсов локального компьютера, включая специальные административные общие ресурсы, можно, выполнив команду `net share` в консоли командной строки. А просмотреть список всех общих ресурсов на любом компьютере сети можно следующим образом:

1. Запустите консоль **Управление компьютером** в окне **Администрирование** Панели управления либо выполните для этого команду `compmgmt.msc` в поле поиска панели **Приложения** или в консоли командной строки. По умолчанию консоль **Управление компьютером** подключена к локальному компьютеру, и корневой узел дерева консоли помечен как **Управление компьютером (локальным)**.
2. Нажмите или щелкните правой кнопкой мыши по узлу **Управление компьютером** в дереве консоли и в контекстном меню выберите команду **Подключиться к другому компьютеру**. Откроется диалоговое окно **Выбор компьютера**, в котором по умолчанию установлен переключатель **к другому компьютеру**. Введите в смежное с этим переключателем поле полное имя удаленного компьютера. Например, `engdpcOS` или `engpc08.microsoft.com`, где `engpcOS` означает имя компьютера, а `microsoft.com` — имя домена. Если имя требуемого компьютера неизвестно и включена функциональность сетевого обнаружения, нажмите кнопку **Поиск** и выполните поиск требуемого компьютера.
3. Выполнив подключение к другому компьютеру, разверните в дереве консоли узел **Служебные программы\Общие папки** и выберите в нем подузел **Общие ресурсы**, чтобы просмотреть ресурсы с общим сетевым доступом на данном удаленном компьютере.

Иногда при обслуживании файлов и папок желательно, чтобы в это время к затрагиваемым общим объектам не были подключены пользователи. Например, если требуется переместить файлы в новое место, прежде чем выполнять перемещение будет разумным проверить, что никто не использует эти файлы. Одним из способов проверить, кто работает с общими папками и содержащимися в них папками, будет просмотр пользовательских сеансов и открытых файлов.

При каждом подключении пользователя к общей папке создается пользовательский сеанс. Чтобы просмотреть подключенных в данный момент пользователей, в узле **Общие папки** выберите подузел **Сеансы**. В правой панели консоли будет отображен список пользователей, подключенных в данный момент к общим папкам. Чтобы отключить пользователя и завершить его сеанс, щелкните правой кнопкой мыши на сеансе в панели сведений и в контекстном меню выберите команду **Закрыть сеанс** (Close session). Подтвердите желание закрыть сеанс, нажав кнопку **OK** в окне запроса. Чтобы отключить все пользовательские сеансы, щелкните правой кнопкой мыши по узлу **Сеансы** в дереве консоли и в контекстном меню выберите команду **Отключить все сеансы** (Disconnect all sessions). Подтвердите желание закрыть сеансы, нажав кнопку **OK** в окне запроса.

Чтобы просмотреть открытые файлы общих папок, в узле **Общие папки** выберите подузел **Открытые файлы**. В правой панели консоли будет отображен список всех открытых в данный момент файлов в общих папках. Чтобы закрыть файл, щелкните на нем правой кнопкой мыши и в контекстном меню выберите команду **Закрыть открытый файл** (Close open file). Чтобы закрыть все открытые в общих папках файлы, щелкните правой кнопкой мыши по узлу **Открытые файлы** в дереве консоли и в контекстном меню выберите команду **Отключить все открытые файлы** (Disconnect all open files). Подтвердите желание отключить все файлы, нажав кнопку **OK** в окне запроса.

Поиск и устранение неполадок с общим доступом к файлам

Причину большинства проблем с общим доступом к файлам можно выяснить и устранить, применяя следующие методы диагностирования.

- **Проверьте подключение между компьютером, предоставляющим общие ресурсы, и компьютером, с которого пользователь пытается получить доступ к этим ресурсам.** Оба компьютера должны быть подключены к сети и их параметры TCP/IP должны быть настроены должным образом. Настройки брандмауэров обоих компьютеров должны разрешать входящие и исходящие подключения. Настройки брандмауэра компьютера, предоставляющего общие ресурсы, должны содержать исключение общего доступа к файлам и принтерам. Брандмауэр Windows поддерживает несколько одновременных активных профилей, и активный используемый профиль должен быть правильно настроен. Если используется брандмауэр стороннего разработчика, входящие подключения должны быть разрешены для UDP-порта 137, UDP-порта 138, TCP-порта 139, всех портов ICMpv4 и (если требуется для запросов отклика) портов ICMPv6.
- **Проверьте учетные данные подключения.** Когда оба компьютера являются членами домена, пользователь должен подключаться к общему ресурсу, используя доменные учетные данные. Если пользователь вошел в систему по локальной, а не доменной учетной записи, необходимо обеспечить, чтобы он подключался к общему ресурсу по другим учетным данным и это были соответствующие учетные данные для соответствующего домена.
- **Проверьте настройку расширенного общего доступа в Центре управления сетями и общим доступом.** С целью беспроблемного предоставления общего доступа к файлам

на компьютере под управлением Windows 8 для активного сетевого профиля должен быть включен общий доступ к файлам и принтерам, а параметр политики **Запретить пользователям в их профиле предоставлять общий доступ к файлам** должен быть отключен. Компьютеры могут быть одновременно подключены к нескольким сетям, и тип каждой активной сети должен быть правильно настроен в Центре управления сетями и общим доступом.

- **Проверьте тип текущей сети.** В Центре управления сетями и общим доступом обоих компьютеров должен быть установлен правильный тип сети. Если установлен тип сети **Общий**, многие параметры подключения и общего доступа будут заблокированы и запрещены.
- **Проверьте разрешения доступа для общего ресурса, полномочия NTFS и флаги атрибутов файлов.** Разрешения общего доступа и полномочия NTFS для пользователя должны быть настроены так, чтобы разрешить доступ и работу с общими файлами. Флаги атрибутов файлов **Только чтение**, **Скрытый** и **Системный** должны быть сняты, если требуется.

Для более глубокого диагностирования нужно проверить настройки DNS и членство в домене обоих компьютеров. В идеальном варианте оба компьютера должны быть подключены к одной и той же сети или к сетям, соединенным высокоскоростным подключением Ethernet. И также в идеальном случае оба компьютера должны быть членами одного и того же домена или находиться в доверенном домене.

Для предоставления общего доступа к файлам необходимо, чтобы работала служба **Сервер**. Проверьте, что на компьютере, предоставляющем доступ к общим файлам, служба **Сервер** настроена и работает. Обычно, служба **Сервер** должна быть настроена для автоматического запуска и входа в систему с учетной записью **Локальная система**. Эта служба зависит от драйвера **Server SMB**, поэтому проверьте наличие этого драйвера на вкладке **Зависимости** окна свойств службы **Сервер**.

В групповой политике компьютера, предоставляющего доступ к общим файлам, проверьте, что пользователь включен в список параметра политики **Доступ к компьютеру из сети** (Access this computer from the network). Этот параметр политики находится в узле редактора управления групповыми политиками **Конфигурация компьютера\Политики\Конфигурация Windows\Параметры безопасности\Локальные политики\Назначение прав пользователя** (Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment). По умолчанию все прошедшие проверку пользователи включены в этот список.

В групповой политике также можно настроить параметры политики **Помощь при ошибке "Отказано в доступе"**, чтобы помочь пользователям определить, к кому им нужно обращаться в случае проблем с доступом к файлам. Параметр политики **Помощь при ошибке "Отказано в доступе"** можно настроить для отображения дополнительных более подробных сообщений об ошибке, ссылок на справочные страницы или документы, а также для предоставления адресов электронной почты, по которым можно обратиться за помощью касательно проблем с получением доступа к общим ресурсам.

Чтобы включить параметр политики **Помощь при ошибке "Отказано в доступе"** для всех типов файлов, включите параметр политики **Включить исправление ошибки "Отказано в доступе" для всех типов файлов клиента** (Enable access-denied assistance on client for all file types), а также включите и настройте параметр политики **Настроить сообщение об ошибке "Отказано в доступе"** (Customize message for access denied errors). Эта политика и ее параметры находятся в узле **Конфигурация компьютера\Административные шаблоны**

Система\Помощь при ошибке "Отказано в доступе" (Computer Configuration\Administrative Templates\System\Access-Denied Assistance) редактора управления групповыми политиками.

Использование общих папок и настройка доступа к ним

Общие папки предназначены для предоставления пользователям доступа к файлам и папкам из одной точки. Они позволяют пользователям быстро сформировать весь материал, к которому они предоставили общий доступ, а также распределить предоставляемые для общего доступа файлы по типам. В этом разделе мы рассмотрим работу предоставления доступа к общим папкам и настройку этой функциональности.

Использование общих папок

Функциональность общих папок позволяет предоставлять общий доступ к файлам посредством помещения их в папку компьютера *%SystemDrive%*\Пользователи\Общие. Папка Общие содержит несколько подпапок, которые можно использовать для упорядочения по типам файлов, предоставляемых для общего доступа:

- **Общий рабочий стол** (Public Desktop) — используется для предоставления общего доступа к элементам рабочего стола;
- **Общие документы** (Public Documents), **Общая музыка** (Public Music), **Общие изображения** (Public Pictures), **Общедоступные ТВ-записи** (Public Recorded TV), **Общие видео** (Public Videos) — используются для предоставления общего доступа к документам и файлам мультимедиа;
- **Общие загруженные файлы** (Public Downloads) — используется для предоставления общего доступа к загруженным файлам.

Любое содержимое, помещаемое в эти подпапки, доступно всем пользователям компьютера, а также всем пользователям сети, если к папке Общие был предоставлен общий сетевой доступ.

Обычно пользователи получают доступ к общим файлам через окно **Библиотеки**, которое можно открыть, щелкнув в левой панели Проводника Windows на одноименном значке. А выбор узла библиотеки открывает соответствующую общую папку. Например, выбор в библиотеке узла **Документы** открывает папку **Общие документы**.

По умолчанию доступ к папке Общие компьютера имеют все пользователи с учетной записью и паролем. При помещении файлов в папку Общие этим файлам присваиваются такие же права, какие имеет сама папка, а также добавляются некоторые другие полномочия.

Полномочия по умолчанию для папки Общие позволяют локальным пользователям просматривать, записывать, изменять и удалять любые файлы в этой папке. Для папок **Общая музыка**, **Общие изображения** и **Общие видео** пользователям предоставлены права доступа **Чтение и выполнение** и **Чтение**.

Настройки параметров доступа по умолчанию к папке Общие можно изменить двумя основными способами.

- Разрешить сетевым пользователям просматривать список и открывать общие файлы, но запретить им изменять, удалять или создавать общие файлы. При установке этой опции группе **Все** предоставляются полномочия **Чтение и выполнение** и **Чтение** для общих

файлов и полномочия **Чтение и выполнение**, **Список содержимого папки** и **Чтение** для общих папок.

- Разрешить сетевым пользователям просматривать и управлять общими файлами, в частности открывать, изменять, создавать и удалять общие файлы. При настройке этой опции группе **Все** предоставляются полномочия **Полный доступ** для общих файлов и общих папок.

В следующем разделе рассматривается использование этих двух подходов для настройки доступа к общим папкам.

Настройка доступа к общим папкам

Настройка параметров доступа к общим папкам выполняется для каждого отдельного компьютера. Для доступа к папке Общие и ее подпапкам применяются одни и те же параметры доступа. Настройка доступа к общим папкам выполняется следующим образом:

1. В разделе **Сеть и Интернет** Панели управления щелкните по ссылке **Выбор параметров домашней группы и общего доступа к данным**, а в открывшемся окне **Изменение параметров домашней группы** — по ссылке **Изменить дополнительные параметры общего доступа**.
2. В следующем окне разверните раздел **Все сети**. В разделе **Общий доступ к общедоступным папкам** установите переключатель для требуемой опции доступа к общим папкам. Доступны следующие две опции.
   - **Включить общий доступ, чтобы сетевые пользователи могли читать и записывать файлы в общих папках** (Turn on sharing so anyone with network access can read and write files in the Public folders). Установите этот переключатель, чтобы предоставить полномочия совладельца на все общие папки и все общие данные всем, кто имеет сетевой доступ к компьютеру. При этом следует иметь в виду, что внешний доступ может быть ограничен вследствие настроек брандмауэра Windows.
   - **Отключить общий доступ** (Turn off public folder sharing). Установите этот переключатель, чтобы отключить сетевой доступ к общим папкам, разрешив доступ к ним только локальным пользователям.
3. В частных сетях управление подключениями к другим компьютерам домашней группы обычно выполняется операционной системой Windows. Если для всех компьютеров используется одна и та же учетная запись и пароль, для доступа к общим файлам и принтерам и к папке Общие можно использовать эту учетную запись. Для этого разверните раздел сетевого профиля **Частная** и в подразделе **Подключения домашней группы** (Homegroup connections) установите переключатель **Использовать учетные записи пользователей и пароли для подключения к другим компьютерам** (Use user accounts and passwords to connect to other computers).
4. Установив требуемые параметры, нажмите кнопку **Сохранить изменения**, чтобы сохранить их и закрыть окно настройки параметров общего доступа.

Аудит доступа к файлам и папкам

Хотя полномочия доступа повышают безопасность данных, они не предоставляют информации о попытках несанкционированного доступа к файлам и папкам или об удалении файлов, как непреднамеренных, так и преднамеренных. Чтобы отслеживать обращения

к файлам и папкам и действия с ними, необходимо настроить аудит доступа к файлам и папкам. Отслеживать обращения к файлам и папкам можно, включив аудит, указав, какие файлы и папки подлежат аудиту, а затем проверяя записи в журналах безопасности.

Включение возможности аудита файлов и папок

Настроить политики аудита можно, используя групповую политику или локальную политику безопасности. Групповую политику лучше использовать, когда нужно задать политики аудита для всей организации. Локальною политику безопасности следует использовать, когда нужно задать политики аудита для определенного компьютера, не забывая при этом, что локальная политика может быть замещена групповой политикой.

Включить аудит файлов и папок можно одним из следующих способов.

- Чтобы настроить локальную политику для определенного компьютера, откройте консоль **Локальная политика безопасности** (Local security policy). Если включено отображение средств администрирования на экране **Пуск**, эту консоль можно запустить с помощью ее плитки на этом экране. Другой способ сделать это — выполнить команду `secpol.exe` в поле поиска панели **Приложения** или в командной строке. В левой панели консоли разверните узел **Локальные политики** (Local Policies) и выберите в нем подузел **Политика аудита** (Audit Policy).
- Чтобы настроить политику для всей организации, в редакторе управления групповыми политиками откройте для изменения необходимый объект групповой политики. В правой панели консоли редактора разверните узел **Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики** и выберите в нем подузел **Политика аудита**.

Далее (для настройки как локальной, так и организационной политики) в правой панели консоли дважды щелкните на политике **Аудит доступа к объектам** (Audit object access). Откроется диалоговое окно **Свойства: Аудит доступа к объектам** (Audit access object Properties). Под надписью **Вести аудит следующих попыток доступа** (Audit these attempts) установите флажок **Успех** (Success), чтобы записывать в журнал успешные попытки доступа, или флажок **Отказ** (Failure), чтобы записывать в журнал неудачные попытки доступа, или же установите оба флажка, чтобы журналировать попытки доступа с исходом обоих типов. Нажмите кнопку **OK**, чтобы сохранить настройки и закрыть окно. Функциональность аудита будет включена, но нужно еще указать файлы и папки, подлежащие аудиту.

Настройка и применение аудита

Включив политику **Аудит доступа к объектам**, можно управлять отслеживанием использования файлов и папок, установив уровень аудита для отдельных папок и файлов. При этом следует иметь в виду, что возможность аудита доступна только для томов NTFS и правила наследования также применимы к аудиту файлов и папок. Это позволяет, например, выполнять аудит доступа к каждому файлу и папке тома, просто задав аудит корневой папки тома.

Указать файлы и папки для аудита можно следующим образом:

1. В Проводнике Windows щелкните правой кнопкой мыши на требуемой папке или файле и выберите в контекстном меню команду **Свойства**.
2. В диалоговом окне свойств перейдите на вкладку **Безопасность** и нажмите на ней кнопку **Дополнительно**.

3. В открывшемся диалоговом окне **Дополнительные параметры безопасности** перейдите на вкладку **Аудит** и нажмите на ней кнопку **Продолжить**. Откроется редактируемая версия вкладки **Аудит** (рис. 13.12).

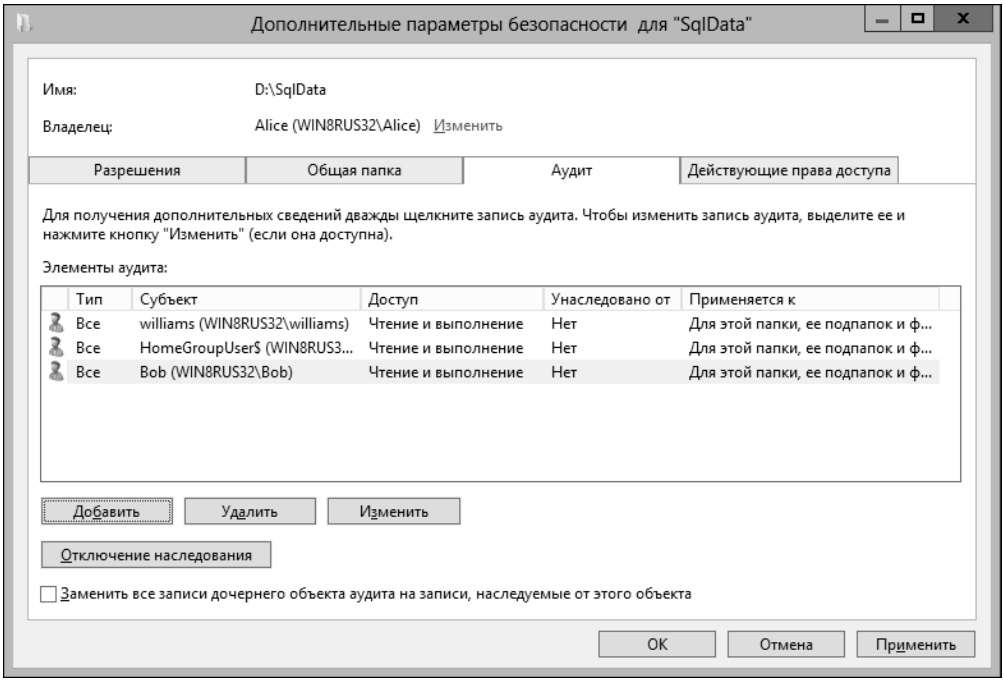


Рис. 13.12. Редактируемая версия вкладки **Аудит** для настройки параметров аудита файлов и папок

4. Нажмите кнопку **Добавить**, в результате откроется диалоговое окно **Элемент аудита для**. Щелкните в этом окне по ссылке **Выберите субъект** — откроется диалоговое окно **Выбор: "Пользователь" или "Группа"**.
5. Введите имя учетной записи пользователя или группы. Вводить нужно именно имя учетной записи пользователя, а не полное имя пользователя. Кроме этого, вводить можно только одно имя за раз.
6. Нажмите кнопку **Проверить имена**. Если для введенной учетной записи система найдет одно совпадение, список диалогового окна автоматически обновится и учетная запись будет подчеркнута. В противном случае появится другое диалоговое окно — **Имя не найдено**. Отсутствие совпадений означает, что либо имя было введено неправильно, либо используется не то размещение. Исправьте имя в диалоговом окне **Имя не найдено** и выполните поиск снова либо нажмите кнопку **Размещение**, чтобы выбрать новое место для поиска. Если для введенного имени система найдет несколько совпадений, которые выводятся в диалоговом окне **Найдено несколько имен**, выберите из них требуемое имя, а затем нажмите кнопку **OK**.
7. Нажмите кнопку **OK**. Выбранный пользователь или группа добавятся как **Субъект**, что отображается в диалоговом окне **Элемент аудита для**. По умолчанию это окно содержит список только основных разрешений. Щелчок по ссылке **Отображение дополнительных разрешений** (Show advanced permissions) выводит в панели **Дополнительные разрешения** список специальных разрешений (рис. 13.13).

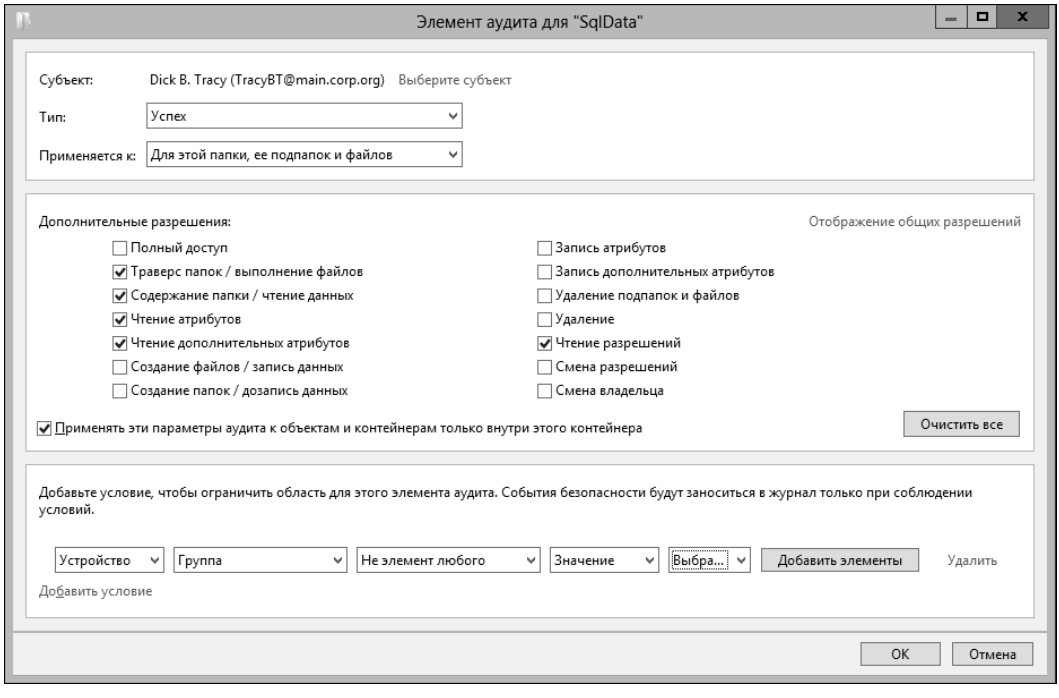


Рис. 13.13. Указание действий, подлежащих аудиту, для заданного пользователя, группы или компьютера

8. В раскрывающемся списке **Применяется к** (Applies to) выберите способ применения элемента аудита. Доступны следующие опции:
   - **Только для этой папки** (This folder only) — параметры аудита применяются только к текущей папке;
   - **Для этой папки, ее подпапок и файлов** (This folder, subfolders and files) — параметры аудита применяются к текущей папке и всем ее подпапкам и файлам, как в текущей папке, так и в ее подпапках;
   - **Для этой папки и ее подпапок** (This folder and subfolders) — параметры аудита применяются к текущей папке и ко всем ее подпапкам, но не к файлам в этих папках;
   - **Для этой папки и ее файлов** (This folder and files) — параметры аудита применяются к текущей папке и ко всем ее файлам, но не к ее подпапкам;
   - **Только для подпапок и файлов** (Subfolders and files only) — параметры аудита применяются ко всем подпапкам данной папки и ко всем файлам в этих папках, но не к самой текущей папке;
   - **Только для папок** (Subfolders only) — параметры аудита применяются ко всем подпапкам текущей папки, но не к самой папке и не к файлам в этих папках;
   - **Только для файлов** (Files only) — параметры аудита применяются ко всем файлам текущей папки и ко всем файлам ее подпапок, но не к самой текущей папке и не к ее подпапкам.
9. В раскрывающемся списке **Тип** выберите требуемый результат попытки доступа к объекту — успешный, неуспешный или оба, а затем укажите действия, подлежащие аудиту. Аудит можно применять к тем же действиям, для которых применяются специальные разрешения, перечисленные в табл. 13.1 и 13.3.

10. Если для папки требуется заменить параметры аудита для всех ее дочерних объектов (но не для самой папки), установите флажок **Применять эти параметры аудита к объектам и контейнерам только внутри этого контейнера** (Only apply these settings to objects and/or containers within this container).

> ***Практический совет***
>
> Параметр **Применяется к** позволяет указать объекты, к которым следует применять параметры аудита. А опция **Применять эти параметры аудита к объектам и контейнерам только внутри этого контейнера** управляет применением этих параметров аудита. Когда этот флажок установлен, параметры аудита родительского объекта заменяют параметры аудита дочерних объектов. А когда этот флажок снят, параметры аудита для родительского объекта сливаются с существующими параметрами аудита дочерних объектов.

11. Если используются политики на основе утверждений и нужно ограничить область действия элемента аудита, к нему можно добавить условия на основе утверждений. Например, если все компьютеры организации являются членами группы **Domain Computers**, желательно выполнять тщательный аудит доступа устройств, которые не являются членами этой группы.
12. Завершив настройку параметра аудита, нажмите кнопку **OK**, чтобы применить и сохранить их. Повторите этот процесс для других пользователей, групп или компьютеров.

Желательно почаще отслеживать неудачные попытки доступа. Таким образом, можно будет сфокусироваться на возможных несанкционированных попытках доступа. Но при этом следует иметь в виду, что неудачная попытка доступа не всегда означает, что кто-то пытается открыть папку, к которой ему запрещен доступ, со злым умыслом. Пользователь мог просто щелкнуть дважды мышью не на той папке или файле по ошибке. Кроме этого, некоторые типы действий могут записываться как повторные неудачные попытки, тогда как пользователь в действительности выполнил только одну попытку. Тем не менее всегда следует проверять повторные неудачные попытки доступа, из-за возможности несанкционированного доступа к компьютеру.

Все попытки обращения к файлам и папкам, для которых настроен аудит, записываются в журнал **Безопасность** системы. Его можно просмотреть в оснастке **Просмотр событий** консоли **Управление компьютером**. Успешные действия, такие как успешное чтение файлов, активируют запись успешных событий, а неудачные, например неуспешное удаление файла, активируют запись неуспешного события. Чтобы настроить расширенную политику аудита, в редакторе управления групповыми политиками откройте для редактирования требуемый объект групповой политики. Затем в дереве консоли редактора разверните узел **Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Конфигурация расширенной политики аудита\Политики аудита системы** (Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\System Audit Policies). Этот узел содержит следующие подузлы для настройки соответствующих политик аудита:

- **Вход учетной записи** (Account Logon);
- **Управление учетными записями** (Account Management);
- **Подробное отслеживание** (Detailed Tracking);
- **Доступ к службе каталогов (DS)** (DS Access);
- **Вход/Выход** (Logon/Logoff);
- **Доступ к объектам** (Object Access);
- **Изменение политики** (Policy Change);

- **Использование привилегий** (Privilege Use);
- **Система** (System);
- **Аудит доступа к глобальным объектам** (Global Object Access Auditing).

Выберите в левой панели требуемую категорию для аудита, например **Вход учетной записи**; в правой панели отобразится список подкатегорий. Дважды щелкните на подкатегории, которую требуется настроить, например **Аудит проверки учетных данных**. В открывшемся диалоговом окне свойств подкатегории установите флажок **Настроить следующие события аудита** (Configure the following audit events). Затем установите флажок **Успех**, **Отказ** или оба, чтобы указать тип события для отслеживания, после чего нажмите кнопку **OK**. В результате будет включен аудит для данной подкатегории.

ГЛАВА 14

Обеспечение доступа и готовности данных

Обеспечение доступа и готовности данных является одной из основных задач администрирования пользователей и систем. Кроме обычного управления файлами и папками, администратору часто приходится выполнять, среди прочих, такие ключевые задачи, как настройка опций Проводника Windows, настройка параметров автономных файлов, настройка дисковых квот, а также управление локальным кэшированием. Опции Проводника Windows контролируют доступные возможности управления файлами и папками, а также доступные типы файлов. Параметры автономных файлов контролируют наличие файлов и папок, когда пользователи работают в автономном режиме. Дисковые квоты устанавливают объем дискового пространства, доступный пользователям. Функциональность кэширования BranchCache сохраняет загруженные документы и файлы локально, для более быстрого доступа в дальнейшем.

Настройка параметров Проводника Windows

Если подумать об этом, то большая часть времени работы с компьютером уходит на управление файлами и папками. Пользователи создают файлы и папки для хранения и упорядочивания информации, перемещают их из одного места в другое, устанавливают разрешения для них и т. п. Так как на работу с файлами и папками тратится так много времени, несколько простых методов для эффективного управления ими помогут вам сэкономить значительный объем времени и усилий.

Настройка Проводника Windows

Проводник Windows является основным инструментом для работы с файлами и папками. К сожалению, его параметры по умолчанию настроены так, чтобы отвечать требованиям как можно более широкого круга пользователей, но не более жестким требованиям опытных пользователей или администраторов. Например, администраторам часто необходимо просматривать скрытые элементы и расширения файлов, которые по умолчанию в Проводнике Windows не отображаются.

В Windows 8 эти опции можно оперативно включить в панели **Представление**. Чтобы открыть эту панель, щелкните на одноименной вкладке Проводника Windows. Затем установите флажок **Скрытые элементы** (Hidden items), чтобы отображать скрытые элементы (но не защищенные файлы операционной системы), а для отображения расширений файлов

установите флажок **Расширения имен файлов** (File name extensions). Выполнить настройку других параметров Проводника Windows можно следующим образом:

1. На вкладке **Представление** Проводника Windows нажмите кнопку **Параметры** (Options). Откроется диалоговое окно **Параметры папок** (Folder Options) с выбранной вкладкой **Общие**.
2. Чтобы получить доступ к расширенным параметрам Проводника Windows, выберите вкладку **Вид** (рис. 14.1).

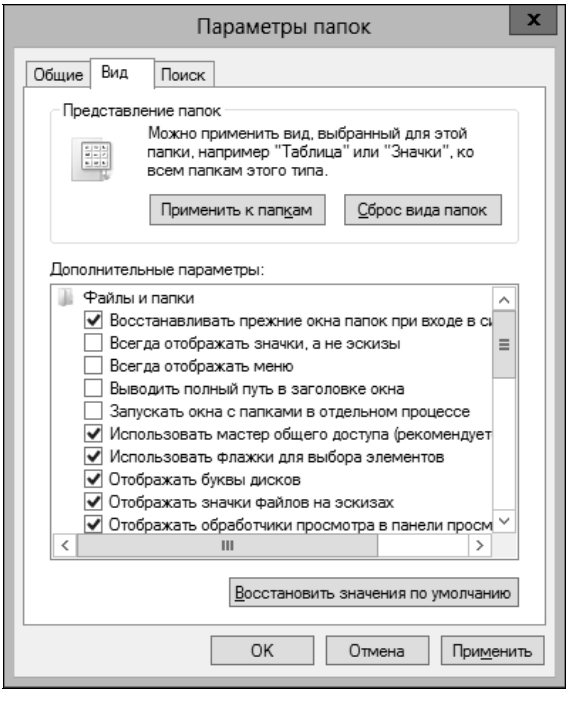


Рис. 14.1. Вкладка **Вид** окна **Параметры папок** для настройки расширенных параметров Проводника Windows

3. На этой вкладке можно выполнить настройку параметров Проводника Windows. Доступны следующие параметры.
   - **Всегда отображать значки, а не эскизы** (Always show icons, never thumbnails). По умолчанию Проводник Windows отображает большие эскизы файлов рисунков и других типов файлов. Для папок, содержащих большое число рисунков, это поведение может быть раздражающим, т. к. Проводник должен отобразить эскиз каждого рисунка, и для отображения эскизов всех изображений папки может понадобиться некоторое время. Чтобы отключить отображение эскизов рисунков, установите этот флажок.
   - **Отображать значки файлов на эскизах** (Display file icon on thumbnails). По умолчанию Проводник Windows добавляет к отображаемым эскизам значки файлов. Чтобы отображать эскизы без значков файлов, снимите этот флажок.
   - **Отображать сведения о размерах файлов в подсказках папок** (Display file size information in folder tips). По умолчанию при наведении указателя мыши на имя или значок папки Проводник Windows выводит всплывающую подсказку, содержащую дату и время создания папки, размер папки, а также частичный список содержащихся

в ней файлов. Чтобы отображать только дату и время создания папки, снимите этот флажок.

- **Выводить полный путь в заголовке окна** (Display the full path in the title bar). По умолчанию, если нажать комбинацию клавиш <Alt>+<Tab>, а затем отпустить клавишу <Tab>, удерживая при этом клавишу <Alt>, Windows открывает панель просмотра всех открытых в настоящее время окон. В этой панели требуемое окно можно выбрать, последовательно перемещаясь по значкам окон в панели, нажимая и отпуская клавишу <Tab> (продолжая удерживать нажатой клавишу <Alt>), или же указав требуемое окно с помощью мыши. По умолчанию в заголовке панели просмотра открытых окон для значков окон папок отображаются только имена папок. При установке этого флажка выводится полный путь к папкам в Проводнике Windows.
- **Скрытые файлы и папки** (Hidden files and folders). По умолчанию Проводник Windows не отображает скрытые файлы, папки или диски. Чтобы отображать эти элементы файловой системы, установите переключатель **Показывать скрытые файлы, папки и диски** (Show hidden files, folders and drives). (Этим параметром можно также управлять с помощью флажка **Скрытые элементы** на вкладке **Представление**.)
- **Скрывать пустые диски в папке "Компьютер"** (Hide empty drives in the Computer folder). По умолчанию Проводник Windows не отображает информацию о пустых дисках в окне **Компьютер**. Чтобы отображать информацию о пустых дисках, снимите этот флажок.
- **Скрывать расширения для зарегистрированных типов файлов** (Hide extensions for knows file types). По умолчанию Проводник Windows не отображает расширения файлов зарегистрированных типов. Чтобы отображать расширения файлов, снимите этот флажок. (Этим параметром можно также управлять с помощью флажка **Расширения имен файлов** на вкладке **Представление**.)
- **Скрыть конфликты слияния папок** (Hide folder merge conflicts). По умолчанию Проводник Windows не отображает информацию о конфликтах слияния папок. Чтобы отображать информацию о таких конфликтах, снимите этот флажок.
- **Скрывать защищенные системные файлы** (Hide protected operating system files). По умолчанию Проводник Windows не отображает файлы операционной системы. Чтобы отображать эти файлы, снимите этот флажок.
- **Запускать окна с папками в отдельном процессе** (Launch folder windows in a separate process). По умолчанию Windows выполняет все экземпляры Проводника Windows в одном процессе. Это позволяет сэкономить память и обычно ускоряет процесс открытия новых окон, но также означает, что все экземпляры Проводника Windows взаимосвязаны. Если в одном экземпляре происходит сбой, сбой также происходит во всех экземплярах, и если один экземпляр находится в состоянии ожидания, все другие экземпляры также могут быть заблокированы. Установите данный флажок, чтобы изменить это поведение и запускать новый процесс для каждого нового экземпляра Проводника Windows.
- **Восстанавливать прежние окна папок при входе в систему** (Restore previous folder windows at logon). Проводник Windows может запоминать открытые папки при выходе пользователя из системы и открывать их при следующем входе пользователя. По умолчанию эта возможность отключена. Чтобы включить эту возможность, установите этот флажок.
- **Отображать буквы дисков** (Show drive letters). По умолчанию Проводник Windows отображает буквы дисков в окне консоли **Компьютер** и в строке заголовка окон дисков. Снимите этот флажок, чтобы не отображать буквы дисков.

- **Отображать сжатые или зашифрованные файлы NTFS другим цветом** (Show encrypted or compressed NTFS files in color). По умолчанию Проводник Windows отображает имена зашифрованных и сжатых файлов другим цветом, чем обычные файлы. Имена зашифрованных файлов отображаются зеленым цветом, а сжатых — синим. Снимите этот флажок, чтобы эти файлы не отображались другим цветом.
- **Отображать описание для папок и элементов рабочего стола** (Show pop-up description for folder and desktop items). По умолчанию при наведении указателя мыши на файл или папку Проводник Windows выводит всплывающую подсказку с дополнительной информацией о данном элементе. Снимите этот флажок, чтобы не выводить эту всплывающую подсказку.
- **Отображать обработчики просмотра в панели просмотра** (Show preview handlers in preview pane). По умолчанию, когда включена область просмотра, в ней выполняется предварительный просмотр выбранных файлов или папок. Снимите этот флажок, чтобы отменить предварительный просмотр.
- **Показывать строку состояния** (Show status bar). По умолчанию Проводник Windows отображает строку состояния. Чтобы не отображать эту строку, снимите этот флажок.
- **Использовать флажки для выбора элементов** (Use check boxes to select items). По умолчанию Проводник Windows позволяет выбирать файлы, папки и другие элементы, используя только стандартные методы, такие как щелчок, щелчок при нажатой клавише <Shift> или щелчок при нажатой клавише <Ctrl>. Установка этого флажка позволяет выбирать несколько, не обязательно смежных, файлов или папок установкой их флажков.
- **Использовать мастер общего доступа** (Use Sharing Wizard). По умолчанию Проводник Windows использует мастер общего доступа для настройки общего доступа к файлам *(см. главу 13)*. Если желательно использовать только расширенные опции предоставления общего доступа к файлам, снимите этот флажок. Тогда для предоставления общего доступа нужно будет на вкладке **Доступ** окна свойств файла или папки нажать кнопку **Расширенная настройка** и настроить параметры разрешений, кэширования и подключений отдельно.
- **При вводе текста в режиме "Список"** (When typing into list view). По умолчанию для этой опции установлен переключатель **Выделять введенный элемент в списке** (Select the typed item in the view), вследствие чего при нажатии в папке клавиши буквы Проводник Windows выбирает в папке первый файл или папку, имя которой начинается с этой буквы. Если же установить переключатель **Автоматически вводить текст в поле поиска** (Automatically type into the Search Box), Проводник Windows будет помещать вводимый с клавиатуры текст в поле поиска.

Настройка расширенных параметров Проводника Windows

И пользователи, и администраторы проводят много времени, работая с Проводником Windows или с одним из связанных представлений, например консолью **Компьютер**. Администраторам часто хотелось бы иметь более продвинутые возможности использования Проводника Windows. Например, следующие:

- ♦ отключать определенные возможности Проводника Windows для некоторых компьютеров. Скажем, может быть желательным запретить пользователям доступ к вкладке **Оборудование**, чтобы они не могли просматривать или изменять оборудование компьютера;

- скрыть локальные диски или ограничить доступ к ним. Например, может требоваться предотвратить доступ пользователей к возможности записи CD/DVD-дисков.

Возможности настройки этих и других расширенных возможностей рассматриваются в этом разделе.

Установка групповой политики для Проводника Windows и представлений папок

Как и в случае со многими возможностями Windows 8, доступностью опций Проводника Windows можно управлять с помощью групповой политики. Так как многие из этих опций распространяются на представления и параметры папок, будет полезно исследовать их. В табл. 14.1 предоставлен обзор параметров политики, применение которых может быть полезным, а также описание особенностей использования этих параметров. Эти параметры политики находятся в узле редактора объекта групповой политики **Конфигурация пользователя\Административные шаблоны\Компоненты Windows\Проводник** (User Configuration\Administrative Templates\Windows Components\File Explorer).

Таблица 14.1. *Параметры групповой политики для Проводника Windows*

Имя параметра	Описание
Разрешить использование только пользовательских или зарегистрированных расширений (Allow only per user or approved shell extensions)	Расширения оболочки увеличивают набор функциональностей Проводника Windows. Этот параметр разрешает исполнение на компьютере только таких расширений оболочки, которые были одобрены администратором или не затрагивают других пользователей данного компьютера. Разрешенные расширения оболочки должны иметь запись в ключе реестра `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows \CurrentVersion\Shell Extensions\Approved`.
Запрашивать подтверждение при удалении файлов (Display confirmation dialog when deleting files)	Отображает диалоговое окно запроса подтверждения при удалении файлов или перемещения их в Корзину
Скрыть выбранные диски из окна "Мой компьютер" (Hide these specified drives in My Computer)	Скрывает значки указанных жестких дисков в окне Проводника. Но при этом доступ к этим дискам не ограничивается, и пользователи могут обращаться к ним другими способами
Скрыть команду "Управление" из контекстного меню Проводника (Hides the Manage item on the File Explorer context menu)	Удаляет значок **Управление** из меню Проводника и экрана **Пуск**. Этот значок используется для запуска консоли **Управление компьютером**
Запретить доступ к дискам через "Мой компьютер" (Prevent access to drives from My Computer)	Не позволяет пользователям использовать значок **Мой компьютер** для доступа к содержимому указанных дисков. Пользователи также не могут использовать для доступа к файлам на этих дисках команду **Выполнить** или **Подключить сетевой диск**
Удалить команды "Подключить сетевой диск" и "Отключить сетевой диск" (Remove "Map Network Drive" and "Disconnect Network Drive")	Запрещает подключение и отключение сетевых дисков посредством Проводника Windows. Данное действие не предотвращает выполнение этих операций посредством других способов, например из консоли командной строки
Удалить возможности записи компакт-дисков (Remove CD Burning features)	Удаляет доступ к средствам записи CD-дисков из Проводника Windows. Не влияет на использование других программ записи CD-дисков

Таблица 14.1 *(окончание)*

Имя параметра	Описание
Удалить вкладку DFS (Remove DFS tab)	Удаляет вкладку **DFS** из окон Проводника Windows и других окон на основе Проводника, предотвращая просмотр и изменение параметров распределенной файловой системы (DFS[1]). Обратите внимание, что вкладка **DFS** доступна только в том случае, если в рабочей группе или домене настроена распределенная файловая система
Удалить меню "Файл" из Проводника (Remove File menu from File Explorer)	Удаляет меню **Файл** из представлений Проводника, но не предотвращает выполнение пользователями заданий, доступных с этого меню, другими средствами
Удалить вкладку "Оборудование" (Remove Hardware tab)	Удаляет вкладку **Оборудование** из всех диалоговых окон, предотвращая просмотр, изменение или диагностирование аппаратных устройств через эту вкладку
Удалить вкладку "Безопасность" (Remove Security tab)	Удаляет вкладку **Безопасность** из всех диалоговых окон свойств для файлов, папок, ярлыков и дисков. Это не дает пользователям возможности просматривать или изменять разрешения файлов и папок
Запретить вывод контекстного меню по умолчанию для Проводника (Remove File Explorer's default context menu)	Отключает вывод контекстного меню при щелчке правой кнопкой мыши по рабочему столу или в Проводнике Windows
Запускать Проводник со свернутой в значок лентой (Start File Explorer with ribbon minimized)	Управляет отображением ленты инструментов Проводника — свернутая или развернутая — при запуске Проводника и для всех новых окон
Отключить кэширование эскизов изображений (Turn off caching of thumbnail pictures)	Отключает кэширование эскизов предпросмотра изображений
Отключить отображение эскизов и отображать только значки (Turn off the display of thumbnails and only display icons)	Отключает создание и отображение эскизов при просмотре локальных папок компьютера. Это может сократить время ожидания и ускорить первый доступ к папке, хотя пользователям придется просматривать изображения, чтобы разобраться с ними
Отключить отображение эскизов и отображать только значки в сетевых папках (Turn off the display of thumbnails and only display icons on network folders)	Отключает создание и отображение эскизов при просмотре сетевых папок. Это может сократить время ожидания и ускорить первый доступ к папке, хотя пользователям придется просматривать изображения, чтобы разобраться с ними
Отключить возможности библиотеки Windows, использующие данные индексированных файлов (Turn off Windows Libraries features that rely on indexed file data)	Отключает все представления упорядочения, за исключением представления **По папке**, и все предлагаемые варианты фильтра поиска, кроме **Дата изменения** и **Размер**. Также отключает просмотр фрагментов содержимого файлов в режиме **Содержимое** и исключает библиотеки из поиска в меню **Пуск**

[1] Distributed file system.

Как можно видеть в табл. 14.1, многие параметры политики для Проводника Windows управляют наличием таких опций, как элементы меню и вкладки диалоговых окон. Настроить эти опции для всех пользователей компьютера можно следующим образом:

1. В редакторе управления групповыми политиками откройте для редактирования требуемый объект групповой политики. Рассматриваемые параметры политики находятся в узле **Конфигурация пользователя\Административные шаблоны\Компоненты Windows\ Проводник**.
2. Дважды щелкните мышью на необходимом параметре политики и в открывшемся диалоговом окне свойств параметра установите один из следующих переключателей:
   - **Не задано** — для этого параметра политики в реестр не будет внесено никаких изменений;
   - **Включить** — включает параметр политики и обновляет реестр;
   - **Отключить** — отключает параметр политики и обновляет реестр.
3. Нажмите кнопку **OK**, чтобы закрыть окно настройки параметра политики.

Примечание

Некоторые из этих параметров политики рассматриваются более подробно в последующих разделах этой главы. В частности, прочитайте следующий раздел, *"Управление доступом к дискам в Проводнике"*, в котором рассматривается, как скрыть диски или предотвратить доступ к ним в Проводнике Windows.

Управление доступом к дискам в Проводнике

Иногда может потребоваться заблокировать доступ к файлам на определенных дисках или даже не отображать некоторые диски в Проводнике. Этими аспектами доступа к файловой системе можно управлять посредством групповой политики, а именно параметрами **Скрыть выбранные диски из окна "Мой компьютер"** и **Запретить доступ к дискам через "Мой компьютер"**.

Скрытие дисков не позволяет пользователям получить доступ к ним в представлениях Проводника, но не может помешать им получить доступ другими способами. В противоположность, запрет доступа к дискам предотвращает доступ пользователями ко всем файлам на дисках, а также не позволяет получить доступ к этим файлам, используя Проводник или команду **Исполнить** или **Подключить сетевой диск**. Но при этом значки дисков и структура папок продолжают отображаться в Проводнике.

Скрыть выбранные диски или запретить доступ к файлам на выбранных дисках можно следующим способом:

1. В редакторе управления групповыми политиками откройте для редактирования необходимый объект групповой политики. Требуемые параметры политики находятся в узле **Конфигурация пользователя\Административные шаблоны\Компоненты Windows\ Проводник**.
2. Чтобы скрыть диски, дважды щелкните на параметре политики **Скрыть выбранные диски из окна "Мой компьютер"** и в открывшемся окне свойств параметра установите переключатель **Включить**. Далее укажите диски, которые нужно скрыть, после чего нажмите кнопку **OK**. Доступны следующие основные опции:
   - **Ограничить доступ ко всем дискам** (Restrict all drives) — ограничивается доступ ко всем внутренним приводам жестких и гибких дисков;
   - **Ограничить доступ к дискам A и B** (Restrict A and B drives only) — ограничивается доступ только к приводам гибких дисков;

- **Ограничить доступ к дискам A, B и C** (Restrict A, B and C drives only) — ограничивается доступ только к приводам гибких дисков и жесткому диску C:;
- **Ограничить доступ к диску C** (Restrict C drive only) — ограничивается доступ только к жесткому диску C:;
- **Ограничить доступ к диску D** (Restrict D drive only) — ограничивается доступ только к жесткому диску D:;
- **Не ограничивать доступ к дискам** (Do not restrict drives) — удаляются дополнительные ограничения, которые могли бы применяться в противном случае.

3. Чтобы заблокировать доступ к файлам на определенных дисках, дважды щелкните на параметре политики **Запретить доступ к дискам через "Мой компьютер"** и установите для него флажок **Включить**. Затем выберите диски, к которым требуется запретить доступ, и нажмите кнопку **OK**.

Примечание

Разрешение **Список содержимого** папки определяет, может ли пользователь просматривать содержимое папки. Чтобы пользователь не мог просматривать список имен папок диска, следует также скрыть диски. Это будет самым легким способом скрыть все папки диска от просмотра.

Управление автономными файлами

Настройка автономных файлов представляет собой многоэтапный процесс, который начинается с установки соответствующих значений параметров групповой политики, продолжается настройкой конкретных автономных папок и завершается установкой параметров пользователя для автономной работы. Хотя работающие автономно пользователи — это в основном пользователи, работающие на ноутбуках, которые они берут с собой домой или в командировку, настройка автономных файлов может быть полезной и для других типов пользователей. Основы настройки параметров групповой политики для автономных файлов рассматриваются в *главе 5*. В этом разделе предоставляется более подробная информация об автономных файлах и излагаются конкретные шаги по их настройке.

Что такое автономные файлы

Автономные файлы позволяют пользователям сохранять содержимое сетевых дисков на своих компьютерах, чтобы иметь возможность работать с ним, когда они не подключены к сети по какой-либо причине. После настройки автономных файлов Windows 8 использует их, когда исходные файлы на сетевом диске недоступны. Это позволяет пользователям продолжать работать с сетевыми файлами без перебоев. После восстановления подключения к сети Windows 8 синхронизирует автономные файлы на компьютере пользователя с соответствующими исходными файлами в сетевой папке.

Способ выполнения такой синхронизации зависит от особенностей изменений автономных файлов. Если изменения в определенный автономный файл внесены несколькими пользователями, они могут прибегнуть к возможностям разрешения конфликтов, чтобы сохранить свою версию файла, заменив ею существующую, оставить без изменений существующую версию файла или же сохранить в сетевой папке обе версии. Если пользователь удаляет автономный файл, этот файл также удаляется и из сетевой папки, за исключением, если другой пользователь изменил этот сетевой файл, и он теперь имеет более позднюю дату и время. В этом исключительном случае файл удаляется с компьютера пользователя, но не из сетевой папки. Если пользователь изменяет автономный файл, который был удален из сете-

вой папки другим пользователем, первый пользователь может либо сохранить свой автономный файл в сетевой папке, либо удалить его со своего компьютера.

Операционная система Windows 8 предоставляет несколько функциональностей, которые влияют на использование автономных файлов.

- **Синхронизация только изменений.** Синхронизация выполняется только для измененных блоков файлов, что обеспечивает более быстрое выполнение операции синхронизации. В процессе синхронизации на сервер записываются только измененные блоки файлов.
- **Дублирование недоступных файлов и папок.** Когда часть содержимого сетевой папки предоставляется для автономного использования, Windows 8 создает несинхронизированные дубликаты других файлов и папок, чтобы сохранить целостность сетевого содержимого. Когда пользователь не подключен к сетевой папке, ему предоставляются дублированные экземпляры сетевых элементов, а также обычные автономные элементы.
- **Разгрузка компьютеров для передачи данных.** Это прозрачная в работе и автоматически включающаяся возможность Windows Server 2012. Суть ее заключается в том, что при копировании или перемещении данных внутри или между совместимыми массивами устройств хранения данных сами данные перемещаются напрямую между устройствами хранения, в обход компьютеров, использующих эти данные. Например, если пользователь копирует или перемещает папку из общей папки с одного файлового сервера на другой, и эти два сервера используют совместимые массивы устройств хранения данных (или один и тот же массив), данные будут передаваться напрямую между устройствами хранения, в обход связанных компьютеров.
- **Синхронизация в платных сетях.** По умолчанию автономные файлы не синхронизируются в фоновом режиме при работе в сотовых и других сетях, в которых может взиматься плата при роуминге, либо при приближении к пределу объема передачи данных тарифного плана или его превышении. Пороговое значение для переключения в режим медленного подключения можно настроить, используя параметр политики **Настроить режим медленного подключения**; а фоновую синхронизацию — используя параметр политики **Включить синхронизацию файлов в платных сетях**. Эти параметры политики находятся в узле редактора групповой политики **Конфигурация компьютера\Административные шаблоны\Сеть\Автономные файлы**.
- **Кэширование перенаправленных папок.** По умолчанию специальные папки, которые перенаправляются на сетевые диски, автоматически доступны в автономном режиме. Если к перенаправленным специальным папкам не нужно предоставлять доступа в автономном режиме, кэширование этих папок можно отключить с помощью параметра политики **Не предоставлять автоматически автономный доступ к определенным перенаправленным папкам** (Do no automatically make specific redirected folders available offline). Этот параметр политики находится в узле редактора управления групповыми политиками **Конфигурация пользователя\Административные шаблоны\Система\ Перенаправление папок**.

Как пользователи, так и администраторы могут управлять тем, когда выполнять синхронизацию автономных файлов. Также автоматическая синхронизация может активироваться при входе пользователя в систему и выходе из нее и при переходе компьютера в режим сна или гибернации. Точные условия автоматической синхронизации зависят от параметров групповой политики и пользовательских настроек. Подробную информацию по настройке автономных файлов посредством групповой политики *см. в разд. "Настройка политики автономных файлов" главы 5*.

Пользователь может инициировать синхронизацию всей сетевой папки, конкретной подпапки и ее содержимого или же конкретного файла. Для этого в Проводнике Windows нужно щелкнуть правой кнопкой мыши на ресурсе и в контекстном меню выбрать команду **Синхронизировать**, а во вложенном меню — команду **Синхронизировать выбранные автономные файлы** (Sync selected offline files).

Синхронизацией также можно управлять вручную из Центра синхронизации, который можно открыть одним из следующих способов:

- в правом верхнем углу Панели управления щелкните по ссылке **Просмотр** (View by) и выберите опцию **Крупные значки** (Large icons) или **Мелкие значки** (Small icons). В списке оснасток щелкните по значку **Центр синхронизации**;
- в поле поиска панели **Приложения** выполните команду `mobsync.exe`.

Предоставление доступа к общим сетевым файлам и папкам в автономном режиме

Общие сетевые папки можно предоставить для использования в автономном режиме. По умолчанию все содержимое общих папок также будет доступно в автономном режиме. Если необходимо, можно настроить доступность отдельных файлов и подпапок. Следует иметь в виду, что файлы, добавленные в общую папку, которая настроена для автономного использования, не распределяются автоматически работающим автономно пользователям. Для получения обновлений автономную папку необходимо синхронизировать.

Настройку автономных файлов можно выполнять с помощью Проводника Windows или консоли **Управление компьютером**. Лучше всего использовать консоль **Управление компьютером**, т. к. она позволяет работать и управлять автономными файлами на любом из компьютеров сети. Предоставление доступа к общим сетевым файлам и папкам в автономном режиме является трехэтапным процессом. Сначала предоставляется общий доступ к папкам, далее эти папки настраиваются для автономного использования, а затем пользователи указывают файлы и папки, которые они хотят использовать в автономном режиме.

Шаг 1. Предоставление общего доступа к папкам

В консоли **Управление компьютером** предоставление общего доступа к папкам выполняется следующим образом:

1. Нажмите или щелкните правой кнопкой мыши на узле **Управление компьютером** в дереве консоли и в контекстном меню выберите команду **Подключиться к другому компьютеру**. С помощью открывшегося диалогового окна **Выбор компьютера** выберите требуемый компьютер.
2. В дереве консоли разверните узел **Служебные программы\Общие папки** (System Tools\Shared Folders) и выберите в нем папку **Общие ресурсы** (Shares). В панели сведений будут отображены текущие общие ресурсы.
3. Щелкните правой кнопкой мыши на папке **Общие ресурсы** и в контекстном меню выберите команду **Новый общий ресурс**. Запустится мастер создания общих ресурсов, с помощью которого предоставьте общий доступ к требуемым папкам *(см. разд. "Предоставление общего сетевого доступа к ресурсу и настройка уровня доступа с помощью консоли Управление компьютером" главы 13)*.

Шаг 2. Настройка общих папок для автономного использования

В консоли **Управление компьютером** настройка автономного использования общих папок выполняется следующим образом:

1. Нажмите или щелкните правой кнопкой мыши на узле **Управление компьютером** в дереве консоли и в контекстном меню выберите команду **Подключиться к другому компьютеру**. С помощью открывшегося диалогового окна **Выбор компьютера** выберите требуемый компьютер.
2. В дереве консоли разверните узел **Служебные программы\Общие папки** и выберите в нем папку **Общие ресурсы**.
3. Дважды щелкните на общей папке, которую требуется настроить для использования в автономном режиме. На вкладке **Общие** открывшегося окна свойств папки нажмите кнопку **Настройка** (Offline Settings).
4. В открывшемся диалоговом окне **Настройка автономного режима** (рис. 14.2) выберите одну из следующих опций.
   - **Вне сети доступны только указанные пользователем файлы и программы** (Only the files and programs that users specify are available offline). Установите этот переключатель, когда требуется, чтобы пользователи указали файлы и папки, с которыми они хотят работать в автономном режиме. Эта опция выбрана по умолчанию и является оптимальной, когда многие пользователи хотят изменять одни и те же файлы в папке. После настройки ручного кэширования файлы автоматически загружаются и предоставляются для автономного использования. Кэшированные ранее более старые версии файлов удаляются. При использовании файла в сети серверная версия файла всегда указывает, что файл используется. Для этой опции можно также включить BranchCache. Эта функциональность позволяет компьютерам в филиалах организации кэшировать загруженные из общих папок файлы, а затем предоставлять эти файлы для общего использования другими компьютерами филиала.

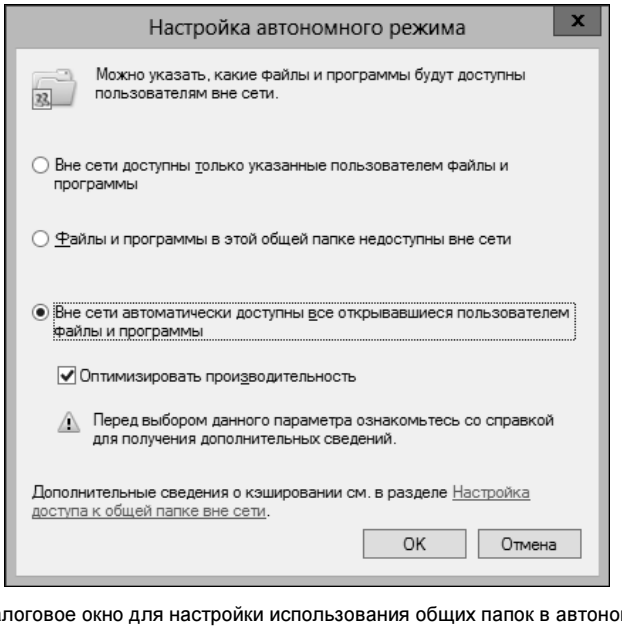


Рис. 14.2. Диалоговое окно для настройки использования общих папок в автономном режиме

- **Вне сети автоматически доступны все открывавшиеся пользователем файлы и программы** (All files and programs that users open from the shared folder are automatically available offline). Эта опции используется для папок, содержащих пользовательские данные и программы. Открытые файлы документов и исполняемых программ автоматически загружаются и предоставляются для автономного использования. Кэшированные ранее более старые версии файлов удаляются из локального кэша. При использовании файла в сети серверная версия файла всегда указывает, что файл используется. В случае конфликтов версий выводятся соответствующие уведомления.

  Для этой опции можно также задать дополнительную опцию, **Оптимизировать производительность** (Optimize for performance), чтобы разрешить расширенное кэширование программ. Расширенное кэширование позволяет кэшировать локально программы общего сетевого доступа, чтобы их можно было выполнять локально, что повышает производительность.

5. Последовательно нажмите кнопку **OK**, чтобы закрыть все окна.

Шаг 3. Задание файлов и папок для автономного использования

После создания общих ресурсов и настройки их работы в автономном режиме можно указать файлы и папки для использования в автономном режиме. Процедура для этого следующая:

1. Подключите общую папку в виде сетевого диска, как рассматривается в *разд. "Доступ к общим ресурсам и их использование" главы 13*.
2. В строке адреса окна Проводника Windows щелкните по значку выбора места и в контекстном меню выберите команду **Компьютер**, в результате чего в правой панели откроется консоль **Компьютер**.
3. Создайте кэш автономных файлов одним из следующих способов.
   - Скопируйте содержимое общей папки на локальный компьютер и настройте его для автономного использования. Для этого в разделе **Сетевое размещение** консоли **Компьютер** щелкните правой кнопкой мыши на подключенном сетевом диске и в контекстном меню выберите команду **Всегда доступны вне сети**.
   - Скопируйте на локальный компьютер только требуемую папку сетевого диска (и ее содержимое) или отдельный файл и настройте их для автономного использования. Для этого на сетевом диске выберите требуемый объект, щелкните на нем правой кнопкой мыши и в контекстном меню выберите опцию **Всегда доступны вне сети**.

Операция назначения файлов и папок для автономного использования создает локальный кэш содержимого этих файлов и папок на компьютере пользователя. Это также устанавливает связь синхронизации между локальным компьютером и компьютером, предоставляющим общий ресурс, или расширяет существующую связь синхронизации, включая в нее дополнительные файлы и папки. Связи синхронизации управляются с помощью Центра синхронизации *(см. следующий раздел, "Управление синхронизацией автономных файлов")*.

Компьютер работает в автономном режиме, когда он не подключен к локальной сети либо к общему ресурсу. О том, что компьютер работает в автономном режиме, пользователь уведомляется значком красного крестика на сетевом диске в окне **Компьютер** или на значке сетевого подключения в области уведомлений панели задач. В автономном режиме с файлами сетевого диска можно работать точно таким же образом, как и при подключении к сети. Также пользователь обладает такими же разрешениями, как и при работе в сети. Поэтому, если для определенного общего ресурса пользователь имеет только разрешения чте-

ния при работе в сети, он будет иметь точно такие же полномочия и при работе в автономном режиме и не сможет вносить никаких изменений в ресурс.

Управление синхронизацией автономных файлов

Синхронизация кэша автономных файлов поддерживает файлы на клиентском компьютере в актуальном состоянии и применяет выполненные пользователем изменения к файлам в общей папке. Как именно выполняется синхронизация, зависит от скорости сетевого соединения и типа сети (т. е. выполняется ли синхронизация по платной сети).

Для управления кэшированными автономными файлами и папками применяется Центр синхронизации (рис. 14.3).

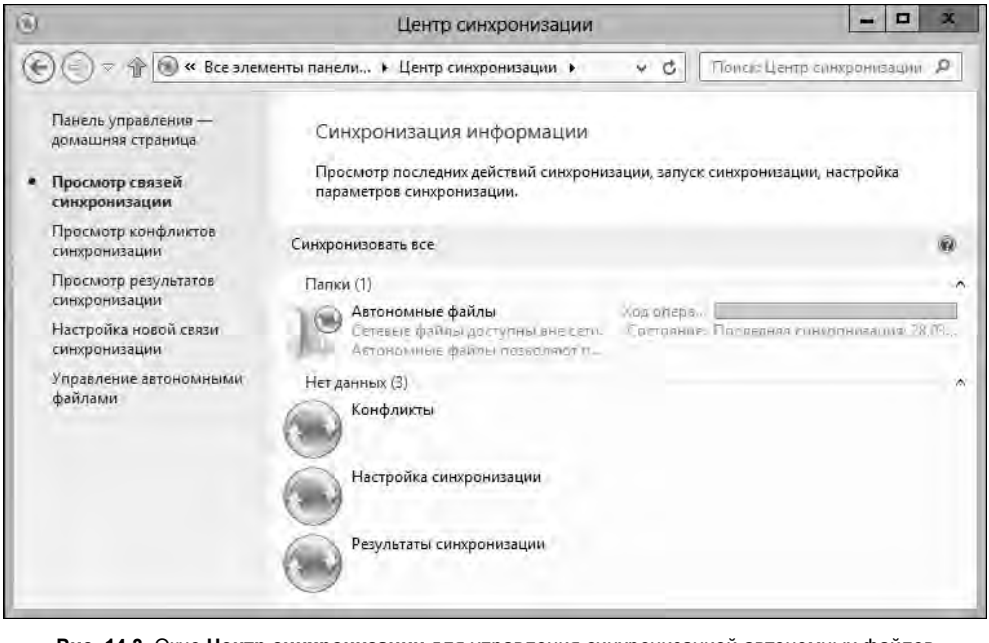


Рис. 14.3. Окно **Центр синхронизации** для управления синхронизацией автономных файлов

В Центре синхронизации для каждой общей папки, содержимое которой кэшируется локально, устанавливается *связь синхронизации* (sync partnership). Каждая связь синхронизации обладает набором свойств, которые позволяют управлять синхронизацией и способом ее выполнения.

Открыть Центр синхронизации можно из Панели управления. Для этого в правом верхнем углу Панели управления щелкните по ссылке **Просмотр** и выберите опцию **Крупные значки** или **Мелкие значки**, а затем в списке оснасток щелкните по значку **Центр синхронизации**. В открывшемся окне оснастки можно с легкостью проверить наличие проблем синхронизации, запустить или остановить процесс синхронизации либо настроить параметры синхронизации.

По умолчанию при открытии Центра синхронизации отображается страница **Просмотр связей синхронизации** (View sync partnership). На этой странице можно вручную синхронизировать автономные файлы. Для этого нужно щелкнуть правой кнопкой мыши по элементу **Автономные файлы** (Offline Files) и в контекстном меню выбрать команду **Синхронизация "Автономные файлы"** (Sync Offline Files).

Управление особенностями синхронизацией автономных файлов выполняется посредством групповой политики. Обычно автономные файлы синхронизируются автоматически, когда пользователь подключается к сети после работы вне сети. Также можно настроить время выполнения синхронизации:

- в определенное, запланированное время;
- при входе пользователя в систему;
- когда компьютер простаивает;
- когда пользователь выполняет блокировку или разблокировку Windows.

Планирование синхронизации

Для создания у управления расписанием синхронизации применяется следующая процедура:

1. В Центре синхронизации щелкните правой кнопкой мыши на связи синхронизации и в контекстном меню выберите команду **Расписание для "Автономные файлы"** (Schedule for Offline Files).
2. Если для этого ресурса ранее уже была запланирована синхронизация, мастер синхронизации предоставит следующие варианты действий:
   - **Создать новое расписание синхронизации** (Create a new sync schedule) — щелкните на этой ссылке, а затем выполните шаги 3—7;
   - **Просмотреть или изменить существующее расписание синхронизации** (View or edit an existing schedule) — щелкните на этой ссылке, выберите на следующей странице мастера требуемое расписание, нажмите кнопку **Далее**, а затем выполните шаги 3—7;
   - **Удалить существующее расписание синхронизации** (Delete an existing schedule) — щелкните на этой ссылке, выберите расписание, которое требуется удалить, и нажмите кнопку **Удалить**. Нажмите кнопку **OK** и пропустите остальные шаги.
3. Просмотрите список объектов для синхронизации и снимите флажки для тех объектов, настраивать которые не требуется. Нажмите кнопку **Далее** и на следующей странице щелкните по ссылке **В указанное по расписанию время** (At a scheduled time).
4. На следующей странице опции даты и времени начала запланированной синхронизации по умолчанию установлены на текущие день и время (рис. 14.4). Чтобы начать запланированную синхронизацию в другой день и время, измените эти параметры.
5. Параметр **Повторять каждые** (Repeat every) задает интервал синхронизации и по умолчанию установлен на выполнение синхронизации каждый день. Интервал повторения можно задать в минутах, часах, днях, неделях или месяцах. Так как синхронизируются только измененные объекты, желательно выполнять синхронизацию чаще, чем это делалось в более ранних версиях Windows. Например, синхронизацию важных файлов желательно выполнять каждые 3—4 часа.
6. Чтобы настроить дополнительные условия запуска и остановки синхронизации, нажмите кнопку **Дополнительно** (More options). По умолчанию синхронизация запускается, только если компьютер не находится в режиме сна или гибернации. Можно также задать следующие условия запуска и остановки синхронизации:
   - запускать синхронизацию, только если компьютер простаивает, по крайней мере, в течение *N* минут, где значение *N* предоставляется пользователем или администратором;
   - запускать синхронизацию, только если компьютер работает от сети (а не от батареи);

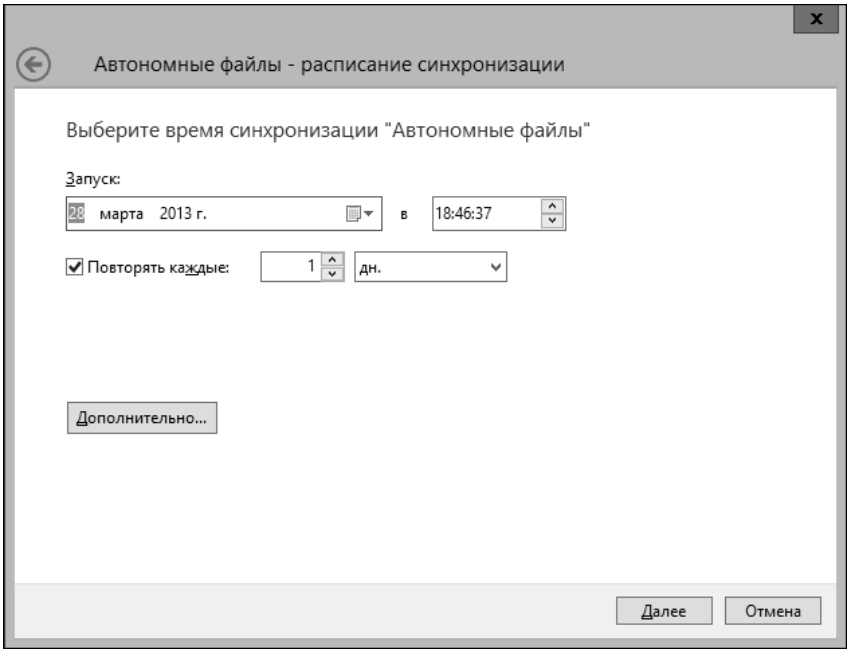


Рис. 14.4. Страница создания нового расписания синхронизации

- останавливать синхронизацию, если компьютер выходит из бездействия;
- останавливать синхронизацию, если компьютер перестает получать питание от сети.

7. Задав желаемые значения параметрам расписания синхронизации, нажмите кнопку **Далее**. На следующей странице введите описательное имя для расписания, а затем нажмите кнопку **Сохранить расписание** (Save Schedule).

Синхронизация по событию или действию

Для создания и управления синхронизацией по событию или действию применяется следующая процедура:

1. В Центре синхронизации щелкните правой кнопкой мыши на связи синхронизации и в контекстном меню выберите команду **Расписание для "Автономные файлы"**.
2. Если для этого ресурса ранее уже была запланирована синхронизация, мастер синхронизации предоставит следующие варианты действий:
   - **Создать новое расписание синхронизации** — щелкните на этой ссылке, а затем выполните шаги 3—5;
   - **Просмотреть или изменить существующее расписание синхронизации** — щелкните на этой ссылке, выберите на следующей странице мастера требуемое расписание, нажмите кнопку **Далее**, а затем выполните шаги 3—5;
   - **Удалить существующее расписание синхронизации** — щелкните на этой ссылке, выберите расписание, которое требуется удалить, и нажмите кнопку **Удалить**. Нажмите кнопку **OK** и пропустите остальные шаги.
3. Просмотрите список объектов для синхронизации и снимите флажки для тех объектов, для которых не требуется выполнять настройку, а затем нажмите кнопку **Далее**. На сле-

дующей странице мастера щелкните по ссылке **Когда происходит определенное событие** (When an event occurs).

4. На следующей странице мастера (рис. 14.5) установите соответствующие флажки, чтобы указать события или действия для автоматического запуска синхронизации. Доступны следующие опции:
   - когда пользователь входит в систему;
   - когда компьютер простаивает в течение *N* минут, где значение *N* предоставляется пользователем или администратором;
   - когда пользователь заблокирует компьютер;
   - когда пользователь разблокирует компьютер.

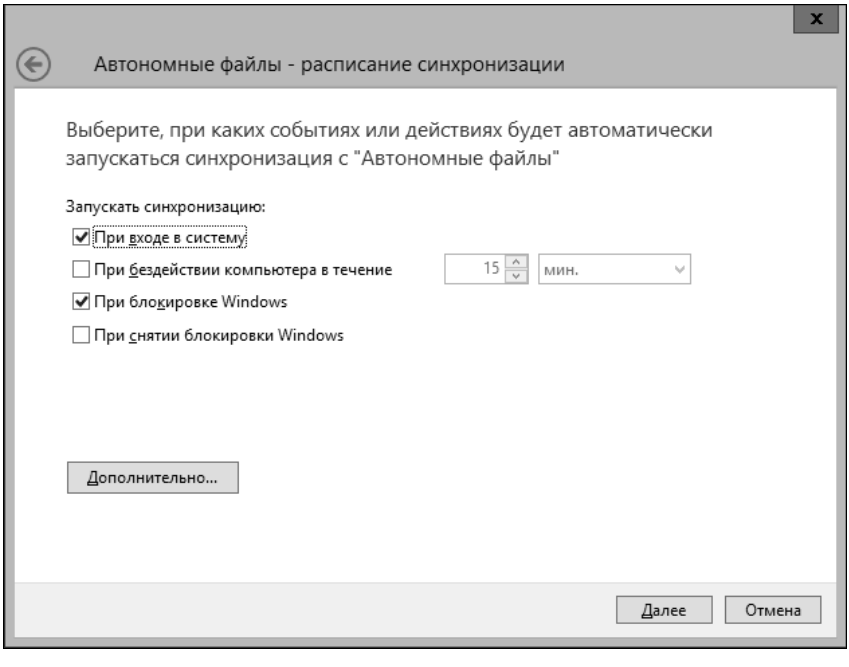


Рис. 14.5. Страница мастера для задания синхронизации по событию или действию

5. Задав желаемые значения параметрам запуска синхронизации по событию, нажмите кнопку **Далее**. На следующей странице введите описательное имя для запланированной синхронизации, а затем нажмите кнопку **Сохранить расписание**.

Устранение конфликтов и ошибок синхронизации

В результатах выполнения синхронизации предоставляются подробные сведения, сообщения об ошибках и предупреждения. Чтобы просмотреть текущие результаты синхронизации, откройте Центр синхронизации, а затем щелкните в левой панели по ссылке **Просмотр результатов синхронизации** (View sync results). Просмотр подробных сведений о результатах синхронизации поможет определить, когда синхронизация была запущена, остановлена или завершена. Также при просмотре результатов синхронизации можно узнать, нет ли каких-либо проблем с настройками конфигурации.

Конфликты синхронизации происходят, когда пользователь изменяет автономный файл, который обновляется на сервере другим пользователем. Просмотреть наличие конфликтов синхронизации и разрешить их (если таковые имеются) можно следующим образом:

1. В левой панели Центра синхронизации щелкните по ссылке **Просмотр конфликтов синхронизации** (View sync conflicts).
2. В панели сведений будет показано, имеются ли какие-либо конфликты (рис. 14.6).

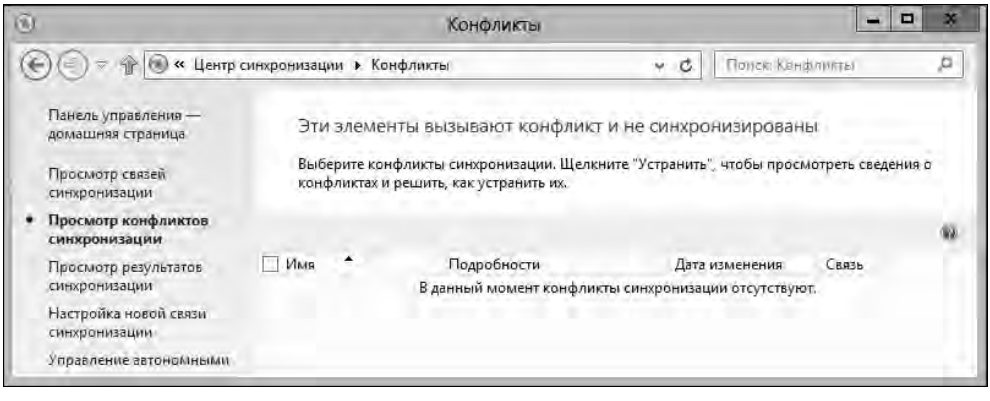


Рис. 14.6. Для конфликтов отображается такая информация, как имя документа, тип файла, время, связь и тип конфликта

3. Двойной щелчок по конфликту, который требуется разрешить, открывает диалоговое окно **Устранить конфликт** (Resolve Conflict).
4. Здесь можно выполнять следующие операции.
   - Щелкните на версии файла, которую нужно оставить. Чтобы оставить локальную версию, заменив ею сетевую версию, щелкните на версии **На этом компьютере** (On this computer). Чтобы оставить сетевую версию, заменив ею локальную версию, щелкните на версии, которая находится в общей сетевой папке.
   - Чтобы записать локальную версию в общую сетевую папку под новым именем, щелкните на опции **Сохранить обе версии** (Keep both versions). Обычно новому файлу присваивается такое же имя, как и у старого, но с числовым суффиксом, указывающим инкремент версии. Если вы не уверены, какую версию файла нужно оставить, сохраните обе версии, а затем тщательно исследуйте их на наличие изменений, которые нужно объединить или отвергнуть.

Настройка ограничений использования диска для автономных файлов

В Центре синхронизации можно управлять объемом дискового пространства, выделяемого для хранения автономных файлов. По умолчанию максимальный объем дискового пространства, который можно использовать для автономных файлов, указывается как процент объема диска, используемого для хранения профилей пользователей, от общего объема диска. Настроить ограничения объема диска для автономных файлов можно следующим образом:

1. В левой панели Центра синхронизации щелкните по ссылке **Управление автономными файлами**. Откроется диалоговое окно **Автономные файлы** (Offline Files).

2. На вкладке **Использование диска** (Disk Usage) этого окна отображается информация о дисковом пространстве, используемом всеми автономными файлами и связанными временными файлами (рис. 14.7). Временные файлы создаются в процессе работы пользователей с автономными файлами.

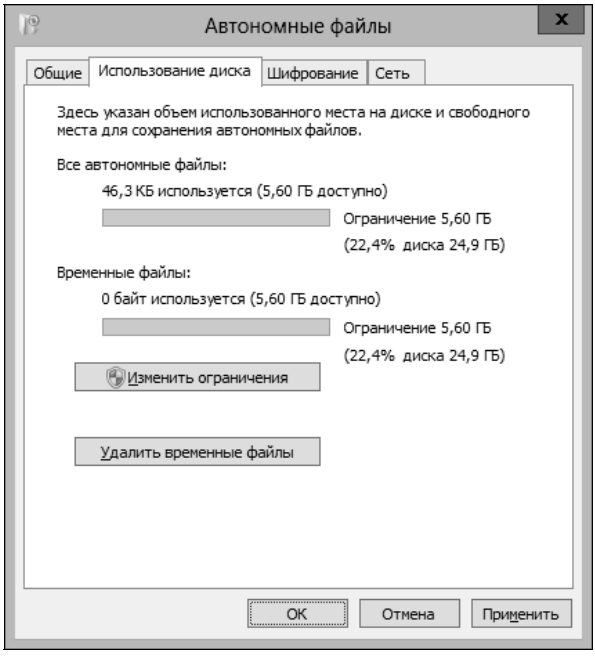


Рис. 14.7. Окно для настройки ограничений использования диска для автономных файлов

3. Обратите внимание на ограничение для всех автономных файлов и связанных временных файлов. Это ограничение указывается в мегабайтах (МБ) или гигабайтах (ГБ), а также как процент от общего объема диска, на котором хранятся профили пользователей.
4. Чтобы изменить эти ограничения, нажмите кнопку **Изменить ограничения** (Change limits). В открывшемся диалоговом окне **Ограничения места на диске для автономных файлов** (Offline files disk usage limits) с помощью горизонтальных ползунков установите требуемые ограничения дискового пространства для хранения всех автономных файлов и связанных временных файлов, после чего нажмите кнопку **OK**.
5. Чтобы удалить неиспользуемые временные файлы, нажмите кнопку **Удалить временные файлы** (Delete temporary files). Удаление временных файлов не затрагивает локальных копий сетевых файлов.
6. Завершив выполнение настроек, нажмите кнопку **OK**, чтобы сохранить их и закрыть диалоговое окно.

Управление шифрованием автономных файлов

Для повышения безопасности автономные файлы можно шифровать. При этом шифруются только копии файлов, хранящиеся на локальном компьютере, но не оригиналы в сетевой папке. Для работы с зашифрованными файлами пользователям не требуется самим расшиф-

ровывать их, т. к. это делается автоматически операционной системой. Шифрование автономных файлов выполняется следующим образом:

1. В левой панели Центра синхронизации щелкните по ссылке **Управление автономными файлами**. Откроется диалоговое окно **Автономные файлы**.
2. На вкладке **Шифрование** (Encryption) этого окна посмотрите, зашифрованы ли уже автономные файлы или еще нет. Если еще не зашифрованы, нажмите кнопку **Зашифровать**, чтобы зашифровать все автономные файлы, а по завершению шифрования нажмите кнопку **OK**, чтобы закрыть диалоговое окно.

Расшифровать зашифрованные автономные файлы можно, нажав кнопку **Расшифровать** (Unencrypt) на вкладке **Шифрование** окна **Автономные файлы**.

Запрещение автономного использования файлов

Администратор может запретить автономное использование определенных файлов или папок. Обычно такая надобность возникает, когда общая папка содержит определенные файлы, которыми пользователи не должны манипулировать. Чтобы запретить использование файла в автономном режиме, необходимо задать конкретную политику исключения *(см. разд. "Настройка политики автономных файлов" главы 5)*.

В консоли **Управление компьютером** запретить автономное использование общей папки можно следующим образом:

1. Нажмите или щелкните правой кнопкой мыши на узле **Управление компьютером** в дереве консоли и в контекстном меню выберите команду **Подключиться к другому компьютеру**. С помощью открывшегося диалогового окна **Выбор компьютера** выберите требуемый компьютер.
2. В дереве консоли разверните узел **Служебные программы\Общие папки** и выберите в нем папку **Общие ресурсы**.
3. Дважды щелкните на общей папке, которую требуется настроить для использования в автономном режиме. На вкладке **Общие** открывшегося окна свойств папки нажмите кнопку **Настройка**.
4. В открывшемся диалоговом окне **Настройка автономного режима** установите переключатель **Файлы и программы в этой общей папке недоступны вне сети** (No files of programs from the shared folder are available offline).
5. Нажмите кнопку **OK**.

Полностью запретить использование автономных папок на клиентском компьютере можно следующим образом:

1. В левой панели Центра синхронизации щелкните по ссылке **Управление автономными файлами**. Откроется диалоговое окно **Автономные файлы**.
2. На вкладке **Общие** этого окна нажмите кнопку **Отключить автономные файлы** (Disable offline files), а затем кнопку **OK**.

Чтобы разрешить использование автономных файлов, повторите эту процедуру, но нажать нужно будет кнопку **Включить автономные файлы** (Enable offline files).

Настройка дисковых квот

В следующих разделах рассматривается использование и управление дисковыми квотами. Дисковые квоты позволяют управлять использованием дискового пространства и настраиваются отдельно для каждого тома. Дисковые квоты можно задавать только для томов

с файловой системой NTFS. Первым шагом в настройке дисковых квот будет включение параметров политик дисковых квот *(см. разд. "Настройка политик дисковых квот" главы 5)*. После настройки необходимых политик можно задавать квоты для конкретных дисков системы.

Использование дисковых квот

Администраторы используют дисковые квоты для управления использованием дискового пространства на важных дисках, например, дисках, которые содержат общие папки корпоративных или пользовательских данных. При включении дисковых квот задаются предел и уровень предупреждения дисковых квот. Предел дисковых квот задает максимальный объем дискового пространства, который может быть занят пользователями (что предотвращает запись пользователями на диск новой информации), записывает в журнал события, когда пользователь превышает свой предел, или и то и другое. Дисковые квоты служат для предупреждения пользователей и записи в журнал событий-предупреждений, когда дисковая квота почти израсходована.

Практический совет

Хотя многие администраторы настраивают дисковые квоты, для которых принудительно соблюдаются пределы, такой подход не является обязательным. В частности, иногда может просто требоваться отслеживать использования дискового пространства отдельными пользователями и знать, когда они превышают некий определенный предел. В таких случаях вместо отказа в дополнительном дисковом пространстве при превышении предела просто выполняется запись в журнал о факте такого превышения.

Пределы дисковых квот применяются только к обычным пользователям, но не к администраторам, даже если они превысят установленный предел. Дисковые квоты и предупреждения можно задавать в килобайтах (КБ), мегабайтах (МБ), гигабайтах (ГБ), петабайтах (ПТ) и экзабайтах (ЭБ). В типичных условиях дисковые квоты обычно задаются в мегабайтах или гигабайтах. Например, для общей сетевой папки с данными организации, которая используется работниками отдела, можно установить дисковую квоту с пределом в 20—100 Гбайт. А для общей сетевой папки с данными пользователей можно установить дисковую квоту со значительно более низким пределом, например в 5—20 Гбайт, не позволяя им, таким образом, генерировать большие объемы данных. Часто для дисковых квот устанавливаются предупреждения при использовании определенного процента квоты. Например, можно установить предупреждение, когда использовано 90—95% дисковой квоты.

Так как использование дисковых квот отслеживается для отдельных дисков и отдельных пользователей, процент использования дисковой квоты одним из пользователей не влияет на дисковые квоты других. Если пользователь исчерпает свою дисковую квоту в 5 Гбайт для данного диска, он больше не сможет записывать данные на этот диск. Но он может освободить место, удалив ненужные более файлы и папки, переместив данные в сжатую область диска или сжав их. Перемещение файлов в другое место диска не влияет на ограничение дисковой квоты. В новом месте данные занимают такой же объем, если только пользователь не переместил их в сжатую папку. В любом случае, исчерпание дисковой квоты любым отдельным пользователем не затрагивает возможности всех других пользователей записывать свои данные на диск (при условии, что на диске имеется достаточное свободное пространство).

Дисковые квоты можно задавать как для локальных дисков, так и для дисков удаленных компьютеров. Управление квотами для локальных дисков выполняется на самих локальных дисках. Для управления квотами на удаленных дисках нужно предоставить общий доступ к корневому каталогу диска, а затем задать для него дисковые квоты. Следует иметь в виду,

что при включении дисковых квот для локального диска файлы операционной системы и прикладных программ не засчитываются в дисковую квоту установившего их пользователя. Обычно владельцем системных файлов является учетная запись **Доверенный установщик** (TrustedInstaller), а файлов программ — учетная запись **Система**.

Только члены группы **Администраторы домена** или группы **Администраторы** локальной системы могут настраивать дисковые квоты. Дисковые квоты для отдельных компьютеров можно задавать посредством групповой политики, а для групп пользователей или компьютеров — посредством политик сайтов, доменов или организационных единиц. Отслеживание дисковых квот может вызвать определенные накладные расходы на компьютерах. Объем этих накладных расходов зависит от количества отслеживаемых дисковых квот, общего размера дисков и хранящихся на них данных и количества пользователей, к которым применяются дисковые квоты.

Хотя кажется, что дисковые квоты отслеживаются по пользователям, незримо Windows 8 управляет квотами, используя идентификаторы безопасности SID[1]. Так как дисковые квоты отслеживаются по идентификаторам SID, имена пользователей можно изменять, не беспокоясь, что это затронет настройки дисковых квот. Отслеживание дисковых квот по идентификаторам SID вызывает определенные дополнительные накладные расходы при просмотре статистики дисковых квот для пользователей. Причиной этому является то обстоятельство, что Windows 8 требуется сопоставить идентификаторы SID с именами учетных записей пользователей, чтобы в диалоговых окнах можно было отображать имена учетных записей. Для этого необходимо связаться с локальной службой диспетчера пользователей или контроллером домена, в зависимости от конкретного случая. После первоначального поиска имен они кэшируются в локальном файле и в следующий раз доступны сразу же. Обновление этого кэша имен выполняется довольно нечасто, поэтому, в случае расхождения между отображаемыми и настроенными данными, эту информацию следует обновить. Обычно это можно сделать, нажав кнопку **Обновить** (Refresh) в текущем окне или же клавишу <F5>.

Включение дисковых квот

Дисковые квоты задаются для отдельных дисков, и только для дисков формата NTFS. Лучше всего настраивать дисковые квоты посредством групповой политики *(см. главу 5)*. Настроив соответствующие дисковые политики, можно создавать отдельные записи квот для управления пользовательскими и групповыми квотами.

Если требуется настроить квоты на каждом отдельном компьютере, это можно сделать следующим способом:

1. Откройте консоль **Управление компьютером**. По умолчанию консоль подключена к локальному компьютеру. Для настройки дисковых квот на удаленных компьютерах щелкните правой кнопкой мыши по корневому узлу **Управление компьютером** в дереве консоли (левая панель) и в контекстном меню выберите команду **Подключиться к другому компьютеру**. С помощью открывшегося диалогового окна **Выбор компьютера** выберите требуемый компьютер.
2. В дереве консоли разверните узел **Запоминающие устройства** и выберите в нем подузел **Управление дисками**. В панели сведений будут отображены тома выбранного компьютера.
3. В виде **Список томов** или **Графическое представление** щелкните правой кнопкой мыши по значку диска и в контекстном меню выберите команду **Свойства**.

[1] Security identifier.

4. В открывшемся окне свойств диска перейдите на вкладку **Квота** (рис. 14.8) и установите на ней флажок **Включить управление квотами** (Enable quota management).
5. Чтобы задать дисковую квоту для каждого пользователя данного компьютера, установите переключатель **Выделять на диске не более** (Limit disk space to), а затем введите максимальный объем дискового пространства, которым может располагать каждый пользователь. Далее настройте порог выдачи предупреждений, установив требуемое значение в соответствующем поле. Порог выдачи предупреждений обычно должен составлять 90—95% от дисковой квоты.

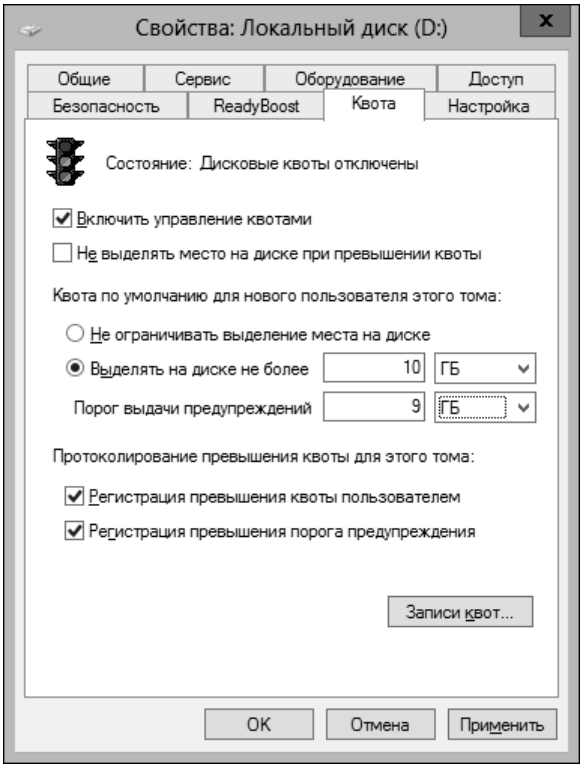


Рис. 14.8. Вкладка **Квота** окна свойств диска для включения и настройки дисковых квот

Совет

Хотя дисковая квота и порог предупреждений применяются для всех пользователей, эти значения можно настроить для каждого отдельного пользователя в диалоговом окне **Записи квот для** (Quota Entries), которое открывается нажатием кнопки **Записи квот**. Записи квот можно экспортировать с одного диска и импортировать на другой.

6. Для принудительного применения квот (т. е. запретить использовать больше, чем выделенное пользователю дисковое пространство) установите флажок **Не выделять место на диске при превышении квоты** (Deny disk space to users exceeding quota limit). При этом имейте в виду, что это ограничение применимо только к обычным пользователям, но не к администраторам.
7. Чтобы настроить запись в журнал превышения пользователями порога предупреждений и/или самой квоты, используйте флажки раздела **Протоколирование превышения квоты для этого тома** (Select the quota logging options for this volume).

8. Завершив настройку квот, нажмите кнопку **Применить**. Если система дисковых квот еще не включена, появится диалоговое окно с запросом включить систему квот. Нажмите кнопку **OK**, чтобы Windows 8 повторно отсканировала том и обновила статистику использования диска. К пользователям, превысившим квоту или порог предупреждения, можно применять различные меры. Например, запрещать дальнейшую запись на диск, предупреждать при следующем обращении пользователя к диску и/или записывать соответствующие события в журнал приложений.

Просмотр записей дисковых квот

Использование дискового пространства отслеживается для каждого отдельного пользователя. Когда система дисковых квот включена, в файле квот диска создается запись для каждого пользователя, который сохраняет данные на этот диск. Эта запись периодически обновляется, чтобы отражать текущее использованное дисковое пространство, применяемую дисковую квоту, порог предупреждений и процент использования выделенного пространства. Администратор может изменять записи дисковых квот и задавать разные квоты и пороги предупреждений для различных пользователей. Дисковые квоты также можно создавать для пользователей, которые еще не сохраняли данные на диске. Таким образом обеспечивается наличие квоты и порога предупреждений для пользователя на тот случай, когда он работает с диском.

Просмотреть текущие записи квот для диска можно следующим образом:

1. Откройте консоль **Управление компьютером**. По умолчанию консоль подключена к локальному компьютеру. Для просмотра дисковых квот на удаленных компьютерах щелкните правой кнопкой мыши по корневому узлу **Управление компьютером** в дереве консоли (левая панель) и в контекстном меню выберите команду **Подключиться к другому компьютеру**. С помощью открывшегося диалогового окна **Выбор компьютера** выберите требуемый компьютер.
2. В дереве консоли разверните узел **Запоминающие устройства** и выберите в нем подузел **Управление дисками**. В панели сведений будут отображены тома выбранного компьютера.
3. В виде **Список томов** или **Графическое представление** щелкните правой кнопкой мыши по значку диска и в контекстном меню выберите команду **Свойства**.
4. На вкладке **Квота** этого окна нажмите кнопку **Записи квот** (Quota Entries). Откроется диалоговое окно **Записи квот для** (Quota entries for).
5. Записи дисковых квот показывают текущее использование дискового пространства на определенном диске, а также соответствующие квоты и пороги предупреждений. Столбец **Состояние** окна позволяет быстро определить, не превысил ли пользователь свой предел. Значение **OK** в этом столбце означает, что данный пользователь работает в пределах своей дисковой квоты. Любое другое состояние обычно означает, что пользователь превысил уровень предупреждения или предел квоты.

Создание записей дисковых квот

Дисковые квоты можно создавать как для тех пользователей, которые еще не сохраняли данные на диске, так и для тех, которые уже сохранили. Это позволяет устанавливать дисковые квоты и пороги предупреждений, настроенные под требования любого отдельного пользователя. Обычно эта возможность применяется в тех случаях, когда один пользователь регулярно сохраняет больший объем информации, чем другие. Например, дизайнеру-гра-

фику может требоваться больше дискового пространства, чем работнику отдела обслуживания клиентов. Другим достоинством настраиваемых записей квот является то, что их можно экспортировать на другие диски, и это позволяет быстро применять один набор правил к нескольким дискам.

Создать запись квоты для диска можно следующим образом:

1. В консоли **Управление компьютером** разверните узел **Запоминающие устройства** и выберите в нем узел **Управление дисками**. В виде **Список томов** или **Графическое представление** щелкните правой кнопкой мыши по значку диска и в контекстном меню выберите команду **Свойства**.
2. На вкладке **Квота** этого окна нажмите кнопку **Записи квот**. Откроется диалоговое окно **Записи квот для**, содержащее список квот для всех пользователей. Обновите список, выполнив последовательность команд меню **Вид | Обновить**.
3. Если у пользователя нет записи квоты для данного диска, создайте ее, выполнив последовательность команд меню **Квота | Создать запись квоты** (Quota | New quota entry). Откроется диалоговое окно **Выбор: "Пользователи"** (Select User).
4. Введите имя пользователя, для которого нужно создать запись квоты, в текстовое поле **Введите имена выбираемых объектов**, а затем нажмите кнопку **Проверить имена**. Если для указанного имени найдутся совпадения, выберите из них требуемую учетную запись и нажмите кнопку **OK**.
5. При отсутствии совпадений исправьте введенное имя и повторите попытку. Повторите процесс поиска, пока не будет найден требуемый пользователь, после чего нажмите кнопку **OK**.
6. Откроется диалоговое окно **Добавление новой квоты** (Add new quota entry) (рис. 14.9). В этом окне можно выбрать один из следующих двух вариантов. Можно удалить все ограничения дисковых квот, установив переключатель **Не ограничивать выделение места на диске** (Do not limit disk usage). Или же можно задать дисковую квоту и порог предупреждений, установив переключатель **Выделять на диске не более** (Limit disk space to) и задав требуемые соответствующие значения.

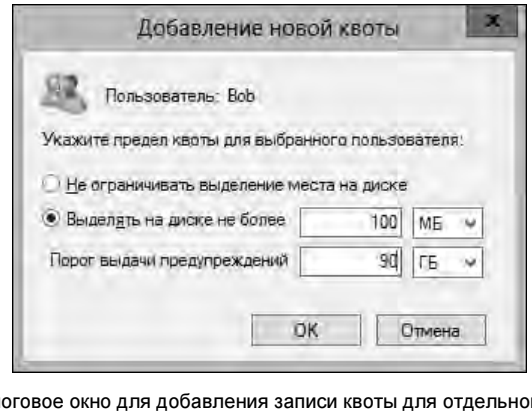


Рис. 14.9. Диалоговое окно для добавления записи квоты для отдельного пользователя

7. Выполнив необходимые настройки, нажмите кнопку **OK**, чтобы закрыть окно. Далее закройте окно **Записи квот для**, а затем диалоговое окно свойств диска, нажав кнопку **OK**.

Обновление и настройка записей дисковых квот

Записи дисковых квот для отдельных пользователей можно обновить и настроить в любое время. Процедура для этого следующая:

1. В консоли **Управление компьютером** разверните узел **Запоминающие устройства** и выберите в нем узел **Управление дисками**. В виде **Список томов** или **Графическое представление** щелкните правой кнопкой мыши по значку требуемого диска и в контекстном меню выберите команду **Свойства**.
2. На вкладке **Квота** этого окна нажмите кнопку **Записи квот**. Откроется диалоговое окно **Записи квот для**, содержащее список квот для всех пользователей. Обновите список, выполнив последовательность команд меню **Вид | Обновить**.
3. Дважды щелкните на записи квоты требуемого пользователя. Откроется диалоговое окно **Параметры квоты для**, практически такое же, как и диалоговое окно на рис. 14.9.
4. Чтобы снять все ограничения дисковой квоты для данного пользователя, установите переключатель **Не ограничивать выделение места на диске**.
5. А чтобы изменить текущий предел дисковой квоты и порог предупреждений, установите переключатель **Выделять на диске не более** и задайте требуемые соответствующие значения.
6. Выполнив требуемые настройки, нажмите кнопку **OK**, чтобы закрыть окно.

Удаление записей дисковых квот

Когда пользователь, который имеет квоту на диске, больше не использует данный диск, его запись квоты для данного диска можно удалить. При удалении записи дисковой квоты все файлы на диске, принадлежащие данному пользователю, отображаются в диалоговом окне. Эти файлы можно безвозвратно удалить, стать их владельцем или переместить в папку на другом диске.

Удалить запись дисковой квоты для пользователя и распорядиться его файлами на диске можно следующим образом:

1. В консоли **Управление компьютером** разверните узел **Запоминающие устройства** и выберите в нем узел **Управление дисками**. В виде **Список томов** или **Графическое представление** щелкните правой кнопкой мыши по значку тома и в контекстном меню выберите команду **Свойства**.
2. На вкладке **Квота** этого окна нажмите кнопку **Записи квот**. Откроется диалоговое окно **Записи квот для**, содержащее список квот для всех пользователей. Обновите список, выполнив последовательность команд меню **Вид | Обновить** или нажав клавишу <F5>.
3. Щелкните правой кнопкой мыши по записи дисковой квоты, которую требуется удалить, и в контекстном меню выберите команду **Удалить**. Или же выберите требуемую запись и выполните последовательность команд меню **Квота | Удалить запись квоты**. Можно выбрать несколько записей, используя при выборе клавишу <Shift> или <Ctrl>.
4. При выводе запроса подтвердить удаление выбранных записей нажмите кнопку **Да**. В результате откроется диалоговое окно **Дисковая квота**, содержащие список файлов, владельцем которых является данный пользователь или пользователи.
5. Чтобы отобразить файлы отдельного пользователя, выберите его имя в раскрывающемся списке **Файлы, которыми владеет** (List files owned by). Затем нужно указать, что делать с файлами пользователя. Файлы можно обрабатывать индивидуально, выбрав необ-

ходимый файл и указав для него требуемое действие. Можно выбрать несколько файлов, используя клавишу <Shift> или <Ctrl>. Для обработки файлов доступны следующие опции.

- **Отображать только папки** (Show folders only). Установка этого флажка позволяет отобразить только папки, в которых пользователь имеет файлы. Таким образом можно удалить, переместить или стать владельцем всех файлов пользователя в определенной папке.
- **Отображать только файлы** (Show files only). Установка этого флажка позволяет отображать все файлы, которыми владеет пользователь, по папкам, в которых они созданы.
- **Безвозвратно удалить файлы** (Permanently delete files). Выберите файлы, которые требуется удалить, а затем нажмите кнопку **Удалить**. При выводе запроса подтвердить удаление выбранных файлов, нажмите кнопку **Да**.
- **Стать владельцем файлов** (Take ownership of files). Выберите файлы, владельцем которых нужно стать, и нажмите кнопку **Сменить владельца**.
- **Переместить в** (Move files to). Выберите файлы, которые требуется переместить, а затем введите в соответствующее поле путь к папке на другом диске. Если путь неизвестен, нажмите кнопку **Обзор** и с помощью окна **Обзор папок** (Browse for folder) найдите необходимую папку. Указав папку, нажмите кнопку **Переместить**.

6. Завершив обработку файлов удаляемой записи дисковой квоты, нажмите кнопку **Закрыть**. Если обработка файлов была выполнена правильно, запись дисковой квоты будет удалена.

Экспорт и импорт параметров дисковых квот

Вместо того чтобы создавать повторно записи дисковых квот для отдельных дисков, можно экспортировать их параметры с одного диска и импортировать на другие. Как исходный диск, так и диск назначения должны иметь файловую систему NTFS. Экспорт и последующий импорт записей дисковых квот выполняется так:

1. Откройте консоль **Управление компьютером**. По умолчанию консоль подключена к локальному компьютеру. Для работы с дисковыми квотами на удаленных компьютерах щелкните правой кнопкой мыши по корневому узлу **Управление компьютером** в дереве консоли (левая панель) и в контекстном меню выберите команду **Подключиться к другому компьютеру**. С помощью открывшегося диалогового окна **Выбор компьютера** выберите компьютер.
2. В дереве консоли разверните узел **Запоминающие устройства** и выберите в нем подузел **Управление дисками**. В панели сведений будут отображены тома выбранного компьютера.
3. В виде **Список томов** или **Графическое представление** щелкните правой кнопкой мыши по значку диска и в контекстном меню выберите команду **Свойства**.
4. На вкладке **Квота** этого окна нажмите кнопку **Записи квот**. Откроется диалоговое окно **Записи квот для**.
5. В меню **Квота** выберите команду **Экспорт**. Откроется диалоговое окно **Параметры экспорта квоты** (Export Quota Settings). Выберите с помощью этого окна папку для хранения файла с параметрами записи квоты. Введите имя файла в соответствующее текстовое поле и нажмите кнопку **Сохранить**.

Совет

Если файл параметров сохранить на подключенном сетевом диске целевого тома, то в дальнейшем будет легче импортировать эти параметры. Файлы параметров квот обычно имеют небольшой размер, поэтому не стоит беспокоиться об используемом дисковом пространстве.

6. В меню **Квота** выберите команду **Закрыть**, чтобы закрыть диалоговое окно **Записи квот**. Нажмите кнопку **OK**, чтобы закрыть окно свойств диска.
7. В дереве консоли щелкните правой кнопкой мыши по узлу **Управление компьютером**. В контекстном меню выберите команду **Подключиться к другому компьютеру**. С помощью открывшегося диалогового окна **Выбор компьютера** выберите компьютер, содержащий диск, на который требуется импортировать экспортированные параметры записи дисковой квоты.
8. Разверните узел **Запоминающие устройства** и выберите в нем узел **Управление дисками**. В виде **Список томов** или **Графическое представление** щелкните правой кнопкой мыши по значку тома и в контекстном меню выберите команду **Свойства**.
9. Выберите вкладку **Квота**, проверьте, что установлен флажок **Включить управление квотами**, а затем нажмите кнопку **Записи квот**. Откроется диалоговое окно **Записи квот для** для данного диска.
10. В меню **Квота** выберите команду **Импорт**. В открывшемся диалоговом окне **Параметры импорта квоты** (Import Quota Settings) выберите файл параметров экспортированной ранее записи квоты и нажмите кнопку **Открыть**.
11. Если для диска уже имеется запись дисковых квот, их можно сохранить или заменить. В окне предупреждения о конфликте нажмите кнопку **Да**, чтобы заменить существующую запись, или **Нет**, чтобы сохранить ее. Опцию сохранения или замены существующей записи можно применить ко всем записям диска, установив флажок **Применить ко всем записям квот** (Do this for all quota entries) перед тем, как нажать кнопку **Да** или **Нет**.

Отключение дисковых квот

Дисковые квоты можно отключить для отдельных или всех пользователей диска. Когда дисковые квоты отключены для отдельного пользователя, к нему больше не применяются ограничения квоты, но использование диска другими пользователями продолжает отслеживаться. Когда дисковые квоты отключены для всего тома, отслеживание и управление использованием диска для всех пользователей полностью снимается. Чтобы отключить дисковые квоты для определенного пользователя, следуйте инструкциям, изложенным в *разд. "Обновление и настройка записей дисковых квот" ранее в этой главе*. А отключить отслеживание и управление дисковыми квотами для всех пользователей диска можно следующим образом:

1. Откройте консоль **Управление компьютером**. По умолчанию консоль подключена к локальному компьютеру. Для отключения дисковых квот на удаленном компьютере щелкните правой кнопкой мыши по корневому узлу **Управление компьютером** в дереве консоли (левая панель) и в контекстном меню выберите команду **Подключиться к другому компьютеру**. С помощью открывшегося диалогового окна **Выбор компьютера** выберите компьютер.
2. В дереве консоли разверните узел **Запоминающие устройства** и выберите в нем подузел **Управление дисками**. В панели сведений будут отображены тома выбранного компьютера.

3. В виде **Список томов** или **Графическое представление** щелкните правой кнопкой мыши по значку тома и в контекстном меню выберите команду **Свойства**.
4. На вкладке **Квота** открывшегося окна свойств тома снимите флажок **Включить управление квотами**. Нажмите кнопку **OK**. При выводе запроса подтвердить отключение управления квотами нажмите кнопку **OK**.

Использование локального кэширования

Возможность локального кэширования файлов Windows BranchCache работает совместно со службой BITS. С помощью групповой политики администраторы могут включить локальное кэширование, чтобы позволить компьютерам филиала получать документы и другие типы файлов из локального кэша, а не по сети из центрального сервера.

Локальное кэширование работает с файлами, передаваемыми по протоколам HTTP и SMB. Это означает, что кэшируются файлы, передаваемые как с внутрисетевых веб-серверов, так и с внутренних файловых серверов. Такое кэширование может существенно сократить время отклика и время пересылки документов, веб-страниц и содержимого мультимедиа.

Функциональность BranchCache использует архитектуру "клиент-сервер" и тесно интегрирована с файловыми службами и службами хранилища Windows. Существуют две версии функциональности BranchCache:

- первая версия была выпущена с Windows 7 и Windows Server 2008 R2 (а также сделана доступной для Windows Vista с установленной службой BITS 4.0);
- вторая версия выпускается в Windows 8 и Windows Server 2012.

Эти версии работают по-разному и используют несовместимые способы кэширования. В первой версии применяется традиционный способ кэширования. А во второй версии BranchCache используются методы дедупликации данных для оптимизации передачи данных по глобальным сетям в филиалы. Вследствие этого BracnhCache v2 использует блоки переменного размера и сжатие для большей эффективности передачи файлов. Кэшированные файлы сохраняются не в виде потоков данных, а в виде заглушек, которые указывают на требуемые блоки данных в общем хранилище кэша. Разбиение файлов на блоки обеспечивает загрузку клиентскими компьютерами и сохранение функциональностью BranchCache только одного экземпляра дублированного содержимого. Это также позволяет передавать только измененную часть файла, а не весь файл. Также важно отметить, что если общая папка находится на диске, для которого уже была выполнена дедупликация, функциональность BranchCache может использовать уже разбитые на блоки файлы, и выполнять повторную обработку файлов для передачи не требуется.

В общем, особенности работы этой функциональности после ее реализации зависят от пределов локальной сети. Если локальная сеть подключена к центральному офису через сеть, для которой двусторонняя сетевая задержка превышает 80 мс, клиенты локальной сети будут использовать локальный кэш, когда таковой имеется. Обратите внимание, что несколько локальных сетей, объединенных высокоскоростной сетью, также могут использовать один локальный кэш.

Когда включено локальное кэширование, при первом обращении по сети к файлу из внутрисетевого веб-сайта или файлового сервера, Windows передает этот файл с исходного сервера и кэширует его в филиале. При следующем запросе этого файла любым пользователем в филиале Windows выполняет поиск этого файла в локальном кэше. Если файл существует в локальном кэше, Windows запрашивает у исходного сервера, не был ли файл изменен после помещения в кэш. Если файл не был изменен, Windows берет файл из локального кэша,

избегая передачи его с исходного сервера по глобальной сети. Если же файл был изменен, Windows получает его с исходного сервера и обновляет копию файла в локальном кэше.

Во второй версии BranchCache кэшированные данные по умолчанию зашифровываются для повышения уровня безопасности, а размещенный кэш на серверах Windows содержится с помощью технологии баз данных ESE[1]. Использование базы данных ESE позволяет серверу размещенного кэша хранить терабайты данных и эффективно обслуживать большое число клиентов. Кроме этого, администраторы могут предварительно загружать содержимое на серверы размещенного кэша до запроса этого содержимого. Предварительная загрузка содержимого в локальный кэш обеспечивает быстрый доступ к нему. Также предварительная загрузка содержимого с носителей, например с внешнего диска или DVD-диска, устраняет необходимость передачи содержимого по сети.

Локальное кэширование BranchCache можно настроить для работы в одном из следующих двух режимов.

- **Распределенное кэширование.** В этом режиме компьютер пользователя под управлением совместимой версии Windows содержит распределенный файловый кэш. Так как каждый локальный компьютер кэширует и отправляет файлы, содержать для этого специальный сервер в филиале не требуется.
- **Размещенный кэш.** В этом режиме локальный файловый кэш размещается на файловых серверах в филиале. Эти серверы кэшируют файлы и отправляют их клиентам филиала.

> ***Примечание***
>
> Хотя BranchCache v2 позволяет масштабировать кэширование на несколько серверов, BranchCache v1 позволяет иметь в филиале только один сервер размещенного кэша.

Очевидно, что каждый из этих методов имеет свои преимущества и недостатки. В случае распределенного режима кэширования для задействования локального кэширования не требуется устанавливать специальные серверы. Но тогда на пользовательские компьютеры ложится бремя содержать кэш и распределять файлы, что требует дополнительных вычислительных мощностей и может отрицательно сказаться на производительности. А в случае режима размещенного кэширования для задействования локального кэширования необходимо установить требуемые файловые серверы. Но после установки и запуска этих серверов вся работа и накладные расходы по содержанию кэша ложится на серверы, что является значительным преимуществом над режимом распределенного кэша.

При этом нужно иметь в виду следующее:

- функциональность локального кэширования не запрещает пользователям сохранять локальные копии файлов; она работает с запросами чтения, например, когда пользователь запрашивает файл с файлового сервера;
- функциональность локального кэширования работает бесшовно с технологиями шифрования и безопасной передачи данных, такими как подписывание и шифрование SMB-пакетов;
- по умолчанию сетевые файлы кэшируются в филиале только в том случае, когда двусторонняя сетевая задержка превышает 80 мс.

Установка и настройка функциональности BranchCache выполняется следующим образом:

1. Устанавливается файловый сервер с возможностью BranchCache, при этом файловому серверу добавляется роль службы BranchCache для сетевых файлов.

[1] Extensible Storage Engine — расширенный обработчик хранилищ.

2. Устанавливается сервер содержимого с возможностью BranchCache (например, веб-сервер или сервер приложений на основе службы BITS) с добавлением серверу компонента BranchCache.
3. Устанавливается сервер размещенного кэша с добавлением серверу в филиале возможности BranchCache.
4. Устанавливается клиент с возможностью BranchCache, на клиенте включаются функциональность и режим BranchCache.

Включить и настроить функциональность BranchCache можно следующим образом:

1. В редакторе управления групповыми политиками откройте для редактирования требуемый объект групповой политики. Разверните узел редактора групповой политики **Конфигурация компьютера\Административные шаблоны\Сеть\BranchCache**.
2. Дважды щелкните на параметре политики **Включить BranchCache** (Turn on BranchCache). В открывшемся окне свойств параметра установите переключатель **Включить**, а затем нажмите кнопку **OK**.
3. Далее, выполните одно из следующих действий.
   - Чтобы включить распределенное локальное кэширование, дважды щелкните на параметре **Включить режим распределенного кэша BranchCache** (Set BranchCache distributed cache mode). В открывшемся окне свойств параметра установите переключатель **Включить**, а затем нажмите кнопку **OK**.
   - Чтобы включить размещенный режим кэширования для поддержки клиентов BranchCache v1, дважды щелкните на параметре политики **Включить режим размещенного кэша BranchCache** (Set BranchCache hosted cache mode). В открывшемся окне свойств параметра установите переключатель **Включить**, введите в соответствующее поле имя сервера размещенного кэша и нажмите кнопку **OK**.
   - Чтобы включить размещенный режим кэширования для поддержки клиентов BranchCache v2, дважды щелкните на параметре политики **Настройка серверов размещенного кэша** (Configure hosted cache servers). В открывшемся окне свойств параметра установите переключатель **Включить**, а затем нажмите кнопку **Показать** (Show). В диалоговом окне **Вывод содержания** (Show contents) введите полное имя или IP-адрес каждого сервера кэша BranchCache v2 для филиала, к которому будет применен данный объект групповой политики. Последовательно нажмите кнопку **OK**, чтобы закрыть все окна.

   Примечание

   Если включить параметр политики **Настройка серверов размещенного кэша**, клиенты Windows 8 будут игнорировать параметр политики **Включить режим размещенного кэша BranchCache**.

   Практический совет

   Одновременное использование обеих версий BranchCache может вызвать неэффективное кэширование и проблемы совместимости. Если требуется, чтобы клиенты с Windows 8 использовали BranchCache v1 вместо BranchCache v2, включите параметр политики **Настройка поддержки версий BranchCache на клиентах** (Configure client BranchCache version support) и выберите связанную опцию **Windows Vista с установленной службой BITS 4.0, Windows 7 или Windows Server 2008 R2** (Windows Vista with BITS 4.0 installed, Windows 7 or Windows Server 2008 R2).

4. Чтобы изменить значение задержки для активирования локального кэширования, дважды щелкните на параметре политики **Настройка BranchCache для сетевых файлов** (Configure BranchCache for network files). В открывшемся окне свойств параметра уста-

новите переключатель **Включить**, а затем введите требуемую задержку сети для активирования кэширования сетевых файлов. Это значение указывается в миллисекундах. При значении 0 файлы всегда будут кэшироваться.

5. Если включен размещенный режим кэширования, дважды щелкните на параметре политики **Установить процент дискового пространства, используемого для кэша клиентского компьютера** (Set percentage of disk space usage for client computer cache). В открывшемся окне свойств параметра установите переключатель **Включить**, задайте процент дискового пространства, которое клиентские компьютеры должны зарезервировать для BranchCache, и нажмите кнопку **OK**. По умолчанию максимальный размер кэша установлен в 5% общего объема диска.

Для BranchCache v2 совместимые клиенты могут искать в службе каталогов Active Directory серверы размещенного кэша, связанные с их текущим сайтом Active Directory, и автоматически настраивать себя на работу в режиме размещенного кэша, если это возможно. Для этого необходимо включить и настроить параметр политики **Включить автоматическое обнаружение размещенного кэша по точке подключения службы** (Enable automatic hosted cache discovery by service connection point).

ГЛАВА 15

Настройка и диагностирование сетей TCP/IP

В этой главе рассматривается управление проводными и беспроводными сетевыми соединениями, которые используются для сетевого взаимодействия устройств. Для правильной работы сети необходимо установить сетевые компоненты и настроить сетевое взаимодействие, используя протокол DHCP[1], систему DNS[2] и службу WINS[3]. Протокол DHCP применяется для динамической настройки параметров сети и IP-адресов. Службы DNS и WINS предоставляют услуги разрешения имен. Основной из этих двух служб является служба DNS, а служба WINS содержится для обратной совместимости с более ранними версиями операционной системы Windows.

Обзор сетевых возможностей Windows 8

Операционная система Windows 8 включает следующие сетевые возможности.

- **Сетевой проводник** (Network Explorer). Центральная консоль для просмотра компьютеров и устройств в сети.
- **Центр управления сетями и общим доступом** (Network and Sharing Center). Центральная консоль для просмотра и управления параметрами сети и общего доступа компьютера.
- **Диагностика сети** (Network Diagnostics). Средство автоматической диагностики, предоставляющее помощь в решении проблем с работой сети.

Прежде чем изучать использование этих сетевых инструментов, мы рассмотрим функциональности Windows 8, на которые эти инструменты полагаются в своей работе. Первая функциональность — это сетевое обнаружение, которое управляет возможностью компьютера "видеть" в сети другие компьютеры и устройства, а вторая — служба сведений о состоянии сети, которая докладывает об изменениях в сетевой связности и конфигурации.

Принципы сетевого обнаружения и категории сетей

Параметры сетевого обнаружения компьютера определяют, какие компьютеры и устройства можно просматривать в сетевых инструментах Windows 8. Параметры сетевого обнаруже-

---

[1] Dynamic Host Configuration Protocol — протокол динамического конфигурирования хоста.

[2] Domain Name System — служба доменных имен.

[3] Windows Internet Naming Service — Windows-служба имен Интернета.

ния работают совместно с параметрами брандмауэра Windows, чтобы блокировать или разрешать:

- обнаружение компьютером других компьютеров и устройств в сети;
- обнаружение компьютера другими компьютерами и устройствами.

Параметры общего сетевого доступа служат для предоставления соответствующего уровня безопасности для каждой категории сети, к которой может подключаться компьютер. Определены три категории сетей:

- *доменные сети* — сети с компьютерами, подключенными к домену организации, к которой они принадлежат;
- *частные сети* — сети, в которых компьютеры используются в рабочих или домашних группах и не подключены напрямую к Интернету;
- *общедоступные сети* — сети в общественных местах, например кафе или гостиницах, в противоположность внутренним сетям.

> ***Примечание***
>
> По умолчанию сетевое обнаружение и общий доступ к файлам отключены, но эти возможности можно включить для доменных, рабочих и домашних сетей в консоли **Изменение параметров сетевого доступа для различных сетевых профилей** (Change sharing options for different network profiles). Открыть эту консоль можно, щелкнув по ссылке **Изменить дополнительные параметры общего доступа** (Change advanced sharing settings) в левой панели Центра управления сетями и общим доступом. Включение этих возможностей сокращает количество ограничений, разрешает компьютерам в сети обнаруживать другие компьютеры и устройства этой сети и предоставлять общий доступ к файлам. Но для общедоступных сетей сетевое обнаружение и общий доступ к файлам по умолчанию заблокированы. Это повышает уровень безопасности, не позволяя компьютерам в общедоступной сети обнаруживать другие компьютеры и устройства в этой сети и быть обнаруженными самим. При отключенном сетевом обнаружении и общем сетевом доступе файлы и принтеры компьютера, к которым был предоставлен общий доступ, недоступны из сети. Кроме этого, возможно, что некоторые программы не смогут получить доступ к сети.

Так как параметры для каждой категории сети сохраняются на компьютере отдельно, для каждой категории сети можно задать разные параметры для блокирования и разрешения сетевого трафика. При первом подключении компьютера к сети Windows 8 пытается определить местонахождение компьютера — дома, на работе или в общественном месте, чтобы установить категорию сети. При изменении сетевого соединения или при подключении к новой сети Windows 8 попытается определить категорию этой сети. Если Windows 8 не в состоянии определить категорию сети, сеть считается общедоступной. Если компьютер подключается к домену, сеть, к которой подключен компьютер, становится доменной сетью.

В зависимости от категории сети Windows 8 устанавливает параметры, которые включают или отключают сетевое обнаружение. Состояние **Включено** означает, что данный компьютер может обнаруживать другие компьютеры и устройства в сети и другие компьютеры в сети могут обнаруживать данный компьютер. Состояние **Выключено** означает, что данный компьютер не может обнаруживать другие компьютеры и устройства в сети и другие компьютеры в сети не могут обнаруживать данный компьютер.

Иногда Windows 8 ошибочно классифицирует сеть, как общедоступную, когда в действительности компьютер подключен к частной сети и является членом рабочей группы (или еще не присоединен к домашней группе). Обычно эта проблема возникает вследствие неправильной настройки параметров TCP/IP, но может также возникать даже и при правильной настройке этих параметров и компьютера.

Для правильной работы сети необходимо изменить ее категорию. В противном случае компьютер может не подключиться к сети и не сможет работать с другими ее ресурсами. При-

чиной этому будет то обстоятельство, что как брандмауэр Windows, так и брандмауэр Windows в режиме повышенной безопасности руководствуются категорией сети, чтобы определить, как обезопасить компьютер. Для каждой категории сети компьютеры имеют отдельный профиль брандмауэра Windows, самым строгим из которых является профиль для общедоступных сетей.

Одним из способов решения этой проблемы будет изменение профиля сети с общедоступной на частную с помощью средства устранения неполадок домашней группы. Процедура для этого следующая:

1. В разделе **Сеть и Интернет** Панели управления щелкните по ссылке **Выбор параметров домашней группы и общего доступа к данным**, а в следующем окне щелкните по ссылке **Запустить средство устранения неполадок домашней группы** (Start the HomeGroup troubleshooter).
2. В открывшемся окне средства нажмите кнопку **Далее**.
3. Следующая страница средства содержит сообщение о том, что некоторые проблемы домашних групп связаны с сетевыми проблемами, и предлагается устранить возможные неполадки или пропустить этот шаг. Пропустите этот шаг, щелкнув по соответствующей ссылке.
4. Средство устранения неполадок должно обнаружить, что задана неправильная категория сети, и предложить сменить категорию сети на частную. Согласитесь с этим предложением, щелкнув по ссылке **Применить это исправление** (Apply this fix).
5. Если вы пытаетесь создать домашнюю группу или присоединиться к уже существующей домашней группе, следуйте выводимым инструкциям. В противном случае нажмите кнопку **Отменить**, чтобы завершить работу средства устранения неполадок.

Практический совет

Иногда компьютер, сетевому соединению которого присвоена категория общедоступной сети, будет испытывать проблемы с присоединением к домену. Хотя в данном случае причиной проблемы могут быть неправильные настройки параметров TCP/IP компьютера, в равной степени виновником может быть и применяемый профиль брандмауэра. Так как профиль брандмауэра Windows для общедоступных сетей является по умолчанию самым ограничивающим, параметры этого профиля могут блокировать требуемые для присоединения к домену подключения. Эту проблему можно обойти, временно отключив брандмауэр Windows или выполнив только что описанную процедуру, чтобы изменить категорию сети с общедоступной на частную.

Использование сетевого проводника

Сетевой проводник отображает список обнаруженных компьютеров и устройств сети. Открыть сетевой проводник можно одним из следующих способов:

- запустите Проводник Windows и щелкните в левой панели на значке **Сеть**;
- в Панели управления щелкните по ссылке **Сеть и Интернет**. В разделе **Центр управления сетями и общим доступом** щелкните по ссылке **Просмотр сетевых устройств и компьютеров** (View network computers and devices).

Какие компьютеры и устройства отображаются в сетевом проводнике, определяется настройками сетевого обнаружения компьютера. Если сетевое обнаружение включено, в проводнике отображаются другие компьютеры сети (рис. 15.1).

Если сетевое обнаружение отключено, об этом выводится соответствующее сообщение в области уведомлений сетевого проводника. Щелчок по этому сообщению и выбор команды **Включить сетевое обнаружение и общий доступ к файлам** (Turn on network discovery and

file sharing) в контекстном меню включает сетевое обнаружение и открывает соответствующие порты в брандмауэре Windows, требуемые для работы этой функциональности. Если настройки сетевого обнаружения не были изменены никаким другим образом, компьютер перейдет в режим "только обнаружение". Общий доступ к файлам, принтерам и мультимедиа нужно будет настроить вручную *(см. главу 13)*.

Рис. 15.1. Окно сетевого проводника используется для сетевого обнаружения и просмотра ресурсов согласно текущей конфигурации

При условии наличия соответствующих разрешений в сетевом проводнике можно просматривать любой компьютер или устройство. Двойной щелчок по значку компьютера предоставляет доступ к его общим ресурсам, а двойной щелчок по значку устройства — доступ к его интерфейсу управления или ресурсам.

Лента сетевого проводника содержит несколько значков для сетевого управления.

- **Управление сетями и общим доступом.** (Network and Sharing Center). Предоставляет возможность просмотра состояния и управления параметрами сети. Дополнительную информацию *см. в следующем разделе "Использование Центра управления и сетями и общим доступом"*.
- **Добавление устройств и принтеров** (Add printers and devices). Запускает мастер **Добавление устройства** для добавления локального, сетевого, беспроводного или Bluetooth-принтера, а также других беспроводных устройств, которые были обнаружены, но не настроены.
- **Поиск в Active Directory** (Search Active Directory). Открывает диалоговое окно **Поиск** (Find), с помощью которого можно выполнить поиск пользователей, контактов, групп, компьютеров, общих папок и других ресурсов в Active Directory (доступно только для доменных сетей).

Использование Центра управления и сетями и общим доступом

Центр управления сетями и общим доступом (рис. 15.2) предоставляет возможность просмотра текущего состояния и конфигурации сетей. Центр управления сетями можно открыть из Панели управления, щелкнув в разделе **Сеть и Интернет** по ссылке **Просмотр состояния сети и задач** (View network status and tasks).

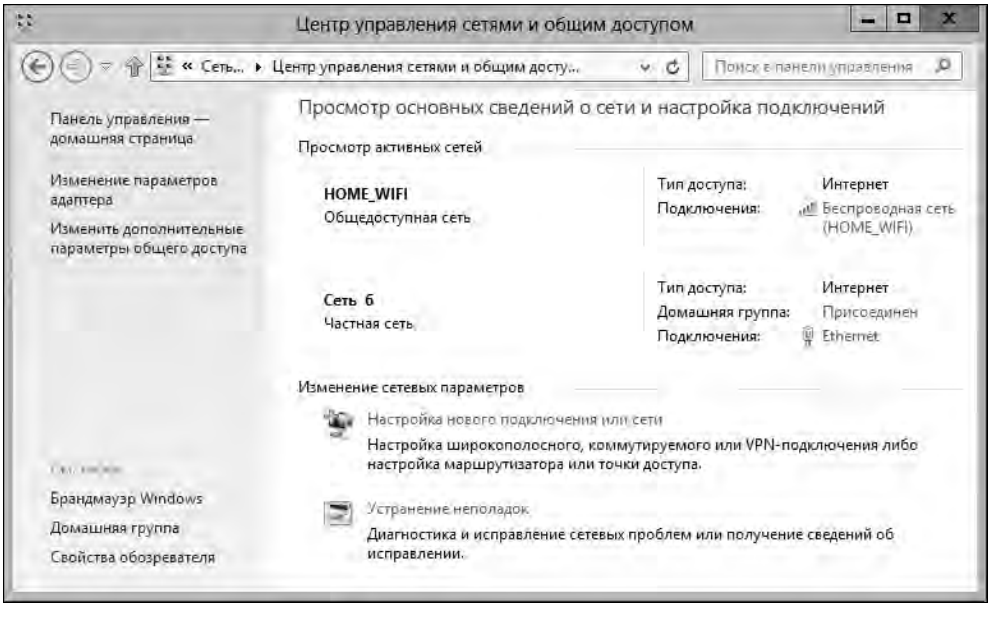


Рис. 15.2. Консоль Центра управления сетями и общим доступом

В панели сведений Центра управления сетями отображается список текущих активных сетей и краткие сведения о них. Имена сетей отображаются жирным шрифтом. Под именем сети указывается ее категория — **Общедоступная сеть** (Public Network), **Частная сеть** (Private Network) или **Доменная сеть** (Domain Network). В заголовке **Тип доступа** (Access Type) указывается состояние подключения к данной сети: **Без доступа к сети** (No network access), **Без доступа к Интернету** (No Internet access) или **Интернет** (Internet). Щелчок по имени сетевого подключения открывает соответствующее диалоговое окно состояния.

Щелкнув в левой панели по ссылке **Изменение параметров адаптера** (Change adapter settings), можно открыть страницу **Сетевые подключения** (Network Connections), с которой можно управлять сетевыми подключениями. Для настройки общего доступа щелкните в левой панели Центра по ссылке **Изменить дополнительные параметры общего доступа**. В открывшемся окне можно настроить параметры доступа к общим ресурсам и сетевого обнаружения для всех сетевых профилей. Для настройки параметров определенного сетевого профиля нужно развернуть его раздел, щелкнув по значку галочки в кружке справа от имени профиля, установить или снять требуемые переключатели и флажки, а затем нажать кнопку **Сохранить изменения**.

Из Центра управления сетями и общим доступом можно выполнять диагностирование сетевых проблем. Для этого нужно в панели сведений щелкнуть по ссылке **Устранение неполадок** (Troubleshoot problems), в следующем окне, **Сеть и Интернет**, щелкнуть по ссылке

требуемого средства устранения неполадок (например, **Входящие подключения** или **Сетевой адаптер**), а затем следовать выводимым инструкциям. Средство диагностики сетей Windows попытается определить проблему с сетью и предоставить возможное решение этой проблемы.

Установка сетевых компонентов

Чтобы оснастить компьютер сетевой функциональностью, на нем необходимо установить сетевое программное обеспечение TCP/IP и сетевой адаптер. Операционная система Windows 8 использует стек протоколов TCP/IP в качестве протокола по умолчанию для глобальных сетей (WAN). Сетевые компоненты обычно устанавливаются при установке Windows 8. Сетевое программное обеспечение TCP/IP можно также установить в диалоговом окне свойств сетевого подключения.

Использование стека протоколов TCP/IP и двойного IP-стека

Протоколы TCP и IP позволяют компьютерам взаимодействовать по разным сетям и через Интернет, используя сетевые адаптеры разных типов: на платах расширения, подключаемые через USB-порт, на платах PC Card или встроенные в системную плату. Операционная система Windows 8 использует архитектуру двойного уровня протокола IP, в которой реализуется как IP-протокол четвертой версии (IPv4), так и IP-протокол шестой версии (IPv6), оба использующие общие транспортный и сетевой уровни.

Протоколы IPv4 и IPv6 применяются разными способами. Протокол IPv4 использует 32-разрядную адресацию и является основной версией IP-протокола, используемой в большинстве сетей, включая Интернет. Протокол IPv6 использует 128-разрядную адресацию и является следующим поколением IP-протокола.

32-разрядные адреса протокола IPv4 обычно представляются в виде четырех групп цифр, каждая содержащая от 1 до 3 цифр, разделенных точками, например: 127.0.0.1 или 192.168.1.20. Каждое число называется *октетом*, т. к. представляет 8 битов 32-разрядного числа. Одна переменная часть стандартного индивидуального адреса IPv4 представляет идентификатор сети, а вторая — идентификатор хоста. Адрес IPv4 хоста и адрес MAC сетевого адаптера никаким образом не взаимосвязаны друг с другом.

Адреса протокола IPv6 представлены в виде восьми 16-разрядных блоков в шестнадцатеричном формате, разделенных двоеточиями. Первые 64 разряда стандартных индивидуальных (unicast) адресов протокола IPv6 представляют сетевой идентификатор, а последние 64 — адрес сетевого интерфейса. Ниже приводится пример адреса протокола IPv6:

```
FEC0:0:0:02BC:FF:BECB:FE4F:961D
```

Так как значение отдельных блоков адресов IPv6 может быть равно 0, непрерывная последовательность смежных блоков представляется в виде двойного двоеточия, т. е. как "::". Такое представление так и называется — *представлением двойного двоеточия* (double-colon notation). В этом представлении два нулевых блока в предшествующем примере сжимаются следующим образом:

```
FEC0::02BC:FF:BECB:FE4F:961D
```

Таким же образом сжимаются три и больше последовательных нулевых блоков. Например, `FFE8:0:0:0:0:0:0:1` становится `FFE8::1`.

Когда при установке операционной системы обнаруживается сетевое оборудование, по умолчанию включается как протокол IPv4, так и протокол IPv6. Таким образом, устанавливать отдельный сетевой компонент для поддержки протокола IPv6 не требуется. Такая IP-архитектура Windows 8 называется *двойным стеком TCP/IP*[1]. В табл. 15.1 приведен список и краткое описание возможностей, реализованных в двойном стеке TCP/IP, а в табл. 15.2 — список и описание возможностей двойного стека TCP/IP, специфичных для протокола IPv6.

Таблица 15.1. *Основные возможности двойного стека TCP/IP*

Поддерживаемая возможность	**Описание**
Автоматическое обнаружение маршрутизаторов типа "черная дыра"	Предотвращает завершение TCP-подключений вследствие выбрасывания промежуточными маршрутизаторами больших TCP-пакетов, повторных передач или сообщений об ошибках, не уведомляя об этом
Автоматическая проверка нерабочего шлюза	Обеспечивает периодическую проверку неоткликающегося шлюза, чтобы определить, не стал ли он доступен
Составной TCP	Оптимизирует передачи TCP для отправляющего хоста, увеличивая объем пересылаемых по подключению данных, одновременно обеспечивая ситуацию, когда другие TCP-подключения не затрагиваются
Расширенные SACK[2]	Расширяет методы использования SACK, позволяя принимающему узлу указывать до четырех непоследовательных блоков принятых данных и подтверждать дубликаты пакетов. Это помогает принимающему узлу определить, когда была выполнена ненужная ретрансляция сегмента, и откорректировать свое поведение, чтобы избежать этого в будущем
Модифицированный алгоритм быстрого восстановления	Обеспечивает повышенную пропускную способность, изменяя способ повышения скорости передачи данных передающим узлом, при потере в окне данных нескольких сегментов и при получении отправляющим узлом подтверждения об успешном получении только части данных
Определение отсутствия соседнего узла для IPv4	Определяет, когда соседние узлы и маршрутизаторы больше недосягаемые, и уведомляет об этом состоянии
Инфраструктура сетевой диагностики	Расширяемая инфраструктура, помогающая пользователям диагностировать и устранять проблемы сетевых подключений и восстанавливаться от их последствий
Автоматическая настройка окна получения	Оптимизирует TCP-обмен для получающего узла, автоматически управляя размером буфера (окна получения), используемого для хранения входящих данных, в зависимости от текущего состояния сети
Сегменты маршрутизации[3]	Предотвращает нежелательную переадресацию трафика между интерфейсами, ассоциируя интерфейс или набор интерфейсов с сеансом входа в систему, который имеет свой набор таблиц маршрутизации
Восстановление потерь на основе SACK	Позволяет использовать информацию SACK для восстановления потерь при получении дубликатов подтверждений и для более быстрого восстановления при отсутствии в узле назначения нескольких сегментов

[1] Dual TCP/IP stack.

[2] Selective Acknowledgment — избирательное подтверждение.

[3] Англ. *routing compartments*.

Таблица 15.1 *(окончание)*

Поддерживаемая возможность	**Описание**
Определения случайных превышений времени ожидания для повторной передачи	Обеспечивает исправление случайных временных тайм-аутов для повторной передачи и предотвращает ненужную повторную передачу сегментов
Расширенная TCP-статистика	Помогает определить причину узкого места подключения — передающее приложение, принимающее приложение или сеть
Платформа фильтрации Windows	Предоставляет интерфейс API для расширения архитектуры фильтрации TCP/IP с целью поддержки дополнительных возможностей

Таблица 15.2. *Основные возможности двойного стека TCP/IP для IPv6*

Поддерживаемая возможность	**Описание**
DHCP-клиент, поддерживающий DHCPv6	Расширяет возможности DHCP-клиента для поддержки протокола IPv6 и позволяет выполнять автоматическую конфигурацию адреса с учетом состояния соединения сервером DHCPv6
Безопасность протокола IP	Позволяет использовать протокол IKE[1] и шифрование данных для IPv6
Протокол IPv6 по протоколу PPP[2] (PPPv6)	Позволяет передавать исходный IPv6-трафик по подключениям протокола PPP, что, в свою очередь, позволяет клиентам удаленного доступа подключаться к поставщикам Интернета, использующим протокол IPv6, по коммутируемому подключению или по подключению PPPoE[3]
Протокол LLMNR[4]	Позволяет узлам IPv6, размещенным в одной подсети без сервера DNS, определять имена друг друга
Протокол MLDv2[5]	Предоставляет поддержку зависящего от отправителя многоадресного трафика и является эквивалентом протокола IGMPv3[6] для IPv3
Произвольные идентификаторы интерфейса	Предотвращает сканирование адресов IPv6 на основе известных идентификаторов производителей сетевых адаптеров. По умолчанию Windows 8 генерирует произвольные идентификаторы интерфейса для постоянных автоматически настраиваемых адресов IPv6, включая общественные адреса и адреса локального канала
Симметричное преобразование сетевых адресов	Сопоставляет внутренний (частный) адрес и номер порта разным внешним (общественным) адресам и портам, в зависимости от внешнего адреса назначения

[1] Internet Key Exchange — обмен ключами по Интернету.

[2] Point-to-Point Protocol — протокол соединения "точка-точка".

[3] PPP over Ethernet — PPP по Ethernet.

[4] Link-Local Multicast Name Resolution — разрешение широковещательных адресатов локальной сети.

[5] Multicast Listener Discovery — определение получателей широковещательных запросов.

[6] Internet Group Management Protocol — межсетевой протокол управления группами.

Установка сетевых адаптеров

Сетевые адаптеры представляют собой аппаратные устройства, которые используются для сетевого взаимодействия между узлами сети. Установка и настройка сетевых адаптеров выполняется следующим образом:

1. Следуйте инструкциям производителя сетевого адаптера. Например, может потребоваться использовать программное обеспечение, поставляемое совместно с адаптером, чтобы изменить настройки прерывания или порта адаптера.
2. При установке внутреннего сетевого адаптера выключите и полностью обесточьте компьютер, отсоединив шнур питания, а затем вставьте плату сетевого адаптера в соответствующий разъем в системной плате компьютера. Завершив физическую установку платы сетевого адаптера, подключите шнур питания и включите компьютер.
3. Операционная система Windows 8 должна определить новый адаптер в процессе загрузки. Если для адаптера имеется диск с драйверами, вставьте его в привод на данном этапе. В противном случае система может запросить вставить диск с драйверами.
4. Если Windows 8 не определит адаптер автоматически, следуйте инструкциям по установке устройств, изложенным в *разд. "Работа с драйверами устройств" главы 9*.
5. Если в системе не установлено сетевое программное обеспечение, установите его, как рассматривается в следующем разделе.

Установка сетевого программного обеспечения (TCP/IP)

Чтобы установить сетевое программное обеспечение TCP/IP после установки Windows 8, войдите в систему по учетной записи администратора, а затем выполните следующую процедуру:

1. В Панели управления щелкните по ссылке **Сеть и Интернет**, а в следующем окне — по ссылке **Центр управления сетями и общим доступом**.
2. Далее, в разделе **Просмотр активных сетей** (View your active networks) щелкните по ссылке требуемого сетевого подключения.

> ***Совет***
>
> Если требуемое сетевое подключение неактивно, в левой панели Центра управления щелкните по ссылке **Изменение параметров адаптера**, а в следующем окне, **Сетевые подключения**, щелкните правой кнопкой мыши по значку требуемого подключения и в контекстном меню выберите команду **Свойства**.

3. В диалоговом окне **Состояние** нажмите кнопку **Свойства**. В результате откроется диалоговое окно свойств данного сетевого подключения с выбранной вкладкой **Сеть** (рис. 15.3).
4. Если в списке установленных компонентов отсутствует протокол TCP/IPv4, протокол TCP/IPv6 или оба эти протокола, их нужно будет установить. Для этого нажмите кнопку **Установить**, в открывшемся окне **Выбор сетевых компонентов** (Select Network Feature Type) выберите **Протокол** и нажмите кнопку **Добавить**. В следующем диалоговом окне, **Выбор сетевого протокола** (Select Network Protocol), выберите требуемый протокол и нажмите кнопку **OK**. Чтобы установить другой протокол, повторите этот шаг.
5. В диалоговом окне свойств подключения проверьте, что установлены флажки **Протокол Интернета версии 6 (TCP/IPv6)** и **Протокол Интернета версии 4 (TCP/IPv4)** или, если требуется, оба. Нажмите кнопку **OK**, чтобы сохранить настройки и закрыть окно.

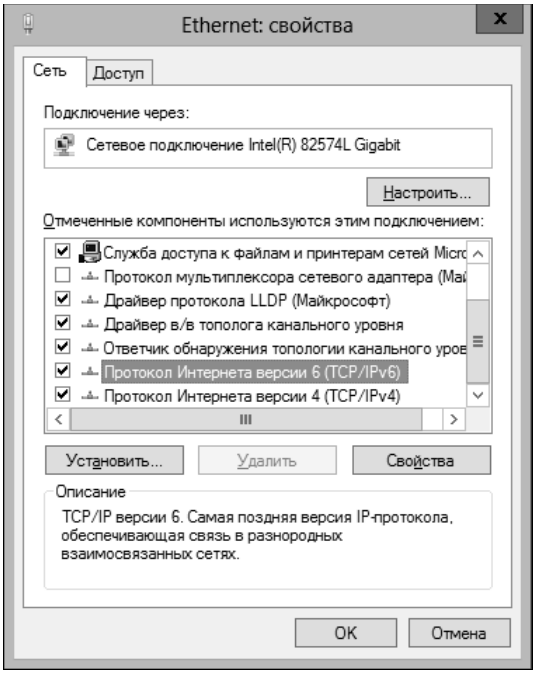


Рис. 15.3. Окно свойств сетевого подключения

6. Настройте сетевые подключения компьютера, как рассматривается в следующем разделе.

Настройка сетевых подключений

Сетевое подключение создается автоматически, если компьютер оснащен сетевым адаптером и подключен к сети. Если компьютер оснащен несколькими сетевыми адаптерами и подключен к сети, сетевое подключение создается для каждого адаптера. В случае отсутствия сетевых подключений компьютер следует подключить к сети или создать подключение другого типа, как рассматривается в *разд. "Управление сетевыми подключениями" далее в этой главе*.

Для взаимодействия по стеку протоколов TCP/IP компьютеры используют IP-адреса. Операционная система Windows 8 предоставляет следующие способы для настройки IP-адресов.

- **Вручную.** Заданные вручную IP-адреса называются *статическими*. Статические IP-адреса фиксированы и меняются только тогда, когда явно изменены пользователем. Статические IP-адреса обычно присваиваются серверам Windows. В таком случае также необходимо настроить дополнительные параметры, чтобы сервер мог должным образом определять все элементы сети и иметь доступ к ним.
- **Динамически.** Динамические IP-адреса назначаются при запуске сервером DHCP (если таковой установлен в сети). Эти адреса могут меняться со временем. Динамическое выделение IP-адресов применяется по умолчанию.
- **Альтернативно** (только для IPv4). Когда компьютер настроен для получения динамических адресов от сервера DHCPv4, но такой сервер отсутствует в сети, Windows 8 автоматически выделяет альтернативный частный IP-адрес. Альтернативные адреса выделяют-

ся в диапазоне от 169.254.0.1 до 169.254.255.254 и с маской подсети 255.255.0.0. Пользователь также может задать определенный альтернативный адрес IPv4, что особенно полезно для ноутбуков.

Настройка статических IP-адресов

При статической адресации компьютеру вручную присваивается требуемый IP-адрес, маска подсети для этого адреса и, если необходимо, шлюз по умолчанию для межсетевого обмена. IP-адрес является числовым идентификатором компьютера. Схемы назначения IP-адресов варьируются в зависимости от текущей настройки сети, но обычно они назначаются на основе определенного сегмента сети.

Как рассматривается в *разд. "Использование стека протоколов TCP/IP и двойного IP-стека" ранее в этой главе*, между адресами IPv4 и IPv6 существует очень большая разница. В адресах IPv6 первые 64 разряда представляют сетевой идентификатор, а последние 64 — адрес сетевого интерфейса. А в адресах IPv4 переменное число начальных разрядов представляет сетевой идентификатор, а остальные — идентификатор хоста. Например, в адресе 10.0.10.0 с маской подсети 255.255.255.0 первые три октета являются идентификатором сети. Иными словами, адрес 10.0.10.0 является однозначным сетевым идентификатором. А для компьютеров этой сети будут доступны адреса в диапазоне от 10.0.10.1 до 10.0.10.254. Адрес 10.0.10.255 зарезервирован для широковещательных передач.

В частных сетях, подключенных к Интернету не напрямую, следует использовать частные адреса IPv4. В табл. 15.3 приведены диапазоны частных адресов и соответствующие маски подсети.

Таблица 15.3. *Частные сетевые адреса IPv4*

Идентификатор сети	Маска подсети	Диапазон доступных адресов	Широковещательный адрес
10.0.0.0	255.0.0.0	10.0.0.0—10.255.255.254	10.255.255.255
172.16.0.0	255.240.0.0	172.16.0.0—172.31.255.254	172.31.255.255
192.168.0.0	255.255.0.0	192.168.0.0—192.168.255.254	192.168.255.255

Все другие сетевые адреса IPv4 являются общественными, и их требуется брать в аренду или покупать. Если сеть подключена к Интернету напрямую и поставщик Интернета предоставил вам диапазон адресов IPv4, можно использовать эти адреса для компьютеров сети.

Использование команды *ping*

Прежде чем назначить компьютеру или устройству статический IP-адрес, следует проверить, что этот адрес уже не используется или не был зарезервирован для использования с системой DHCP. Проверить, используется ли адрес, можно с помощью команды `ping`. Для этого выполните данную команду в консоли командной строки с адресом, который требуется проверить.

Например, проверка адреса IPv4 10.0.10.12 выполняется следующим образом:

```
ping 10.0.10.12
```

А проверка адреса IPv6 FECO::02BC:FF:BECB:FE4F:961D выполняется так:

```
ping FECO::02BC:FF:BECB:FE4F:961D
```

Получение ответа означает, что данный IP-адрес используется. Если же все четыре попытки не дают ответа, значит, в данный момент этот IP-адрес в сети не активен и, скорее всего, не используется. Но запрос `ping` может блокироваться брандмауэром, поэтому следует также подтвердить доступность данного IP-адреса у администратора сети.

Настройка статических адресов IPv4 и IPv6

Каждый установленный сетевой адаптер предоставляет одно подключение к локальной сети. Эти подключения создаются автоматически. Настройка IP-адреса для сетевого подключения выполняется следующим образом:

1. В Панели управления щелкните по ссылке **Сеть и Интернет**, а в следующем окне — по ссылке **Центр управления сетями и общим доступом**.
2. Далее, в разделе **Просмотр активных сетей** щелкните по ссылке требуемого сетевого подключения.
3. В открывшемся диалоговом окне **Состояние** нажмите кнопку **Свойства**. В результате откроется диалоговое окно свойств для данного сетевого подключения.
4. Дважды щелкните на необходимом протоколе: **Протокол Интернета версии 4 (TCP/IPv4)** или **Протокол Интернета версии 6 (TCP/IPv6)**.
5. Для настройки адреса IPv6 выполните следующие действия.
   - Установите переключатель **Использовать следующий IPv6-адрес** (Use the following IPv6 address), а затем введите требуемый адрес в соответствующее текстовое поле. Назначаемый сетевому подключению IPv6-адрес не должен использоваться ни для какого другого устройства сети.
   - Значение поля **Длина префикса подсети** (Subnet prefix length) обеспечивает правильную работу компьютера в сети. В это поле Windows 8 должна автоматически вставить значение по умолчанию. Если в сети не используются подсети с идентификатором переменной длины, это значение по умолчанию должно быть приемлемым. Если же в сети используются подсети с идентификатором переменной длины, это значение следует заменить значением, требуемым для данной сети.
6. Для настройки адреса IPv4 выполните следующие действия.
   - Установите переключатель **Использовать следующий IPv4-адрес** (Use the following IPv4 address), а затем введите требуемый адрес в соответствующее текстовое поле. Назначаемый сетевому подключению IPv4-адрес не должен использоваться ни для какого другого устройства сети при использовании данного сетевого соединения.
   - Значение поля **Маска подсети** (Subnet mask) обеспечивает правильную работу компьютера в сети. В это поле Windows 8 должна автоматически вставить значение по умолчанию. Если в сети не используются подсети с идентификатором переменной длины, это значение по умолчанию должно быть приемлемым. Если же в сети используются подсети с идентификатором переменной длины, это значение следует заменить значением, требуемым для данной сети.
7. Если компьютеру нужен доступ к другим сетям TCP/IP, Интернету или другим подсетям, необходимо указать основной шлюз. Для этого в текстовое поле **Основной шлюз** (Default Gateway) введите IP-адрес основного маршрутизатора сети.
8. Служба DNS требуется для разрешения доменных имен. Введите адреса предпочитаемого и альтернативного серверов DNS в соответствующие поля.
9. Завершив настройку статического IP-адреса сетевого подключения, нажмите дважды кнопку **OK**, а затем **Закрыть**, чтобы сохранить настройки и закрыть все окна. Повто-

рите этот процесс для других IP-протоколов и сетевых адаптеров, которые нужно настроить.

10. При настройке адресов IPv4 также настройте должным образом службу WINS, следуя инструкциям, изложенным в *разд. "Настройка службы WINS" далее в этой главе.*

Настройка динамических и альтернативных IP-адресов

Хотя статические IP-адреса можно также использовать и для рабочих станций, в большинстве случаев для рабочих станций используются динамические или альтернативные IP-адреса либо оба типа. Настройка динамического или альтернативного адреса выполняется следующим образом:

1. В Панели управления щелкните по ссылке **Сеть и Интернет**, а в следующем окне — по ссылке **Центр управления сетями и общим доступом**.
2. Далее, в разделе **Просмотр активных сетей** щелкните по ссылке требуемого сетевого подключения.
3. В открывшемся диалоговом окне **Состояние** нажмите кнопку **Свойства**. В результате откроется диалоговое окно свойств для данного сетевого подключения.

> ***Примечание***
>
> В диалоговом окне **Просмотр активных сетей** отображается одно сетевое подключение для каждого установленного сетевого адаптера. Эти подключения создаются автоматически. Если для установленного адаптера не отображается соответствующее сетевое подключение, проверьте правильность установки драйвера данного адаптера.

4. Дважды щелкните на нужном протоколе: **Протокол Интернета версии 4 (TCP/IPv4)** или **Протокол Интернета версии 6 (TCP/IPv6)**.
5. В зависимости он настраиваемого протокола установите переключатель **Получить IPv6-адрес автоматически** (Obtain an IPv6 address automatically) или **Получить IP-адрес автоматически** (Obtain an IP address automatically). Для DNS-сервера можно задать автоматическое получение адреса или его ручную настройку, установив флажок **Получить адрес DNS-сервера автоматически** (Obtain DNS server address automatically) или **Использовать следующие адреса DNS-серверов** (Use the following DNS server address) соответственно. При ручной настройке адреса DNS-сервера введите требуемые адреса для предпочитаемого и альтернативного DNS-серверов в соответствующие поля.
6. При использовании динамических IPv4-адресов с настольными компьютерами следует настроить автоматический альтернативный адрес. Для этого выберите вкладку **Альтернативная конфигурация** (Alternate configuration) и установите переключатель **Автоматический частный IP-адрес** (Automatic private IP address). Нажмите дважды кнопку **OK**, а затем кнопку **Закрыть** и пропустите остальные шаги.
7. При настройке динамических IPv4-адресов для мобильных компьютеров обычно желательно настроить альтернативный адрес вручную. Для этого выберите вкладку **Альтернативная конфигурация** и установите на ней переключатель **Настраиваемый пользователем** (User configured). Далее, введите в текстовое поле **IP-адрес** требуемый адрес. Присваиваемый компьютеру IP-адрес должен быть частным адресом из диапазона частных адресов, указанных в табл. 15.3. Кроме этого, данный адрес не должен использоваться ни для какого другого устройства.

8. При использовании динамических IPv4-адресов выполните альтернативную настройку, задав маску подсети, основной шлюз, а также адреса DNS- и WINS-серверов. Завершив настройку альтернативного IP-адреса сетевого подключения, дважды нажмите кнопку **OK**, а затем **Закрыть**, чтобы сохранить настройки и закрыть все окна.

Примечание

Более подробные сведения по настройке ноутбуков приводятся в *разд. "Настройка сети для мобильных устройств" главы 16*.

Настройка нескольких шлюзов

Чтобы обеспечить отказоустойчивость в случае проблем с маршрутизатором, компьютеры под управлением Windows 8 можно настроить на использование нескольких основных шлюзов. Для нескольких шлюзов Windows 8 применяет метрики шлюзов, чтобы определить, какой из них использовать и когда. Метрика шлюза указывает затраты на маршрутизацию при использовании данного шлюза. Шлюз, который имеет самые низкие расходы на маршрутизацию, задействуется первым. Если компьютер не может связаться с этим шлюзом, Windows 8 пытается использовать следующий шлюз с наименьшей метрикой.

Лучший способ настроить несколько шлюзов зависит от конфигурации сети. Если компьютеры используют динамические адреса, скорее всего, будет желательным настроить дополнительные шлюзы посредством параметров DHCP-сервера. Если же компьютеры используют статические адреса или требуется назначить конкретные шлюзы, адреса шлюзов назначаются следующим образом:

1. В Панели управления щелкните по ссылке **Сеть и Интернет**, а в следующем окне — по ссылке **Центр управления сетями и общим доступом**.
2. Далее, в разделе **Просмотр активных сетей** щелкните по ссылке требуемого сетевого подключения.
3. В диалоговом окне **Состояние** нажмите кнопку **Свойства**. В результате откроется диалоговое окно свойств для данного сетевого подключения.
4. Дважды щелкните на протоколе: **Протокол Интернета версии 4 (TCP/IPv4)** или **Протокол Интернета версии 6 (TCP/IPv6)**.
5. Нажмите кнопку **Дополнительно** (Advanced), чтобы открыть диалоговое окно **Дополнительные параметры TCP/IP** (Advanced TCP/IP Settings) (рис. 15.4).
6. В области **Основные шлюзы** (Default gateways) отображаются адреса шлюзов, которые были настроены вручную (если таковые имеются). Если требуется, можно добавить дополнительные основные шлюзы. Для этого нажмите кнопку **Добавить**, а затем введите требуемый адрес шлюза в поле **Шлюз**.
7. По умолчанию Windows 8 автоматически присваивает шлюзу метрику. Метрику также можно присвоить вручную. Для этого снимите флажок **Автоматическое назначение метрики** (Automatic metric), а затем введите требуемую метрику в соответствующее поле.
8. Нажмите кнопку **Добавить**, а затем повторите шаги 6—7 для каждого добавляемого шлюза.
9. Трижды нажмите кнопку **OK**, а затем **Закрыть**, чтобы закрыть все диалоговые окна, связанные с настройкой дополнительных шлюзов.

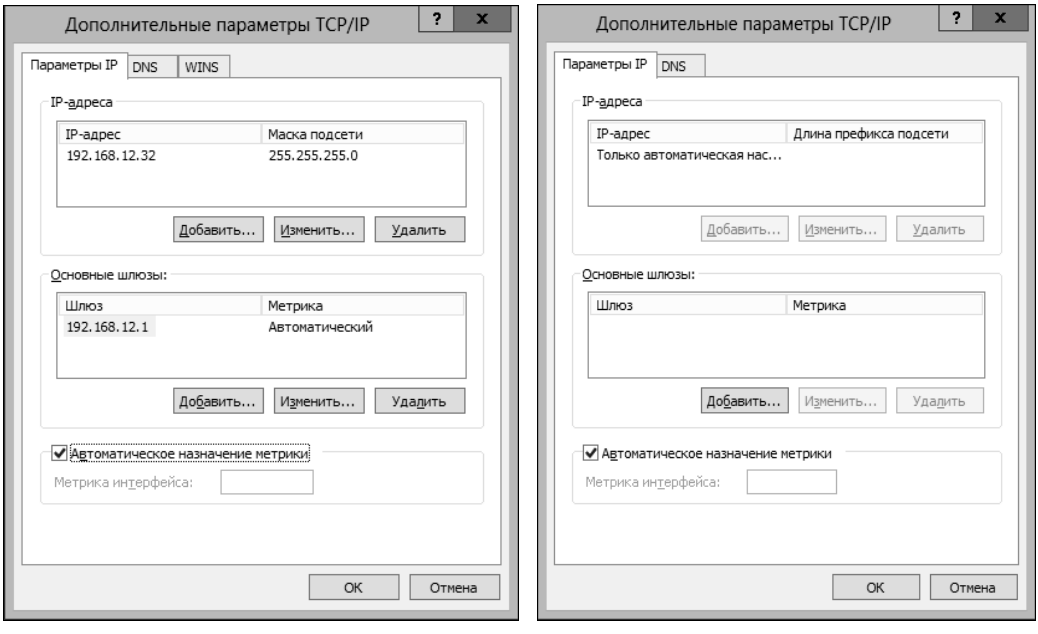


Рис. 15.4. Диалоговое окно **Дополнительные параметры TCP/IP**:
слева — для IPv4; *справа* — для IPv6

Настройка DNS-сервера

Служба DNS предоставляет услуги разрешения имен, ее можно использовать, чтобы определить IP-адрес компьютера по его имени хоста или наоборот. Это дает возможность пользователям работать с именами хостов, например, **http://www.msn.com** или **http://www.microsoft.com**, а не с IP-адресами, например, 192.168.5.102 или 192.168.12.68. Служба DNS является основной службой имен Windows 8 и Интернета.

Как и в случае с настройкой шлюзов, лучший способ настройки службы DNS зависит от конфигурации сети. Если компьютер использует динамические адреса, скорее всего, надо настроить DNS-сервер посредством параметров DHCP-сервера. Если же компьютер использует статические адреса или требуется настроить DNS-сервер для отдельного пользователя или системы, это следует сделать вручную.

Основные DNS-параметры

Основные параметры службы DNS можно настроить следующим образом:

1. В Панели управления щелкните по ссылке **Сеть и Интернет**, а в следующем окне — по ссылке **Центр управления сетями и общим доступом**.
2. Далее, в разделе **Просмотр активных сетей** щелкните по ссылке требуемого сетевого подключения.
3. В открывшемся диалоговом окне **Состояние** нажмите кнопку **Свойства**. В результате откроется диалоговое окно свойств для данного сетевого подключения.
4. Дважды щелкните на протоколе: **Протокол Интернета версии 4 (TCP/IPv4)** или **Протокол Интернета версии 6 (TCP/IPv6)**.

5. Если компьютер использует службы DHCP и требуется, чтобы адрес DNS-сервера был предоставлен этой службой, установите флажок **Получить адрес DNS-сервера автоматически**. В противном случае установите флажок **Использовать следующие адреса DNS-серверов**, а затем введите адреса основного и альтернативного сервера DNS в соответствующие поля.
6. Завершив настройку адреса DNS-сервера для подключения, дважды нажмите кнопку **OK**, а затем кнопку **Закрыть**, чтобы сохранить настройки и закрыть все окна.

Дополнительные DNS-параметры

Дополнительные DNS-параметры для подключения настраиваются на вкладке **DNS** диалогового окна **Дополнительные параметры TCP/IP** (рис. 15.5).

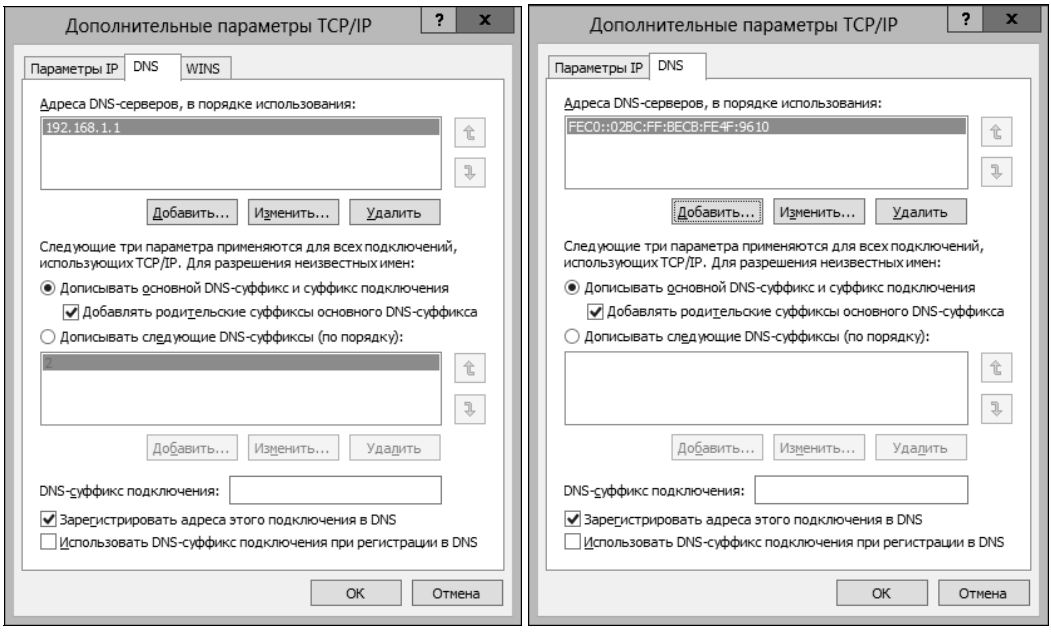


Рис. 15.5. Вкладка **DNS** диалогового окна **Дополнительные параметры TCP/IP** для настройки дополнительных параметров DNS: *слева* — для IPv4; *справа* — для IPv6

Опции на вкладке **DNS** используются следующим образом.

- **Адреса DNS-серверов, в порядке использования** (DNS server addresses, in order of use). В этом поле указываются IP-адреса всех DNS-серверов, которые используются в домене для разрешения имен. Чтобы добавить сервер в этот список, нажмите кнопку **Добавить**, а чтобы удалить сервер из списка — кнопку **Удалить**. Чтобы отредактировать адрес выбранного сервера, нажмите кнопку **Изменить**. Для предоставления услуг разрешения имен можно указать несколько DNS-серверов. Приоритет использования этих серверов определяется их порядковым положением в списке. Если первый сервер в списке не отвечает на запрос узла для разрешения имени, запрос направляется следующему DNS-серверу в списке, и т. д. Чтобы изменить положение сервера в списке, выберите в списке требуемый сервер, а затем переместите его вверх или вниз с помощью соответствующих стрелок справа от поля списка.

- **Дописывать основной DNS-суффикс и суффикс подключения** (Append primary and connection specific DNS suffixes). Обычно этот переключатель установлен по умолчанию. Эта опция применяется для разрешения неполных имен компьютеров в основном домене. Например, имя компьютера `Randolph` в родительском домене `microsoft.com` будет разрешено к полному имени компьютера `randolph.microsoft.com`. Если в домене отсутствует соответствующее полное имя компьютера, запрос завершается неудачей. Родительский домен указан на вкладке **Имя компьютера** диалогового окна **Свойства системы**. (Чтобы проверить эти параметры, щелкните в Панели управления по ссылке **Система и безопасность** и в открывшемся списке элементов этой категории выберите ссылку **Система**.)
- **Добавлять родительские суффиксы основного DNS-суффикса** (Append parent suffixes of the primary DNS suffix). Этот флажок установлен по умолчанию и применяется для разрешения неполных имен компьютеров посредством доменной иерархии с родительскими и дочерними элементами. Если имя не разрешается в непосредственном родительском домене, выполняется попытка разрешить запрос с помощью суффикса родителя родительского домена. Этот процесс продолжается до тех пор, пока не будет достигнута вершина доменной иерархии DNS. Например, чтобы определить полное имя компьютера `Randolph` в домене `dev.microsoft.com`, служба DNS сначала попытается разрешить полное имя компьютера как `randolph.dev.microsoft.com`. В случае неудачи, следующая попытка будет относиться к разрешению полного имени компьютера как `randolp.microsoft.com`.
- **Дописывать следующие DNS-суффиксы** (по порядку) (Append these DNS suffixes (in order)). Установите этот переключатель, чтобы указать DNS-суффиксы, которые следует использовать для разрешения имен вместо разрешения имен через родительский домен. Нажмите кнопку **Добавить**, чтобы добавить доменный суффикс в этот список; а чтобы удалить выбранный доменный суффикс из списка — кнопку **Удалить**. Чтобы отредактировать выбранный суффикс, нажмите кнопку **Изменить**. Можно задать несколько доменных суффиксов, которые будут использоваться в указанном порядке. Если разрешение по первому суффиксу оказывается неудачным, служба DNS попытается выполнить разрешение, используя следующий суффикс в списке, и т. д. до успешного разрешения или достижения последнего суффикса. Чтобы изменить порядок суффикса в списке, выберите требуемый суффикс, а затем переместите его вверх или вниз с помощью соответствующих кнопок-стрелок справа от поля списка.
- **DNS-суффикс подключения** (DNS suffix for this connection). В этом поле указывается конкретный DNS-суффикс для данного подключения, который имеет приоритет над DNS-именами, уже указанными для него. Но это доменное DNS-имя обычно устанавливается следующим образом: в Панели управления щелкните по ссылке **Система и безопасность**, в следующем окне — по ссылке **Система**, а справа в разделе **Имя компьютера, имя домена и параметра рабочей группы** (Computer name, domain, and workgroup settings) открывшегося окна **Система** щелкните по ссылке **Изменить параметры** (Change settings). На вкладке **Имя компьютера** открывшегося диалогового окна **Свойства системы** нажмите кнопку **Изменить**, а в следующем диалоговом окне — кнопку **Дополнительно**. В диалоговом окне **DNS-суффикс и NetBIOS-имя компьютера** (DNS Suffix and NetBIOS Computer Name) нажмите последовательно три раза кнопку **OK**, чтобы сохранить заданные настройки и закрыть все окна.
- **Зарегистрировать адреса этого подключения в DNS** (Register this connection's addresses in DNS). Установите этот флажок, если требуется зарегистрировать все IP-адреса для этого компьютера в службе DNS под полным доменным именем данного компьютера. Этот флажок установлен по умолчанию. Динамические обновления DNS

используются совместно со службой DHCP, чтобы позволить клиенту обновить свою A-запись (адрес хоста) в случае изменения его IP-адреса и разрешить DHCP-серверу обновить PTR-запись (указатель) для клиента на DNS-сервере. Серверы DHCP также можно настроить, чтобы обновлять как A-запись, так и PTR-запись от имени клиента. Динамические обновления DNS поддерживаются только DNS-сервером BIND 5.1 или более поздними версиями сервера, а также Microsoft Windows 2000 Server и более поздними версиями Windows.

- **Использовать DNS-суффикс подключения при регистрации в DNS** (Use this connection's DNS suffix in DNS registration). Установите этот флажок, если требуется зарегистрировать все IP-адреса для данного подключения в службе DNS под родительским доменом.

Настройка службы WINS

Служба WINS используется для сопоставления (разрешения) NetBIOS-имен компьютеров их IPv4-адресам. Службу WINS также можно использовать, чтобы помочь компьютерам сети определить адреса других компьютеров в сети. Если в сети установлен WINS-сервер, его можно использовать для разрешения имен компьютеров. Хотя служба WINS поддерживается всеми версиями Windows, в Windows 8 она применяется в основном для совместимости с более ранними версиями Windows.

Компьютеры под управлением Windows 8 также можно настроить на использование локального файла LMHOSTS для разрешения NetBIOS-имен компьютеров. Но обращение к файлу LMHOSTS выполняется только в том случае, если обычные способы разрешения имени не принесли результата. В правильно настроенной сети эти файлы редко применяются. Таким образом, предпочтительным способом разрешения NetBIOS-имен компьютеров является использование службы WINS и сервера WINS.

Как и в случае с настройкой шлюзов и DNS, лучший способ настройки службы WINS зависит от конфигурации сети. Если компьютеры используют динамические адреса, скорее всего, надо настроить WINS посредством параметров DHCP-сервера. Если же компьютеры используют статические адреса либо требуется настроить WINS-сервер для отдельного пользователя или системы, это следует сделать вручную.

Настройка параметров WINS выполняется следующим образом:

1. Откройте диалоговое окно **Дополнительные параметры TCP/IP** и перейдите в нем на вкладку **WINS** (рис. 15.6).
2. В поле **WINS-адреса, в порядке использования** (WINS addresses, in order of use) введите IPv4-адреса всех WINS-серверов, используемых для разрешения NetBIOS-имен. Чтобы добавить сервер в список, нажмите кнопку **Добавить**, а чтобы удалить сервер из списка — кнопку **Удалить**. Чтобы отредактировать выбранный сервер, нажмите кнопку **Изменить**.
3. Можно задать несколько серверов WINS, которые будут использоваться в указанном порядке. Если первый сервер в списке не отвечает на запрос узла для разрешения NetBIOS-имени, запрос направляется следующему WINS-серверу в списке, и т. д. Чтобы изменить положение WINS-сервера в списке, выберите в списке требуемый сервер, а затем переместите его вверх или вниз с помощью соответствующих кнопок-стрелок справа от поля списка.
4. Чтобы включить поиск в файле LMHOSTS, установите флажок **Включить просмотр LMHOSTS** (Enable LMHOSTS lookup). Если требуется использовать файл LMHOSTS, который находится на другом компьютере сети, импортируйте этот файл, нажав кнопку **Импорт LMHOSTS**. Файл LMHOSTS обычно используется только в том случае, когда все основные способы разрешения имени не дадут результатов.

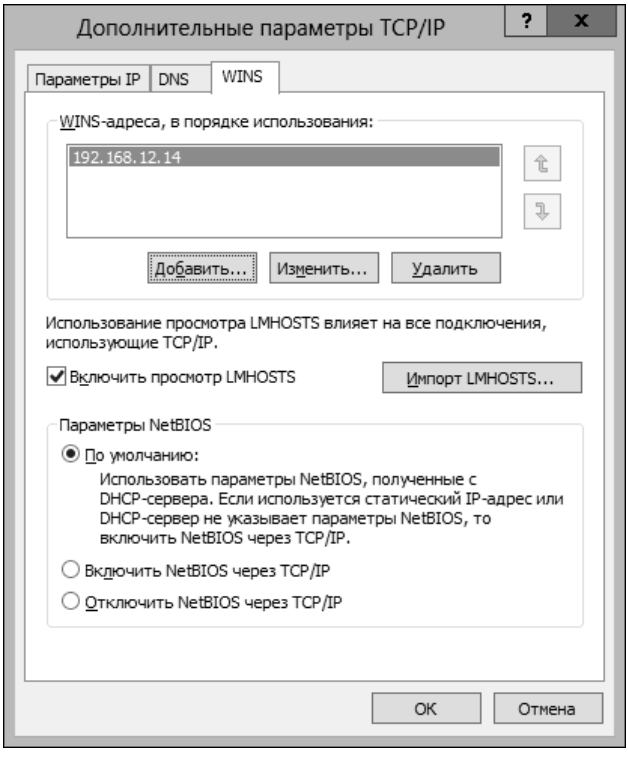


Рис. 15.6. Вкладка **WINS** для настройки WINS-сервера при настройке IPv4-протокола сетевого подключения

5. Для работы разрешения имен WINS требуются службы NetBIOS через TCP/IP. Для настройки разрешения имен WINS, используя NetBIOS, установите один из следующих переключателей.
   - При использовании для подключения динамического адреса параметры NetBIOS можно получить с DHCP-сервера. В таком случае установите переключатель **По умолчанию: использовать параметры NetBIOS, полученные с DHCP-сервера** (Default: Use NetBIOS setting from the DHCP server).
   - При использовании статического адреса или DHCP-сервера, которые не предоставляют параметры NetBIOS, установите переключатель **Включить NetBIOS через TCP/IP** (Enable NetBIOS over TCP/IP).
   - Если в сети не используются WINS и NetBIOS, установите переключатель **Отключить NetBIOS через TCP/IP** (Disable NetBIOS over TCP/IP). Это действие отключает широковещательные передачи NetBIOS, которые будут в противном случае отправляться компьютером.
6. Трижды нажмите кнопку **OK**, а затем кнопку **Закрыть**, чтобы закрыть все диалоговые окна, связанные с настройкой WINS. Повторите этот процесс для других сетевых адаптеров.

Совет

Файлы LMHOSTS содержатся локально на каждом компьютере, вследствие чего они со временем могут стать ненадежными. Вместо того чтобы полагаться на файлы LMHOSTS, обеспечьте правильную настройку серверов DNS и WINS и их доступность в сети для централизованного управления службами разрешения имен.

Управление сетевыми подключениями

Сетевые подключения позволяют компьютерам получать доступ к ресурсам в локальной сети и в Интернете. Для каждого установленного в компьютере сетевого адаптера автоматически создается соответствующее сетевое подключение. В этом разделе мы рассмотрим методы управления этими соединениями[1].

Включение и отключение сетевых подключений

Сетевые подключения создаются и включаются автоматически. Отключить сетевые подключения можно следующим образом:

1. В Панели управления щелкните по ссылке **Сеть и Интернет**, а в следующем окне — по ссылке **Центр управления сетями и общим доступом**.
2. В левой панели Центра управления сетями и общим доступом щелкните по ссылке **Изменение параметров адаптера**.
3. В открывшемся окне **Сетевые подключения** щелкните правой кнопкой мыши по значку требуемого подключения и в контекстном меню выберите команду **Отключить**.
4. Чтобы включить отключенное соединение, щелкните на нем правой кнопкой мыши и в контекстном меню выберите команду **Включить**.

Чтобы отключиться от сети, выполните следующие шаги:

1. В Панели управления щелкните по ссылке **Сеть и Интернет**, а в следующем окне — по ссылке **Центр управления сетями и общим доступом**.
2. В левой панели Центра управления сетями и общим доступом щелкните по ссылке **Изменение параметров адаптера**.
3. В открывшемся окне **Сетевые подключения** щелкните правой кнопкой мыши по значку требуемого подключения и в контекстном меню выберите команду **Отключение**. Обычно, эту опцию имеют только соединения удаленного доступа (например, модемы или беспроводные сетевые соединения).
4. Чтобы активировать отключенное от сети соединение, щелкните на нем правой кнопкой мыши и в контекстном меню выберите команду **Подключение**.

Проверка состояния, скорости и активности сетевых соединений

Проверить состояние сетевого соединения можно следующим образом:

1. В Панели управления щелкните по ссылке **Сеть и Интернет**, а в следующем окне — по ссылке **Центр управления сетями и общим доступом**.
2. Далее, в разделе **Просмотр активных сетей** щелкните по ссылке требуемого сетевого подключения.
3. В результате откроется диалоговое окно состояния для данного сетевого подключения. Но если соединение отключено или отсоединен сетевой кабель, это диалоговое окно будет недоступно. Включите соединение или подключите сетевой кабель, чтобы решить проблему, а затем снова попытайтесь открыть окно состояния подключения.

---

[1] Термины *"сетевое подключение"* и *"сетевое соединение"* являются эквивалентными.

По умолчанию диалоговое окно состояния подключения открывается на вкладке **Общие** (рис. 15.7), которая обычно, но не всегда, является единственной вкладкой сетевого подключения.

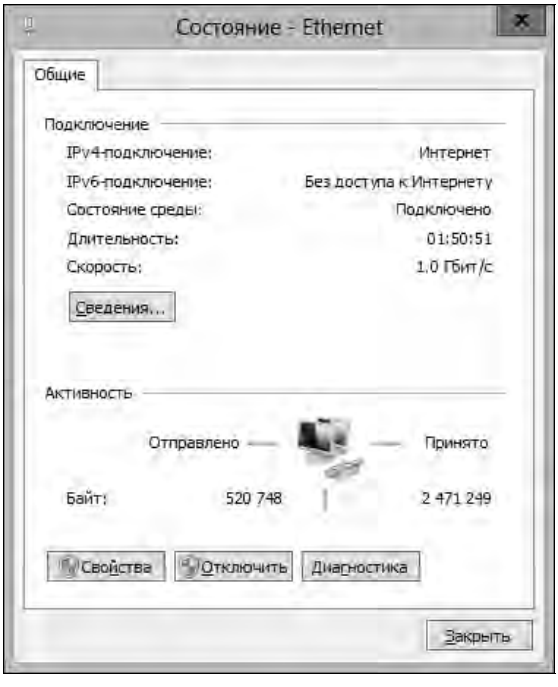


Рис. 15.7. Вкладка **Общие** диалогового окна **Состояние** сетевого подключения

Вкладка **Общие** содержит следующую информацию о подключении.

- **IPv4-подключение** (IPv4 Connectivity). Текущие состояние и тип соединения IPv4. Состояние соединения указывается как **Локальное** при подключении к локальной сети, как **Интернет**, когда имеется доступ к Интернету, или как **Без доступа к Интернету** (No Internet Access), когда нет доступа к Интернету.
- **IPv6-подключение** (IPv6 Connectivity). Текущие состояние и тип соединения IPv6. Состояние соединения указывается как **Локальное** при подключении к локальной сети, как Интернет, когда имеется доступ к Интернету, или как **Без доступа к Интернету**, когда нет доступа к Интернету.
- **Состояние среды** (Media State). Состояние сетевой среды. Так как диалоговое окно состояния доступно только при активном подключении, этот параметр обычно отображается как **Подключено** (Enabled).
- **Длительность** (Duration). Период времени, в течение которого действует соединение. Если это значение довольно небольшое, это означает, что либо пользователь подключился к сети сравнительно недавно, либо недавно был выполнен сброс подключения.
- **Скорость** (Speed). Скорость передачи данных по подключению. Скорость для подключения типа 10 Мбит/с Ethernet должна быть 10 Мбит/с, для подключения типа Fast Ethernet — 100 Мбит/с, а для подключения типа "гигабитный Ethernet" — 1,0 Гбит/с. Неправильное значение этого параметра может отрицательно сказаться на производительности компьютера.

- **Байт** (Bytes). Количество байтов, отправленных и полученных подключением. По мере отправки и получения пакетов компьютеров эти значения обновляются и поток трафика отображается морганием значка в виде экранов.

Просмотр конфигурационной информации сетевых соединений

В Windows 8 текущую конфигурационную информацию сетевого адаптера можно просматривать несколькими способами. В частности, эту информацию можно просматривать в диалоговом окне **Состояние** так:

1. В Панели управления щелкните по ссылке **Сеть и Интернет**, а в следующем окне — по ссылке **Центр управления сетями и общим доступом**.
2. В левой панели Центра управления сетями и общим доступом щелкните по ссылке **Изменение параметров адаптера**.
3. В открывшемся окне **Сетевые подключения** дважды щелкните на требуемом соединении. В результате откроется диалоговое окно состояния для данного сетевого подключения. Но если соединение отключено или отсоединен сетевой кабель, это диалоговое окно будет недоступно. Включите соединение или подключите сетевой кабель, чтобы решить проблему, а затем снова попытайтесь открыть окно состояния подключения.
4. Нажмите кнопку **Сведения** (Details), чтобы просмотреть подробную информацию об IP-параметрах данного соединения, включая следующую:
   - **Физический адрес** (Physical Address) — адрес машины или адрес управления доступом к среде (MAC[1]) сетевого адаптера. Этот адрес уникален для каждого сетевого адаптера;
   - **Адрес IPv4** (IPv4 Address) — IPv4-адрес, присвоенный данному сетевому подключению;
   - **Маска подсети IPv4** (IPv4 Subnet Mask) — маска подсети IPv4, к которой принадлежит данное сетевое подключение;
   - **Шлюз по умолчанию IPv4** (IPv4 Default Gateway) — IPv4-адрес основного шлюза для данного сетевого подключения;
   - **DNS-сервер IPv4** (IPv4 DNS Servers) — IP-адреса DNS-серверов для данного сетевого подключения;
   - **WINS-сервер IPv4** (IPv4 WINS Servers) — IP-адреса WINS-серверов для данного сетевого подключения;
   - **DHCP-сервер IPv4** (IPv4 DHCP Server) — IPv4-адрес DHCPv4-сервера, от которого была получена аренда текущего IPv4-адреса сетевого подключения (только для DHCPv4);
   - **Аренда получена** (Lease Obtained) — дата и время получения от DHCPv4 аренды адреса (только для DHCPv4);
   - **Аренда истекает** (Lease Expires) — дата и время истечения аренды адреса, полученного от DHCPv4 (только для DHCPv4).

[1] Media Access Control — управление доступом к среде.

Для просмотра расширенных настроек подключения можно также использовать команду `ipconfig`. Процедура для этого следующая:

1. Откройте консоль командной строки. Один из способов сделать это — выполнить команду `cmd` в поле поиска панели **Приложения**.
2. В консоли командной строки выполните команду `ipconfig /all`, чтобы просмотреть подробную информацию для всех сетевых адаптеров, установленных на компьютере.

> ***Примечание***
>
> Запущенная таким образом консоль командной строки работает в пользовательском режиме, а не в режиме администратора.

Переименование сетевых соединений

Windows 8 присваивает новым сетевым соединениям имена по умолчанию. Сетевому соединению можно присвоить новое имя. Для этого в окне **Сетевые подключения** щелкните правой кнопкой мыши на требуемом соединении, в контекстном меню выберите команду **Переименовать**, а затем введите новое имя соединения. Возможность переименования подключений полезна в том случае, когда компьютер имеет несколько сетевых подключений. Таким образом, каждому из них можно присвоить имя, отражающее назначение данного подключения. Доступ к окну **Сетевые подключения** можно получить, щелкнув в левой панели Центра управления сетями и общим доступом по ссылке **Изменение параметров адаптера**.

Диагностирование и тестирование сетевых параметров

Операционная система Windows 8 содержит довольно обширный набор инструментов для диагностирования и проверки работоспособности сетей TCP/IP. В последующих разделах мы рассмотрим автоматическое диагностирование, основные тесты, которые следует выполнять при каждой установке или изменении сетевых параметров компьютера, а также методы для решения сложных сетевых проблем, связанных со службами DHCP и DNS. А в последнем разделе обсудим выполнение подробного диагностического тестирования сети.

Диагностирование и решение проблем сетевых соединений

Иногда причиной неработоспособности сетевого подключения может быть отсоединенный сетевой кабель или временная проблема с сетевым адаптером. После подсоединения сетевого кабеля или решения проблемы адаптера сетевое подключение должно быть автоматически восстановлено. Диагностику проблем сетевого подключения можно выполнить, щелкнув правой кнопкой мыши по значку сети в области уведомлений панели задач и выбрав в контекстном меню команду **Диагностика неполадок** (Troubleshoot problems).

Данное действие запустит средство **Диагностика сетей Windows** (Windows Network Diagnostics), которое попытается определить причину проблемы. Средство диагностики сетей Windows также можно запустить, щелкнув правой кнопкой мыши по сетевому соединению в окне **Сетевые подключения** и выбрав в контекстном меню команду **Диагностика**.

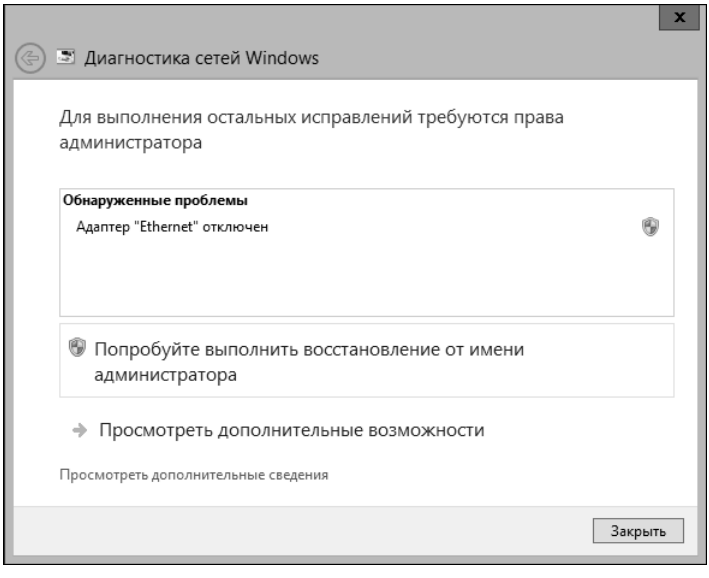


Рис. 15.8. Страница средства диагностики со списком возможных решений проблемы сетевого подключения

Если после выполнения начальной диагностики средство обнаружит известные проблемы конфигурации, будет отображен список возможных решений этих проблем (рис. 15.8).

Некоторые предлагаемые решения исполняются автоматически, по щелчку на соответствующей ссылке. Другие решения требуется реализовывать вручную, например, выполнить сброс сетевого маршрутизатора или широкополосного модема. Если предложенные решения не принесут желаемого результата, попробуйте другие, представленные по ссылке **Просмотреть дополнительные возможности**.

Диагностирование и решение проблем подключений Интернета

Так как между службами, протоколами и настройками параметров существует много взаимозависимостей, задача диагностирования проблем интернет-подключений может оказаться не из легких. К счастью, Windows 8 содержит мощное средство диагностики для локализации причин следующих проблем:

- общих проблем сетевой связности;
- проблем с параметрами интернет-служб для электронной почты, групп новостей и прокси-серверов;
- проблем с модемами, сетевыми клиентами и сетевыми адаптерами;
- проблем с настройками служб DNS, DHCP и WINS;
- проблем с основными шлюзами и IP-адресами.

Для диагностирования проблем подключения щелкните в Центре управления сетями и общим доступом на ссылке **Устранение неполадок**, а в следующем окне выберите требуемое средство поиска и устранения неполадок, например, **Сетевой адаптер**, **Входящие подключения** или **Подключения к Интернету**.

Запущенное средство попытается определить причину проблемы. Если средство обнаружит известные проблемы конфигурации, будет выведен список возможных решений этих проблем. Некоторые предлагаемые решения исполняются автоматически, по щелчку на соответствующей ссылке. Другие решения требуется реализовывать вручную, например, выполнить сброс сетевого маршрутизатора или широкополосного модема. Если предложенные решения не принесут желаемого результата, попробуйте другие, представленные в списке дополнительных возможностей.

Выполнение основных сетевых тестов

При настройке нового компьютера или изменении настроек сетевых параметров компьютера следует проверить конечные результаты. Самым основным TCP/IP-средством тестирования подключения компьютера к сети является команда `ping`. Чтобы проверить наличие сетевого подключения к определенному компьютеру, выполните команду `ping` *<хост>*, где *<хост>* обозначает имя или IP-адрес компьютера, связь с которым нужно проверить.

В Windows 8 команду `ping` можно использовать для проверки сетевой конфигурации следующим образом.

- **Проверка IP-адресов.** Если компьютер настроен должным образом и требуемый хост доступен по сети, выполнение команды `ping` по адресу этого хоста должно возвратить ответ от него (при условии, что прохождение этой команды разрешено брандмауэром компьютера). Если пакеты команды `ping` теряются по пути к целевому компьютеру или блокируются его брандмауэром, выводится сообщение о превышении предела времени ожидания ответа на запрос.
- **Проверка NetBIOS-имен компьютеров в доменах, использующих службу WINS.** Если NetBIOS-имена компьютеров разрешаются правильно командой `ping`, это означает, что средства NetBIOS компьютера, такие как служба WINS, настроены правильно.
- **Проверка DNS-имен хостов в доменах, использующих службу DNS.** Если DNS-имена компьютеров разрешаются правильно командой `ping`, это означает, что служба разрешения имен DNS настроена правильно.

Полезно также протестировать работу сети, попытавшись найти в ней определенный компьютер. Если компьютер является членом домена Windows 8 и разрешен просмотр компьютеров по всему домену, войдите в систему на настроенном компьютере, а затем с помощью Проводника Windows или сетевого проводника попробуйте выполнить просмотр других компьютеров домена. Затем войдите в систему на другом компьютере домена и попробуйте просмотреть компьютер, с которого перед этим выполняли просмотр других компьютеров домена. Эти проверки позволят определить, работает ли должным образом служба DNS в локальной среде. Если с просмотром компьютеров сети возникают проблемы, проверьте настройки служб и протоколов DNS.

ПРАКТИЧЕСКИЙ СОВЕТ

Доступ к сетевым ресурсам посредством сетевого проводника зависит от службы **Браузер компьютеров** (Computer Browser) и параметров сетевого обнаружения. Служба **Браузер компьютеров** отвечает за содержание списка компьютеров в сети. Если эта служба остановлена или не работает должным образом, компьютер не сможет видеть доступные ресурсы в сетевом проводнике. Проверить состояние службы **Браузер компьютеров** можно в консоли **Управление компьютером**. Для этого разверните в дереве консоли узел **Службы и приложения** и выберите в нем подузел **Службы**. Состояние службы **Браузер компьютеров** должно быть указано, как **Выполняется** (Started). Если поле состояния службы пустое, она не работает и ее следует запустить.

В некоторых случаях служба **Браузер компьютеров** может работать нормально, но в сетевом проводнике может не отображаться актуальный список сетевых ресурсов. Причиной этому может быть то обстоятельство, что служба выполняет обновления списка ресурсов периодически, а не постоянно проверяет наличие изменений. Если требуемый ресурс не отображается в сетевом проводнике, можно подождать следующего обновления (которое в большинстве случаев должно выполниться не позже, чем через 15 минут) или же подключиться к ресурсу напрямую, используя его UNC-имя или IP-адрес *(см. разд. "Доступ к общим ресурсам и их использование" главы 13)*.

В некоторых случаях параметры обнаружения и общего доступа могут быть настроены на блокирование сетевого обнаружения. Тогда следует разрешить сетевое обнаружение следующим образом:

1. В разделе **Сеть и Интернет** Панели управления щелкните по ссылке **Просмотр состояния сети и задач**.
2. В левой панели открывшегося Центра управления сетями и общим доступом щелкните по ссылке **Изменение параметров адаптера**.
3. В открывшемся окне можно настроить параметры доступа к общим ресурсам и сетевого обнаружения для всех сетевых профилей. Установите требуемые значения параметров для каждого сетевого профиля. Например, если для данного профиля отключено сетевое обнаружение, когда оно должно работать, включите его, установив флажок **Включить сетевое обнаружение** (Turn on network discovery) для данного сетевого профиля.
4. Нажмите кнопку **Сохранить изменения**, чтобы применить заданные параметры.

Устранение проблем с IP-адресами

Текущие настройки IP-адреса компьютера можно получить, следуя инструкциям, изложенным в *разд. "Просмотр конфигурационной информации сетевых соединений" ранее в этой главе*. Если на компьютере возникают проблемы с доступом к сетевым ресурсам или взаимодействием с другими компьютерами, одной из возможных причин этому может быть проблема с IP-адресом. Проверьте текущий IP-адрес подключения, а также другие параметры IP-протокола. В процессе поиска и устранения неполадки руководствуйтесь следующим рекомендациям.

- Если компьютеру присвоен IPv4-адрес в диапазоне от 169.254.0.1 до 169.254.255.254, это означает, чтобы компьютер использует APIPA-адреса. Сетевому подключению присваивается автоматический частный IP-адрес в том случае, когда оно настроено для работы с DHCP, но его DHCP-клиент не может связаться с DHCP-сервером. При использовании технологии APIPA Windows 8 периодически проверяет наличие в сети DHCP-сервера. Если сетевое подключение в конечном итоге не получит динамический IP-адрес, это обычно означает наличие проблемы с данным сетевым подключением. Проверьте исправность и подключение сетевого кабеля и, если необходимо, протрассируйте кабель к сетевому коммутатору или концентратору, к которому он подсоединен.
- Если IPv4 и маска подсети компьютера имеют значение 0.0.0.0, это означает, что либо отключена сеть, либо была попытка использования IP-адреса, уже используемого в сети. В таком случае следует открыть окно **Сетевые подключения** и определить состояние данного сетевого соединения. Если соединение отключено или отсоединено, это состояние должно отображаться. Щелкните правой кнопкой мыши на подключении и в контекстном меню выберите команду **Включить** или **Исправить**. Если соединение уже включено, следует откорректировать настройки его IP-адреса.

- Если IP-адрес назначается динамически, проверьте, что этот адрес уже не используется другими компьютерами сети. Для этого отключите сетевой кабель от диагностируемого компьютера и выполните команду `ping` по этому IP-адресу с другого компьютера. Получение ответа будет означать, что данный IP-адрес используется каким-либо другим компьютером сети. Этот компьютер, вероятно, имеет неправильно настроенный статический адрес или неправильно настроенное резервирование.
- Если IP-адрес правильный, проверьте маску подсети и параметры шлюза, DNS-сервера и WINS-сервера, сравнив сетевые параметры диагностируемого компьютера с такими же параметрами компьютера с заведомо корректной сетевой конфигурацией. Больше всего проблем возникает с маской подсети. При использовании подсетей маска подсети для одной области сети может быть очень похожей на маску подсети для другой области. Например, маска подсети для одного сегмента сети может быть 255.255.255.240, а для другого — 255.255.255.248.

Освобождение и обновление DHCP-параметров

Серверы DHCP могут автоматически присваивать большое количество параметров сетевой конфигурации. Это такие параметры, как IP-адреса подключения, основного шлюза, основного и вторичного DNS-сервера, основного и вторичного WINS-сервера и др. Когда для подключения используется динамическая IP-адресация, ему дается в аренду определенный IP-адрес. Эта аренда действительна в течение определенного времени и должна периодически обновляться. Когда наступает время обновления аренды адреса, компьютер подает запрос DHCP-серверу, предоставившему исходную аренду. Если сервер доступен, аренда обновляется на новый период. Аренду адресов отдельных компьютеров можно обновлять вручную или с помощью DHCP-сервера.

В процессе выделения и обновления аренды IP-адреса могут возникнуть проблемы, влияющие на нормальное сетевое взаимодействие. Если компьютер не сможет связаться с DHCP-сервером до истечения срока аренды IP-адреса, этот адрес может стать недействительным. Если это случится, компьютер может использовать альтернативную конфигурацию IP-протокола, чтобы получить альтернативный адрес. В большинстве случаев параметры альтернативной конфигурации будут неправильными, вследствие чего нормальная связь будет невозможна. Для решения этой проблемы нужно освободить, а затем обновить аренду IP-параметров.

Другая проблема возникает, когда пользователи перемещаются из одного офиса организации в другой и, соответственно, из одной подсети организации в другую. В процессе такого перемещения с одного места в другое компьютер пользователя может получить IP-параметры не от того DHCP-сервера. Когда пользователь возвращается назад в основной офис, компьютер может работать медленно или с ошибками вследствие получения IP-параметров от DHCP-сервера, обслуживающего другое место и другой сегмент сети. Эта проблема также решается освобождением и последующим обновлением аренды IP-параметров.

Освободить и обновить аренду IP-параметров можно следующим образом:

1. В левой панели Центра управления сетями и общим доступом щелкните по ссылке **Изменение параметров адаптера**.
2. В следующем окне, **Сетевые подключения**, щелкните правой кнопкой мыши по значку требуемого подключения и в контекстном меню выберите команду **Диагностика**.
3. Запустится средство диагностики сетей Windows, которое попытается определить причину проблемы, а затем выведет список возможных проблем и вероятных решений этих

проблем. Если компьютеру присвоено один или несколько динамических IP-адресов, одним из рекомендуемых решений будет **Автоматически получить новые параметры IP** (Automatically get new IP settings). Выберите эту ссылку и следуйте выводимым инструкциям.

Сбросить и обновить IP-параметры можно также с помощью команды `ipconfig` следующим образом:

1. Откройте консоль командной строки от имени администратора. Один из способов сделать это — ввести `cmd` в поле поиска панели **Приложения**, на экране **Приложения** щелкнуть правой кнопкой мыши по значку **Командная строка**, а затем в открывшейся панели внизу экрана щелкнуть на опции **Запуск от имени администратора**.
2. Чтобы сбросить текущие параметры для всех сетевых адаптеров, выполните команду `ipconfig /release`, а затем обновите аренду параметров, выполнив команду `ipconfig /renew`.
3. Чтобы только обновить аренду IP-параметров без предварительного их сброса, выполните только команду `ipconfig /renew`.
4. Просмотреть текущие IP-параметры можно, выполнив команду `ipconfig /all`.

Практический совет

Если перед обновлением аренды IP-параметров не выполнить их сброс, компьютер будет пытаться обновить параметры для сети, к которой он был подключен последний раз. Если в настоящее время компьютер подключен к другой сети, ему, возможно, не удастся установить подключение к DHCP-серверу, который выдал исходную аренду IP-параметров.

Если компьютер оснащен несколькими сетевыми адаптерами, но требуется настроить только один или часть из них, это можно сделать, указав после команды `ipconfig /renew` или `ipconfig /release` имя сетевого подключения или только часть его. Для обозначения любого единственного или нескольких символов подключения употребляется подстановочный символ звездочки (*). Например, чтобы обновить аренду IP-параметров для всех сетевых подключений, чьи имена начинаются с символов `loc`, выполните команду `ipconfig /renew loc*`. А сбросить IP-параметры для всех сетевых подключений, содержащих слово `network`, можно, выполнив команду `ipconfig /release *network*`.

Очистка и перерегистрация кэша DNS

Кэш сопоставителя DNS-имен содержит историю просмотров в DNS, которые выполнялись при обращении пользователя к сетевым ресурсам с использованием средств TCP/IP. Кэш содержит историю как прямых просмотров, которые сопоставляют имени хоста IP-адрес, так и обратных просмотров, которые сопоставляют IP-адресу имя хоста. После сохранения записи DNS для определенного DNS-узла в кэше сопоставителя локальному компьютеру больше не требуется запрашивать IP-информацию об этом узле у внешних DNS-серверов. Это позволяет компьютеру разрешать DNS-запросы локально, что ускоряет их выполнение.

Длительность хранения записей в кэше сопоставителя зависит от значения параметра **Срок жизни**, присвоенного записи узлом-источником. Чтобы просмотреть текущие записи кэша и их соответствующие значения параметра **Срок жизни**, выполните команду `ipconfig /displaydns` в консоли командной строки, открытой от имени администратора. Эти значения указываются, как количество секунд, в течение которых данная запись может содержаться в локальном кэше. Локальный компьютер непрерывно уменьшает эти значения. Когда значение срока жизни записи достигает нуля, запись больше не является действительной и удаляется из кэша сопоставителя.

Иногда возникает необходимость очистить кэш сопоставителя, чтобы удалить содержащиеся в нем записи и позволить компьютеру получить новые DNS-данные перед выполнением

очистки и записи в штатном порядке. Обычно такая необходимость возникает, когда изменяются IP-адреса серверов, а текущие записи в кэше сопоставителя продолжают указывать на старые адреса. Также иногда может произойти сбой синхронизации кэша сопоставителя, в особенности при неправильной конфигурации DHCP.

> ***ПРАКТИЧЕСКИЙ СОВЕТ***
>
> Опытные администраторы знают, что за несколько недель до выполнения изменений им следует начинать уменьшать значения параметров **Срок жизни** DNS-записей, которые будут изменены. Обычно это означает уменьшение значения параметра **Срок жизни** с дней (или недель) до часов, что позволяет более быструю передачу изменений компьютерам, которые сохранили в кэше соответствующие DNS-записи. По завершению выполнения изменений следует восстановить исходное значение параметра **Срок жизни**, чтобы сократить количество запросов на обновление.

В большинстве случаев проблемы с кэшем сопоставителя DNS можно решить, очистив кэш или выполнив перерегистрацию DNS-записей, т. е. заполнив его новыми DNS-записями. При очистке кэша сопоставителя из него удаляются все DNS-записи, но новые записи создаются только при следующем DNS-запросе имени или IP-адреса компьютера. При перерегистрации DNS-записей Windows 8 пытается обновить все текущие аренды IP-параметров, после чего выполняет DNS-поиск для всех записей в кэше сопоставителя. Вследствие выполнения повторного поиска имен или IP-адресов компьютеров осуществляется обновление всех записей в кэше сопоставителя. Обычно следует только полностью очистить кэш и позволить компьютеру выполнять DNS-поиск и внесение соответствующей записи в кэш сопоставителя по мере надобности. Перерегистрацию DNS-записей следует выполнять только в случае подозрения наличия проблем с DHCP и кэшем сопоставления DNS.

Очистить кэш сопоставления и выполнить перерегистрацию DNS-записей можно с помощью команды `ipconfig`. Процедура для этого следующая:

1. Откройте консоль командной строки от имени администратора. Один из способов сделать это — ввести `cmd` в поле поиска панели **Приложения**, на экране **Приложения** щелкнуть правой кнопкой мыши по значку **Командная строка**, а затем в открывшейся панели внизу экрана щелкнуть на опции **Запуск от имени администратора**.
2. Чтобы очистить кэш сопоставления, выполните в консоли команду `ipconfig /flushdns`.
3. Чтобы обновить все DHCP-аренды и выполнить перерегистрацию DNS-записей, выполните в консоли команду `ipconfig /registerdns`.
4. Проверить результаты выполнения команд очистки и перерегистрации можно, выполнив в консоли команду `ipconfig /displaydns`.

ГЛАВА 16

Управление мобильными сетями и удаленным доступом

Пользователи часто хотят подключаться к сети своей организации с удаленного компьютера. Для этого им требуется какое-либо средство подключения — коммутируемое или широкополосное соединение, соединение по виртуальной частной сети (virtual private network, VPN) или по DirectAccess. Коммутируемое соединение позволяет пользователям подключиться с удаленного компьютера к сети своей организации, используя модем и обычную телефонную линию. Широкополосное соединение делает возможным удаленное подключение к сети с помощью высокоскоростного маршрутизатора DSL или кабельного модема. Соединения VPN или DirectAccess используют шифрование, чтобы предоставить безопасную связь по существующему соединению, которое может быть подключением по локальной сети, коммутируемым или широкополосным соединением. Кроме этого, все большее распространение получают беспроводные соединения. Для использования беспроводного соединения компьютер оснащается сетевым адаптером в виде радиоприемопередатчика, который взаимодействует с подобными сетевыми устройствами на других компьютерах.

Настройка сети для мобильных устройств

Для большинства мобильных устройств требуется несколько сетевых конфигураций: одна для офиса, другая для дома, а третья, например, для командировок или отпусков. На работе мобильному устройству сетевые параметры назначаются DHCP-сервером сети организации. А дома мобильное устройство использует другие сетевые параметры для работы в домашней сети и для доступа к общему принтеру и устройству широкополосного доступа к Интернету. В некоторых случаях может понадобиться настроить мобильное устройство для использования Wi-Fi-соединения, когда пользователь работает вдали от своего обычного рабочего места, и для использования сетевого подключения с параметрами, присвоенными DHCP-сервером, когда устройство подключено к проводной сети, или наоборот. Систему, которая получает основные сетевые параметры посредством протокола DHCP, можно настроить на использование альтернативных сетевых параметров на случай, когда DHCP-сервер недоступен, например, когда пользователь работает дома или во время командировки. Система может использовать альтернативные конфигурации либо автоматически, либо с вмешательством пользователя. На совещаниях или в других подобных ситуациях, возможно, понадобится подключение мобильного устройства к сетевым проекторам. Эта задача с легкостью решается с помощью мастера подключения к сетевому проектору (Connect to a Network Projector wizard).

Управление мобильными параметрами

Центр мобильности Windows (рис. 16.1) представляет собой универсальное средство для управления важными параметрами мобильных устройств посредством набора плиток, предоставляющих быстрый доступ к наиболее часто употребляемым параметрам.

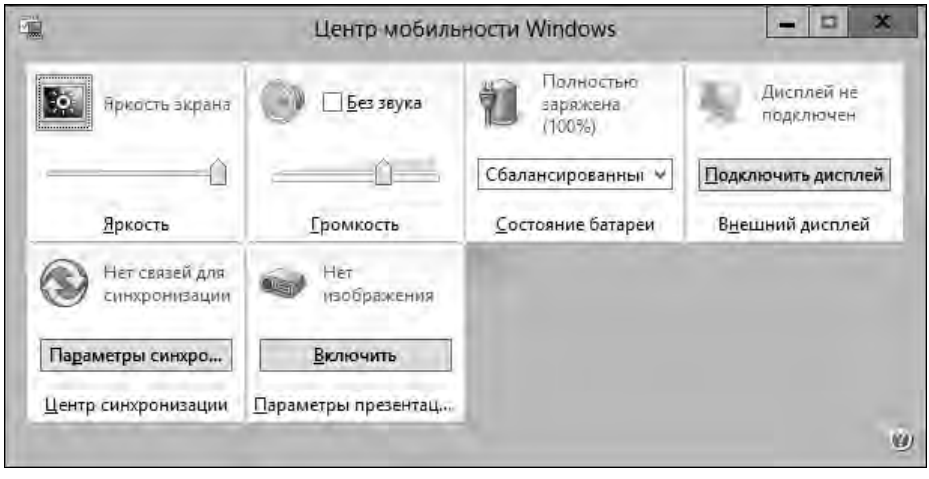


Рис. 16.1. Главное окно Центра мобильности Windows

Центр мобильности Windows можно открыть, щелкнув правой кнопкой мыши по значку питания в области уведомлений панели задач и выбрав в контекстном меню команду **Центр мобильности Windows** (Windows Mobile Center). Также его можно открыть из Панели управления, щелкнув в разделе **Оборудование и звук** по ссылке **Настройка параметров мобильности по умолчанию** (Adjust commonly used mobility settings).

Плитки Центра мобильности позволяют выполнять настройку параметров мобильности, используя такие средства, как ползунки (для настройки, например, яркости экрана), раскрывающиеся списки (для выбора, например, плана электропитания) и переключатели (для включения или отключения, например, параметров презентации). Хотя набор доступных плиток управления зависит от типа и производителя мобильного устройства, наиболее часто встречаются следующие.

- **Состояние батареи** (Battery Satus). Отображает состояние батареи компьютера. В раскрывающемся списке можно переключиться с одного стандартного плана электропитания на другой. Если были созданы пользовательские планы электропитания, они также предоставляются в списке. Щелчок по значку на плитке открывает окно **Электропитание**.
- **Яркость** (Brightness). Позволяет управлять параметрами яркости экрана путем перемещения ползунка влево или вправо. Щелчок по значку на плитке открывает окно **Изменить параметры плана** (Change plan settings) для настройки параметров плана электропитания. Обратите внимание, что значок питания в области уведомления панели задач имеет подобные опции, и панель **Параметры** также имеет на ней элемент управления **Яркость**.
- **Внешний дисплей** (External Display). Позволяет подключить второе устройство отображения, что может потребоваться для презентации. Для доступа к вторичному устройству отображения, подключенному посредством кабеля, нажмите кнопку **Подключить дис-**

плей (Connect Display). Щелчок по значку дисплея на плитке открывает окно **Разрешение экрана** для настройки разрешения экрана.

- **Параметры презентации** (Presentation Settings). Позволяет включать и отключать режим презентации. В режиме презентации дисплей и жесткий диск мобильного устройства не переходят в режим сна при простаивании компьютера. Чтобы включить режим презентации, нажмите кнопку **Включить**. Щелчок по значку проектора на плитке открывает диалоговое окно **Параметры презентации** (Presentation Settings).
- **Центр синхронизации** (Sync Center). Позволяет просматривать состояние синхронизации автономных файлов и запускать синхронизацию. Щелчок по значку синхронизации на плитке открывает окно Центра синхронизации.
- **Громкость** (Volume). Позволять регулировать громкость выходного аудиоустройства путем перемещения ползунка влево или вправо. Установка флажка **Без звука** (Mute) отключает звук. Щелчок по значку динамика на плитке открывает диалоговое окно **Звук** для настройки параметров записи и воспроизведения. Обратите внимание, что значок **Динамики** (Volume) в области уведомления панели задач имеет подобные опции.

> ***Примечание***
>
> Некоторые производители мобильных устройств модифицируют Центр мобильности Windows, добавляя в него плитки управления для расширения этих общих возможностей. Например, некоторые Центры мобильности мобильных устройств компании Hewlett-Packard содержат плитку управления **HP Wireless Assistant**, которую можно использовать для настройки параметров беспроводной сети для встроенного беспроводного устройства.

Мобильным пользователям будет полезна информация о том, как быстро отключить сетевые возможности. Это можно сделать несколькими способами, но самым легким будет включить режим "в самолете" (Airplane mode). Включение этого режима временно отключает все сетевые функциональности, а выключение возвращает их в исходное рабочее состояние. Чтобы включить режим "в самолете", откройте панель **Сети**, щелкнув по значку сети в области уведомлений панели задач, и включите режим "в самолете", установив соответствующий переключатель. Обратите внимание на то, что *включение* режима "в самолете" *отключает* беспроводные сетевые возможности.

Режим "в самолете" можно также включить следующим способом:

1. Проведите пальцем справа к центру экрана или нажмите комбинацию клавиш <Windows>+<I>.
2. Щелкните по значку текущей сети.
3. Установите переключатель режима "в самолете", что должно изменить его состояние на **Вкл** (включен).

Повторение этой процедуры устанавливает состояние переключателя в **Откл** (выключен).

Настройка динамических IP-адресов

Служба DHCP предоставляет возможность централизованного управления IP-адресами и значениями по умолчанию параметров TCP/IP. Если в сети установлен DHCP-сервер, любому сетевому адаптеру компьютера можно присвоить динамический IP-адрес. Впоследствии задача по предоставлению основной информации, требуемой для функционирования TCP/IP-сети, возлагается на DHCP-сервер. Чтобы включить возможность динамического назначения IP-адресов как для IPv4, так и для IPv6, для этих протоколов необходимо установить отдельные службы DHCP.

Настройка динамических адресов выполняется следующим образом:

1. В разделе **Сеть и Интернет** Панели управления щелкните по ссылке **Просмотр состояния сети и задач**.
2. В левой панели Центра управления сетями и общим доступом щелкните по ссылке **Изменение параметров адаптера**.
3. В результате откроется окно **Сетевые подключения**, содержащее список (или значки, в зависимости от выбранного представления) всех сетевых подключений компьютера. Щелкните правой кнопкой мыши на требуемом подключении и в контекстном меню выберите команду **Свойства**.
4. В списке компонентов дважды щелкните на компоненте **Протокол Интернета версии 4 (TCP/IPv4)** (Internet Protocol Version 4 (TCP/IPv4)), в результате чего откроется диалоговое окно свойства выбранного протокола (рис. 16.2). (Это окно можно также открыть, выбрав компонент **Протокол Интернета версии 4 (TCP/IPv4)** и нажав кнопку **Свойства**.)

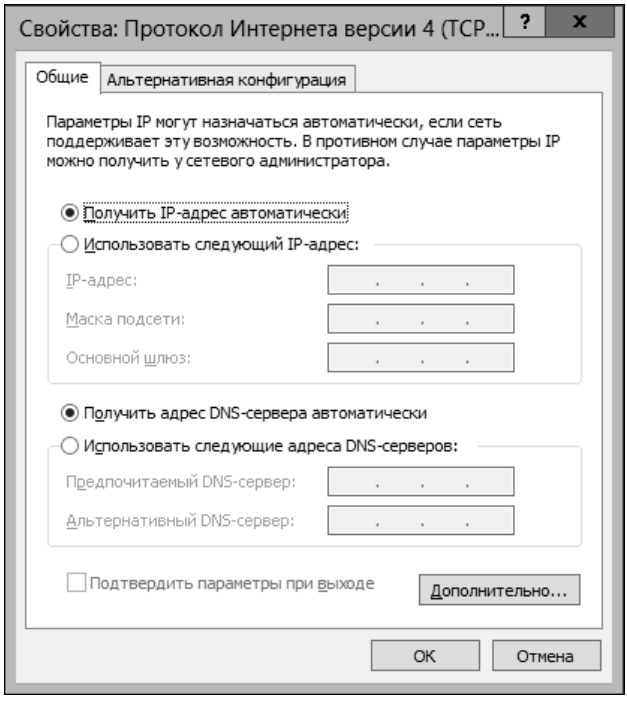


Рис. 16.2. Окно свойств протокола IPv4 для настройки IP-адреса подключения

5. Установите переключатель **Получить IP-адрес автоматически**. Для DNS-сервера можно задать автоматическое получение адреса или его ручную настройку, установив переключатель **Получить адрес DNS-сервера автоматически** или переключатель **Использовать следующие адреса DNS-серверов** соответственно. При ручной настройке адреса DNS-сервера введите требуемые адреса для предпочитаемого и альтернативного DNS-серверов в соответствующие поля.
6. Нажмите кнопку **OK**, чтобы сохранить настройки и закрыть окно.
7. Для настройки параметров протокола IPv6 дважды щелкните на соответствующем компоненте в списки компонентов, в результате чего откроется окно свойств протокола,

почти такое же, как и для протокола IPv4. Установите в нем переключатель **Получить IPv6-адрес автоматически**. Для адреса DNS-сервера можно задать автоматическое получение адреса или его ручную настройку, установив переключатель **Получить адрес DNS-сервера автоматически** или переключатель **Использовать следующие адреса DNS-серверов** соответственно. При ручной настройке адреса DNS-сервера введите требуемые адреса для предпочитаемого и альтернативного DNS-серверов в соответствующие поля. Нажмите кнопку **OK**, чтобы сохранить настройки и закрыть окно.

8. Выполните настройку альтернативных IP-адресов, как требуется *(см. следующий раздел)*.

Настройка альтернативных частных IP-адресов

Альтернативные IP-параметры можно настраивать только для протокола IPv4. При динамическом назначении IPv4-адреса подключению сервером DHCP, подключению присваивается автоматический частный IP-адрес в том случае, когда подключение не может обнаружить DHCP-сервер при загрузке или при обновлении аренды IP-адреса. Автоматический частный IP-адрес присваивается из диапазона адресов 169.254.0.1—169.254.255.254; при этом подключению также присваивается маска подсети 255.255.0.0. Так как конфигурация автоматического частного IP-адреса не содержит IP-адресов основного шлюза, DNS-сервера и WINS-сервера, использующий этот адрес компьютер изолируется в отдельном сетевом сегменте в диапазоне автоматических частных IP-адресов.

Если требуется обеспечить использование конкретного IP-адреса и другие параметры сетевого подключения при отсутствии DHCP-сервера, нужно задать альтернативную конфигурацию. Одной из основных причин для использования альтернативной конфигурации является удовлетворение требований пользователей мобильных устройств, которые берут свои компьютеры с работы домой. Таким образом, мобильное устройство можно настроить на использование в офисе динамически выделяемого IP-адреса, а дома — IP-адреса альтернативной конфигурации. Но прежде чем приступать к выполнению настроек компьютеров пользователей, полезно узнать у пользователей настройки их домашних сетей, включая IP-адреса сетевого подключения, шлюза и DNS-сервера, требуемые их поставщиками Интернета.

Выполнить настройку альтернативных частных IP-адресов можно следующим образом:

1. В разделе **Сеть и Интернет** Панели управления щелкните по ссылке **Просмотр состояния сети и задач**.
2. В левой панели Центра управления сетями и общим доступом щелкните по ссылке **Изменение параметров адаптера**.
3. В результате откроется окно **Сетевые подключения**, содержащее список (или значки, в зависимости от выбранного представления) всех сетевых подключений компьютера. Щелкните правой кнопкой мыши на требуемом подключении и в контекстном меню выберите команду **Свойства**.
4. В списке компонентов дважды щелкните на компоненте **Протокол Интернета версии 4 (TCP/IPv4)**, в результате чего откроется диалоговое окно свойств протокола. (Это окно можно также открыть, выбрав компонент **Протокол Интернета версии 4 (TCP/IPv4)** и нажав кнопку **Свойства**.)
5. Если протокол уже настроен на автоматическое получение IP-адреса, должна быть доступна вкладка **Альтернативная конфигурация** (рис. 16.3). В противном случае установите переключатель **Получить IP-адрес автоматически**, а затем перейдите на эту вкладку.

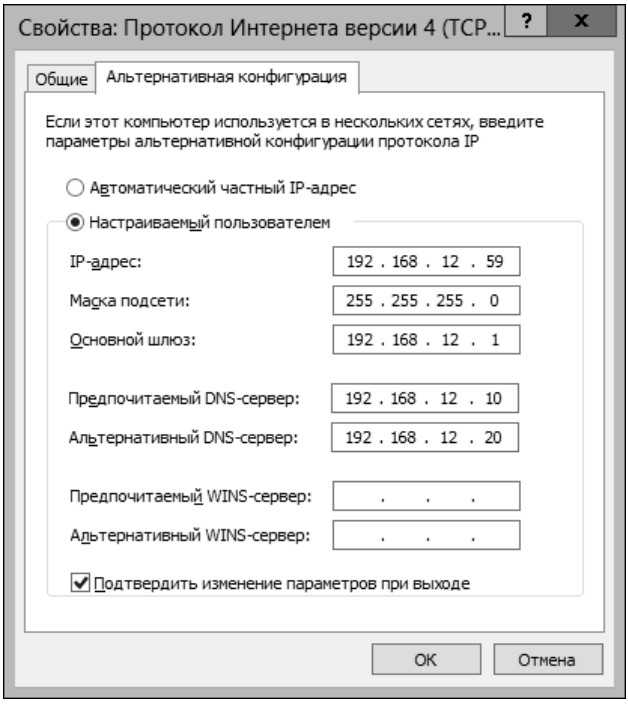


Рис. 16.3. Вкладка **Альтернативная конфигурация** окна свойств протокола IPv4 сетевого подключения

6. На вкладке **Альтернативная конфигурация** установите переключатель **Настраиваемый пользователем** (User configured). Далее в текстовое поле **IP-адрес** введите требуемый адрес. Присваиваемый компьютеру IP-адрес должен быть частным адресом и не должен использоваться никаким другим устройством при его использовании данным подключением. Частные IP-адреса занимают диапазон адресов 10.0.0.1—10.255.255.254, 172.16.0.1—172.31.255.254 и 192.168.0.1—192.168.255.254 (за исключением IP-адресов в этих диапазонах, зарезервированных для сетевых идентификаторов и широковещательных передач).
7. Значение поля **Маска подсети** (Subnet mask) обеспечивает правильную работу компьютера в сети. В это поле Windows 8 должна автоматически вставить значение по умолчанию. Если в сети не используются подсети, это значение по умолчанию должно быть приемлемым. Если же в сети используются подсети, это значение следует заменить значением, требуемым для данной сети.
8. Если компьютеру необходим доступ к другим сетям TCP/IP, Интернету или другим подсетям, следует указать адрес основного шлюза. Для этого в текстовое поле **Основной шлюз** введите IP-адрес основного маршрутизатора сети.
9. Серверы DNS требуются для разрешения доменных имен. Введите адреса предпочитаемого и альтернативного серверов DNS в соответствующие поля.
10. Если в сети используется служба WINS для совместимости с предыдущими версиями Windows, введите адреса предпочитаемого и альтернативного сервера WINS в соответствующие поля.
11. Завершив настройку альтернативного IP-адреса сетевого подключения, дважды нажмите кнопку **OK**, а затем кнопку **Закрыть**, чтобы сохранить настройки и закрыть все окна.

Подключение к сетевым проекторам

Многие залы заседаний и конференц-центры оснащены проекторами, которые нужны посетителями для презентаций. Чтобы использовать такой проектор, пользователю необходимо подключить свой компьютер к локальной сети центра, а затем получить по сети доступ к проектору, используя мастер подключения к сетевому проектору. Этот мастер выводит пошаговые инструкции для обнаружения проекторов в сети и подключения к требуемому.

Но прежде чем можно будет использовать этот мастер, необходимо установить функциональность **Сетевой проектор** (Network Projection). Делается это следующим образом:

1. В Панели управления щелкните по ссылке **Программы**, а в разделе **Программы и компоненты** следующего окна — по ссылке **Включение или отключение компонентов Windows**.
2. В открывшемся диалоговом окне **Компоненты Windows** установите флажок **Сетевой проектор**, а затем нажмите кнопку **OK**.

После установки этого компонента в разделе **Стандартные — Windows** экрана **Приложения** будет добавлена опция **Подключение к сетевому проектору** (Connect to a network projector). Она также должна быть доступной и на экране **Пуск**. Прежде чем приступать к презентации, желательно настроить стандартные параметры для презентации, которые выполняют следующее:

- отключают экранную заставку;
- устанавливают требуемый уровень громкости;
- отображают определенный фон или фоновое изображение.

Настройка этих параметров выполняется в диалоговом окне **Параметры презентации**. Его можно открыть из Центра мобильности, щелкнув по значку проектора на плитке **Параметры презентации**.

Подключение к сетевому проектору с помощью мастера подключения к сетевому проектору выполняется следующим образом:

1. На экране **Пуск** или **Приложения** щелкните по значку **Подключение к сетевому проектору**.
2. Если это первое подключение к сетевому проектору и доступ к нему блокируется брандмауэром Windows, в следующем окне мастера будет выведено соответствующее сообщение. Щелкните в этом окне по ссылке **Открыть доступ для сетевого проектора** (Allow the network projector to communicate with my computer), чтобы снять эту блокировку.
3. В следующем окне мастера предоставляется выбор способа подключения к проектору. Чтобы выполнить поиск доступных сетевых прокторов и выбрать из них требуемый, щелкните по ссылке **Выполнить поиск проектора** (Search for a projector). Мастер осуществит поиск сетевых проекторов и выведет результаты поиска совместно со списком недавно используемых проекторов, если такие имеются. Щелкните на требуемом проекторе, предоставьте пароль доступа к нему, если требуется, а затем нажмите кнопку **Далее**.
4. Если известен сетевой адрес требуемого проектора, щелкните по ссылке **Введите сетевой адрес проектора** (Enter the projector network address). На следующей странице мастера введите полный сетевой адрес проектора, например, **http://intranet.cpandl.local/projectors/confb-proj1**. На этой же странице введите пароль доступа, а затем нажмите кнопку **Подключить**.

5. Установив подключение к проектору, нажмите кнопку **Готово**, чтобы закрыть мастер подключения и приступить к работе с проектором.

Принципы работы мобильных сетей и удаленного доступа

Хотя коммутируемые, широкополосные, VPN- и DirectAccess-подключения основаны на фундаментально разных технологиях, все они позволяют пользователям подключаться к сети организации удаленно. В случае типичной сетевой конфигурации с автоматическим коммутируемым подключением удаленные пользователи используют подключенный (или встроенный) к своему компьютеру модем, чтобы подключиться по обычной телефонной линии к пулу модемов своей организации. Сервер Windows, обслуживающий модемный пул и исполняющий службу **Маршрутизация и удаленный доступ** (Routing and remote access), осуществляет проверку подлинности идентификатора входа и соответствующего пароля и разрешает пользователю подключиться к внутренней сети организации. После этого пользователь может использовать ресурсы этой сети таким же образом, как и на своем рабочем месте в организации.

На рис. 16.4 показано схематическое представление этого типа подключения к сети.

Рис. 16.4. Подключение к сети организации по телефонной линии с помощью модема

Аналоговые телефонные модемы используют выделенные телефонные линии для подключения пользователей к сети организации со скоростью до 33,6 Кбит/с. Цифровые телефонные модемы работают с каналами линий связи T1 для подключения пользователей к сети организации со скоростью до 56 Кбит/с. Стандартная конфигурация модемного пула может содержать 8, 12 или 16 модемов, каждый из которых имеет свою линию (или канал). Обычно для дозвона в модемный пул используется один ведущий номер первого модема пула. Когда этот номер занят, линия автоматически переключается на следующий номер, подключенный к следующему модему пула, и т. д., пока не будет обнаружен свободный модем. Таким образом, для доступа ко всем модемам пула пользователям нужно знать только один номер.

В отличие от прямых коммутируемых подключений, которые предоставляют непосредственное соединение с сетью организации, широкополосные подключения осуществляются через сеть поставщика Интернета. Посредством DSL-маршрутизатора, кабельного или сотового модема пользователь подключается к своему поставщику Интернета, а через него к Интернету. Далее, чтобы подключиться к сети своей организации, пользователю нужно установить DirectAccess- или VPN-подключение между своим компьютером и сетью организации. На рис. 16.5 показано схематическое представление этого типа подключения к удаленной сети.

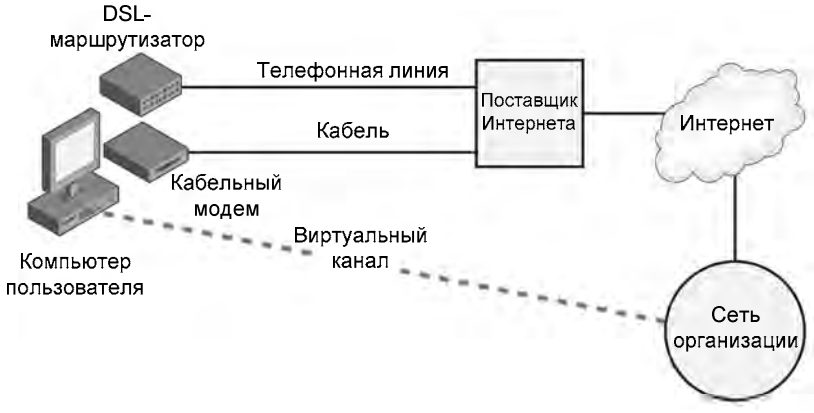


Рис. 16.5. Использование виртуального канала для подключения к сети организации

Виртуальная частная сеть (VPN) представляет собой расширение частной сети через общедоступную сеть Интернет. При подключении пользователя к такой сети для всех практических целей ему кажется, что он подключен непосредственно к сети организации. В частности, он имеет такой же доступ к сетевым ресурсам организации, как и со своего рабочего места в офисе. Такие бесшовные подключения возможны благодаря установке виртуального канала между компьютером пользователя и сетью организации, где VPN-технология обеспечивает маршрутизацию информации по Интернету. Обычно используется одна из двух VPN-технологий: протокол PPTP[1] или протокол L2TP[2].

Протоколы L2TP и PPTP предоставляют средства шифрования для защиты от атак, но только протокол L2TP использует набор протоколов IPSec для обеспечения защиты данных, что делает его более безопасным. К сожалению, настройка протокола L2TP также сопряжена с большими трудностями. При работе с протоколом L2TP требуется использовать службы сертификации Microsoft (Microsoft Certificate Services) или альтернативный сервер сертификатов для выдачи сертификатов каждой системе, которая будет подключаться к сети по протоколу L2TP.

Кроме использования широкополосного подключения для создания виртуальной частной сети можно использовать коммутируемое подключение. В такой конфигурации пользователь подключается к Интернету через своего поставщика услуг Интернета, а затем создает частное подключение к сети офиса. Когда эта конфигурация становится стандартной для пользователей коммутируемых подключений, организации не требуется наличие выделенных частных телефонных линий, как в случае конфигурации с модемным пулом.

Другим вариантом создания виртуального канала является использование технологии DirectAccess. Хотя она фундаментально отличается от VPN, ее основной принцип такой же — подключение DirectAccess является расширением частной сети через общественную сеть Интернет. При подключении пользователя таким образом (оно происходит автоматически при включенной функциональности DirectAccess) ему кажется, что он подключен непосредственно к сети организации. В частности, он имеет такой же доступ к сетевым ресурсам организации, как и со своего рабочего места в офисе. Такие бесшовные подключения возможны благодаря установке виртуального канала между компьютером пользователя

[1] Point-to-Point Tunneling Protocol — протокол туннелирования между двумя узлами.

[2] Layer 2 Tunneling Protocol — протокол туннелирования второго уровня.

и сетью организации, где технология DirectAccess обеспечивает маршрутизацию информации по Интернету.

В Windows Server 2012 функциональность DirectAccess и служба **Маршрутизация и удаленный доступ** совмещены в серверную роль RemoteAccess. Эта реализация функциональности работает иначе, чем ее первоначальная реализация для Windows Server 2008 R2. В новой реализации DirectAccess остается клиент-серверной технологией, которая полагается на протокол IPv6 и набор IPSec, но больше не требует инфраструктуры открытых ключей. Тогда как версия DirectAccess для Windows Server 2008 R2 использует два канала IPSec для установки связи с сетью организации, версия DirectAccess для Windows Server 2012 по умолчанию использует один такой канал (т. к. стандартная реализация не использует аутентификацию на основе сертификатов). Но для двухфакторной проверки подлинности (например, с помощью смарт-карты и технологии NAP[1]) использование DirectAccess требует двух каналов IPSec.

Версия DirectAccess для Windows Server 2012 поддерживает множественные домены и имеет встроенную поддержку для балансирования сетевой нагрузки. Тогда как при удаленном подключении клиенты DirectAccess взаимодействуют посредством протокола IPv6, сервер RemoteAccess содержит встроенные функциональности преобразования протоколов (NAT64) и шлюза разрешения имен (DNS64), которые могут преобразовывать сообщения формата IPv6 клиентов DirectAccess в формат IPv4 для внутренних серверов. Это позволяет клиенту DirectAccess обращаться к компьютерам внутренней сети организации, работающим только с протоколом IPv4, но не позволяет таким компьютерам инициировать подключения к клиентам DirectAccess. Причина этому в том, что преобразование сетевых адресов является однонаправленным процессом, предназначенным для передач, инициируемых клиентами DirectAccess.

Клиентские компьютеры должны работать под управлением Windows 7 Enterprise или более поздних версий Windows. Серверные компьютеры должны работать под управлением Windows Server 2008 R2 или более поздних версий Windows. Для работы с DirectAccess нужно установить и настроить протокол IPv6 для всех клиентских и серверных компьютеров организации, включая необходимую настройку параметров DNSv6 и DHCPv6.

Для управления работой DirectAccess можно использовать параметр политики **Маршрутизировать весь трафик через внутреннюю сеть** (Route all traffic through the internal network), который находится в узле **Конфигурация компьютера\Административные шаблоны\Сеть\Сетевые подключения** редактора объекта групповой политики. По умолчанию, когда пользователь подключен к сети организации, его компьютер имеет прямой доступ к интернет-ресурсам, а не через эту сеть. При включении этого параметра политики доступ к Интернету для компьютера пользователя осуществляется через сеть организации.

Очевидно, что каждый из этих подходов имеет свои достоинства и недостатки. Когда интернет-трафик не маршрутизируется через сеть организации, это снижает нагрузку и уровень трафика на интернет-подключение организации, но при этом теряется дополнительная безопасность и защита, которые могут предоставляться для защиты интрасети. Маршрутизация же интернет-трафика через внутреннюю сеть организации повышает нагрузку и уровень трафика на интернет-подключение организации и, возможно, способно существенно повысить задержку и время отклика при обращении к интернет-ресурсам. Но этот подход обеспечивает применение дополнительных мер безопасности и защиты, которые могут предоставляться для защиты интрасети организации.

[1] Network Access Protection — защита доступа к сети.

Создание подключений для удаленного доступа

Как рассматривалось ранее, для удаленного доступа к сети организации можно использовать как коммутируемые, так и широкополосные подключения. При необходимости обеспечить дополнительную безопасность по этим подключениям можно также установить виртуальную частную сеть. После установки этой функциональности работа DirectAccess прозрачна для пользователя, которому для доступа к сети организации требуется только установить подключение к Интернету.

Для создания этих подключений Windows 8 предоставляет специальный мастер. В большинстве случаев доступ к этому мастеру удобно получить через Центр управления сетями и общим доступом, щелкнув в нем по ссылке **Настройка нового подключения или сети** (Set up a new connection or network). В открывшемся диалоговом окне **Настройка подключения или сети** можно затем создать коммутируемое, широкополосное или VPN-подключение.

Практический совет

Рассмотрите возможность использования групповой политики для снижения уровня нагрузки. Если одни и те же параметры подключения планируется использовать на нескольких компьютерах, коммутируемое или VPN-подключение можно создать, используя предпочтения объекта групповой политики. Кроме этого, параметры в групповую политику можно также импортировать. В любом случае, созданные подключения будут доступны всем компьютерам, на которые распространяется объект групповой политики. Этот метод можно использовать для развертывания новых конфигураций подключений, обновления существующих, а также для удаления существующих подключений и замены их новыми.

Создание коммутируемого подключения

Операционная система Windows 8 предоставляет два способа создания коммутируемого подключения. В частности, можно создать коммутируемое подключение к поставщику услуг Интернета или к сети организации. Хотя эти подключения создаются разными методами, настройки параметров обоих подключений одинаковые, со следующими исключениями.

- Коммутируемое подключение к поставщику услуг Интернета не использует компонент **Клиент для сетей Microsoft** (Client for Microsoft networks) и по умолчанию выполняет повторный дозвон при обрыве связи.
- Коммутируемое подключение к сети организации использует компонент **Клиент для сетей Microsoft** и не выполняет повторный дозвон при обрыве связи. Сетевой компонент **Клиент для сетей Microsoft** позволяет системам под Windows 8 взаимодействовать в доменах и рабочих группах Windows. Так как большинство сетей организаций использует домены или рабочие группы Windows, в то время как некоторые поставщики услуг Интернета не используют эти сетевые конфигурации, данный компонент настраивается для среды внутренних сетей организаций, а не для поставщиков Интернета.

Создание коммутируемого подключения является двухэтапным процессом. Прежде чем приступать к созданию коммутируемого подключения, нужно настроить параметры телефона и модема, которые задают правила набора номера. После настройки правил набора номера можно приступать к созданию коммутируемого подключения.

Работа с правилами набора номера и размещениями

Правила набора номера используются с модемами, чтобы можно было задать способ доступа к телефонной линии, междугородний код, расположение, откуда выполняется звонок, а

также дополнительные возможности, которые следует использовать при наборе по подключениям. Комплекты правил набора номера сохраняются в виде расположений вызовов в инструменте **Телефон и модем**.

Просмотр и установка расположения вызова по умолчанию

Просмотр и установка расположения вызова по умолчанию выполняется следующим образом:

1. В правом верхнем углу Панели управления выберите в списке **Просмотр** опцию **Крупные значки** или **Мелкие значки**.
2. Далее щелкните по ссылке **Телефон и модем**. При первом использовании этого инструмента открывается диалоговое окно **Сведения о расположении** (Location Information) (рис. 16.6).

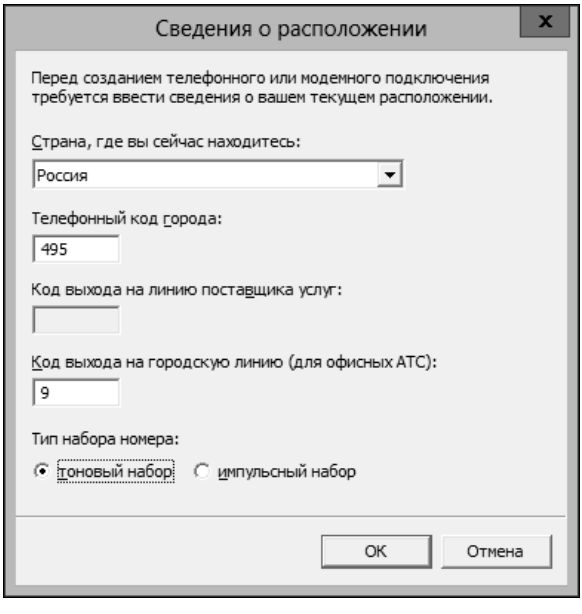


Рис. 16.6. При первом использовании инструмента **Телефон и модем** нужно настроить текущее расположение

3. Предоставьте следующую информацию для настройки расположения по умолчанию, которое называется **Мое расположение** (My location).
   - **Страна, где вы сейчас находитесь** (What country/region are you in now?). Выберите в раскрывающемся списке страну или регион, в котором вы сейчас находитесь, например Россия.
   - **Телефонный код города** (What area code (or city code) are you in now?). Введите телефонный код города, в котором вы сейчас находитесь, например 495.
   - **Код выхода на линию поставщика услуг** (If you need to specify a carrier code, what is it?). Чтобы указать конкретного поставщика услуг телефонной связи при наборе номера и установке подключения, введите его код. Код поставщика телефонных услуг может быть необходим при междугородних или международных звонках.
   - **Код выхода на городскую линию (для офисных АТС)** (If you dial a number to access an outside line, what is it?). Введите код для выхода на городскую линию. Этот код

может быть необходимым для доступа к городской линии при наборе номера через офисную или гостиничную АТС.

4. В разделе **Тип набора номера** (Phone system at this location uses) выберите тоновый или импульсный набор номера, установив соответствующий переключатель. В настоящее время импульсный набор повсеместно вытесняется тоновым.
5. Выполнив настройки исходного расположения, нажмите кнопку **OK**, в результате чего откроется диалоговое окно **Телефон и модем** (рис. 16.7).

   После этого выполнять настройку исходного расположения больше не потребуется.

   В списке **Расположение** этого окна отображаются расположения, настроенные для данного компьютера, упорядоченные по имени и коду города. Имя текущего используемого расположения отображается жирным шрифтом.
6. Вначале расположением по умолчанию выбрано расположение **Мое расположение**. Выбрав другое расположение, его можно сделать текущим расположением (т. е. расположением по умолчанию). Расположение по умолчанию **Мое расположение** рекомендуется переименовать, чтобы имя отображало город или расположение офиса. Чтобы просмотреть конфигурацию выбранного расположения, нажмите кнопку **Изменить**. Чтобы переименовать расположение, введите новое имя в текстовое поле **Имя расположения** (Location name). Завершив редактирование расположения, нажмите кнопку **OK**, чтобы сохранить изменения и закрыть окно.

Примечание

Изо всех правил набора номера наиболее часто приходится работать с кодом города. При установке операционной системы может создаться размещение по умолчанию с кодом города, указанным лицом, которое выполняло установку. Во многих случаях код города по умолчанию не подходит пользователю для набора номера со своего дома.

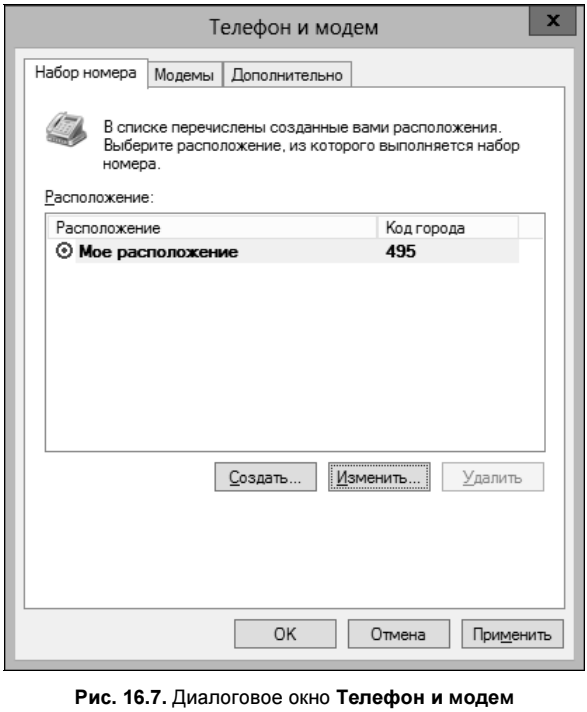


Рис. 16.7. Диалоговое окно **Телефон и модем**

Создание расположений вызова

Расположения вызова можно использовать для создания определенных правил для каждого кода города, с которого пользователь выполняет коммутируемые подключения. Для создания расположения вызова используется следующая процедура:

1. В правом верхнем углу Панели управления выберите в списке **Просмотр** опцию **Крупные значки** или **Мелкие значки**, а затем щелкните по ссылке **Телефон и модем**.
2. На вкладке **Набор номера** (Dialing Rules) открывшегося диалогового окна **Телефон и модем** нажмите кнопку **Создать**. Откроется диалоговое окно **Новое расположение** (New Location).
3. Это диалоговое окно имеет следующие три вкладки.
   - **Общие** (General). Предназначена для установки имени расположения, страны или региона и кода города. На этой вкладке также можно задать номера для доступа к внешней местной или междугородной линии, отключить ожидание звонка, а также указать тоновый или импульсный набор номера. Рекомендуется использовать значимое имя расположения, например, название города или области, с которой пользователь делает вызов.
   - **Код города** (Area Code Rules). На этой вкладке задаются правила, определяющие набор номеров из города расположения в города или области с другими кодами и в пределах области кода города, в котором находится пользователь. Эти правила полезны в тех случаях, когда одно расположение содержит несколько кодов городов, звонки в которые из данного расположения не являются междугородними. Также они полезны в тех случаях, когда в зависимости от префикса номера телефона, звонок в пределах одного кода города может быть локальным или междугородним.
   - **Телефонная карточка** (Calling Card). Предназначена для указания телефонной карточки, которую следует использовать при звонках с данного расположения. Содержит список телефонных карточек основных поставщиков телефонных услуг (США), а также предоставляет возможность создавать свои записи телефонных карточек.
4. Завершив создание расположения и закрыв окно **Новое расположение**, проверьте правильность установки расположения по умолчанию в окне **Телефон и модем**. Если необходимо, установите требуемое расположение по умолчанию. Нажмите кнопку **OK**, чтобы сохранить настройки и закрыть окно.

Удаление расположений вызова

Для удаления расположения вызова используется следующая процедура:

1. В правом верхнем углу Панели управления выберите в списке **Просмотр** опцию **Крупные значки** или **Мелкие значки**, а затем щелкните по ссылке **Телефон и модем**.
2. В открывшемся диалоговом окне **Телефон и модем** выберите расположение, которое требуется безвозвратно удалить, и нажмите кнопку **Удалить**. При выводе запроса подтвердить удаление выбранного расположения нажмите кнопку **Да**.
3. Выберите расположение, которое требуется установить в качестве расположения по умолчанию, и нажмите кнопку **OK**.

Создание коммутируемого подключения к поставщику Интернета

Коммутируемые подключения можно создавать следующими способами.

- Если пользователь совершает вызов через поставщика услуг Интернета, который обладает точками входа в Интернет по всей России и миру, то желательно настроить правила

набора номера и подключения для определенных расположений. Например, можно создать расположение для коммутируемого подключения под названием `Тула` и коммутируемое подключение под названием `Подключение к ISP в Туле`. В этой конфигурации указывается код города для Тулы, а также все особые правила набора номера, после чего подключение настраивается на использование номеров доступа для Тулы. Также потребуется показать пользователям, как изменять их текущие расположения на другие, когда они перемещаются из одного города в другой.

- Для звонков по бесплатному номеру 800 в модемный пул организации или междугородних звонков по специальному номеру доступа поставщика Интернета для абонентов, находящихся вне зоны действия кода города его расположения, желательно настроить отдельные подключения, а не отдельные расположения. В этой ситуации создается междугородное подключение и локальное подключение. Тогда потребуется только одно расположение вызова.

Коммутируемое интернет-подключение создается следующим образом:

1. Прежде чем создавать коммутируемое подключение, следует проверить текущую настройку параметров телефона и модема *(см. разд. "Работа с правилами набора номера и размещениями" ранее в этой главе).*

> ***Примечание***
>
> Если с подключением применить правила набора номера, а затем установить коды города и страны, такое подключение может быть использовано для междугородних или международных звонков, что иногда может оказаться очень дорогим удовольствием. Если в действительности вы не хотите иметь такую конфигурацию, следует рассмотреть использование других параметров.

2. В Центре управления сетями и общим доступом щелкните по ссылке **Настройка нового подключения или сети**. Будет запущен мастер **Настройка подключения или сети**.
3. Выберите опцию **Подключение к Интернету** (Connect to the Internet) и нажмите кнопку **Далее**. Если компьютер уже подключен к Интернету, щелкните в следующем окне по ссылке **Все равно создать новое подключение** (Set up a new connection anyway). Если уже существует коммутируемое подключение, можно его переконфигурировать или же создать новое подключение. Желательно создать новое подключение, поэтому установите переключатель **Нет, создать новое подключение** (No, create a new connection) и нажмите кнопку **Далее**.
4. На следующей странице мастера, **Как выполнить подключение** (How do you want to connect), щелкните на опции **Коммутируемое** (Dial-up). Далее введите в соответствующие текстовые поля номер телефона для подключения.
5. Введите имя пользователя и пароль. Хотя можно указать, что следует запомнить пароль для этого подключения, установив соответствующий флажок, это не безопасно, т. к. позволит использовать это подключение любому лицу, имеющему доступ к компьютеру.
6. Присвойте подключению соответствующее имя, желательно описательное, например, `Поставщик Интернета`. Имейте в виду, что длина имени не должна превышать 50 символов.
7. Если подключение требуется сделать доступным для всех пользователей компьютера, установите флажок **Разрешить использовать это подключение другим пользователям** (Allow other people to use this connection). Эта опция полезна, когда планируется использовать подключение, для которого не предоставлены исходные учетные данные, посредством групповой политики.
8. Завершив ввод требуемой информации, нажмите кнопку **Подключить**, чтобы создать подключение и начать установку связи. Далее, если в данный момент подключаться

к поставщику не требуется, нажмите кнопку **Пропустить** (Skip), а затем **Закрыть**. Чтобы проверить параметры подключения, следуйте инструкциям, изложенным в *разд. "Установка подключений" далее в этой главе*.

Практический совет

Большинство организаций использует цифровые телефонные системы, которые не допускают аналоговые подключения к внешней линии. В таком случае для проверки подключения необходимо получить доступ к аналоговой линии. Некоторые цифровые телефоны могут быть оснащены цифроаналоговыми преобразователями, которые можно использовать для проверки коммутируемого подключения. Эти преобразователи могут использоваться с телефонами конференц-связи или факсами, или же эти устройства могут быть уже подключены к аналоговым телефонным линиям.

Создание коммутируемого подключения к сети организации

Создание коммутируемого подключения к сети организации подобно созданию коммутируемого подключения к поставщику Интернета. Процедура для этого следующая:

1. В Центре управления сетями и общим доступом щелкните по ссылке **Настройка нового подключения или сети**. Будет запущен мастер **Настройка подключения или сети**.
2. Выберите опцию **Подключение к рабочему месту** (Connect to a workplace) и нажмите кнопку **Далее**. Если уже существует коммутируемое подключение, можно его переконфигурировать или же создать новое подключение. Желательно создать новое подключение, поэтому установите переключатель **Нет, создать новое подключение** и нажмите кнопку **Далее**.
3. На следующей странице мастера, **Как выполнить подключение**, щелкните на опции **Использовать прямой набор номера** (Dial directly).
4. Далее введите в соответствующие текстовые поля номер телефона для подключения и описательное имя подключения, например, `Главный офис` или `Офис в Туле`. Имейте в виду, что длина имени не должна превышать 50 символов.
5. Если для подключения будет использоваться смарт-карта, установите соответствующий флажок.
6. Если подключение требуется сделать доступным для всех пользователей компьютера, установите флажок **Разрешить использовать это подключение другим пользователям**. Эта опция полезна, когда планируется использовать подключение, для которого не предоставлены исходные учетные данные, посредством групповой политики.
7. Если подключение не требуется проверять на данном этапе, установите флажок **Не подключаться сейчас** (Don't connect now). В большинстве случаев желательно применить эту опцию, чтобы пропустить активирование подключения. В противном случае установка связи может быть неудачной, т. к. подключение создается для альтернативного размещения, например домашнего подключения пользователя к Интернету, чьи параметры могут не соответствовать требованиям для установки связи через сеть организации.
8. Нажмите кнопку **Далее** и на следующей странице введите имя пользователя и пароль в соответствующие поля.

Внимание!

Хотя можно указать, что следует запомнить пароль для этого подключения, установив соответствующий флажок, это будет не безопасно, т. к. позволит использовать это подключение любому лицу, имеющему доступ к компьютеру.

9. Если подключение создается для домена, можно указать домен входа в соответствующем текстовом поле.
10. Если на предыдущей странице был установлен флажок не устанавливать связь, нажмите кнопку **Создать**, чтобы создать подключение. В противном случае нажмите кнопку **Подключиться**, чтобы создать подключение и установить связь. Нажмите кнопку **Закрыть**.

Коммутируемые подключения можно создавать, редактировать и удалять посредством предпочтений групповой политики. Настроить параметры сетевых предпочтений групповой политики можно таким способом:

1. В редакторе управления групповыми политиками откройте для редактирования требуемый объект групповой политики. Для настройки предпочтений для компьютеров разверните узел **Конфигурация компьютера\Настройка\Параметры панели управления** и выберите в нем подузел **Сетевые параметры** (Network Options). Для настройки параметров пользователя разверните узел **Конфигурация пользователя\Настройка\ Параметры панели управления** и выберите в нем подузел **Сетевые параметры**.
2. Щелкните на этом узле правой кнопкой мыши, в контекстном меню выберите команду **Создать**, а во вложенном меню — команду **Коммутируемое подключение** (Dial-up connection). Откроется диалоговое окно **Новые свойства подключения удаленного доступа** (Network Options Properties).
3. В списке **Действие** выберите требуемую опцию: **Создать**, **Обновить** или **Заменить**.
4. Если подключение требуется сделать доступным для всех пользователей компьютера, установите переключатель **Подключения всех пользователей** (Allow user connection). В противном случае установите переключатель **Подключение пользователя** (User connection), чтобы применить подключение только для пользователя, для которого обрабатывается политика.
5. Введите имя и номер телефона подключения в соответствующие поля.
6. Для управления способом применения настройки предназначены опции на вкладке **Общие параметры**. Часто политику требуется применять только один раз. В таких случаях устанавливается флажок **Применить один раз и не применять повторно**.
7. Нажмите кнопку **OK**. При следующем обновлении групповой политики элемент настройки будет применен должным образом к объекту групповой политики, для которого он был определен.

Создание широкополосного подключения к Интернету

Настройка широкополосных подключений во многих отношениях легче, чем настройка коммутируемых подключений, т. к. для них не требуется указывать правила набора номера или расположения. Также нет надобности беспокоиться о телефонных карточках, номерах дозвона к поставщику Интернета или параметрах повторного вызова. Все это делает работу с широкополосными подключениями намного легче.

Для подключения к сети поставщика большинство поставщиков широкополосного Интернета снабжают пользователя DSL-маршрутизатором или кабельным модемом. Кроме этого, компьютер пользователя должен быть оснащен сетевым адаптером, который подключается к DSL-маршрутизатору или кабельному модему. При такой конфигурации подключение устанавливается по локальной сети, а не по какому-либо широкополосному подключению. Поэтому для получения доступа к Интернету нужно правильно настроить сетевое подключение, а создавать широкополосное подключение не требуется.

Но при необходимости можно создать специальное широкополосное соединение. В некоторых случаях это требуется для того, чтобы установить специальные настройки параметров, например, безопасную проверку подлинности, требуемую поставщиком Интернета. Этот подход также может использоваться для установки имени пользователя и пароля, запрашиваемых поставщиком Интернета.

Широкополосное подключение к Интернету создается следующим образом:

1. В Центре управления сетями и общим доступом щелкните по ссылке **Настройка нового подключения или сети**. Будет запущен мастер **Настройка подключения или сети**.
2. Выберите опцию **Подключение к Интернету** и нажмите кнопку **Далее**. Если компьютер уже подключен к Интернету, щелкните в следующем окне по ссылке **Все равно создать новое подключение**. Если уже существует другое рабочее подключение, можно его переконфигурировать или же создать новое подключение. Обычно желательно создать новое подключение, поэтому установите переключатель **Все равно создать новое подключение** и нажмите кнопку **Далее**. В следующем окне установите переключатель **Нет, создать новое подключение**, а затем нажмите кнопку **Далее**.
3. В следующем окне, **Как выполнить подключение**, щелкните на опции **Высокоскоростное** (Broadband).
4. Выполните следующие действия, а затем нажмите кнопку **Далее**.
   - В очередном окне введите в соответствующие поля имя пользователя и пароль.

     Внимание!

     Хотя можно указать, что следует запомнить пароль для этого подключения, установив соответствующий флажок, это не безопасно, т. к. позволит использовать данное подключение любому лицу, имеющему доступ к компьютеру.

   - В поле **Имя подключения** введите описательное название подключения, например `Безопасное широкополосное в офис в Туле`. Имейте в виду, что длина имени не должна превышать 50 символов.
   - Если подключение требуется сделать доступным для всех пользователей компьютера, установите флажок **Разрешить использовать это подключение другим пользователям**. Эта опция полезна, когда планируется использовать подключение, для которого не предоставлены исходные учетные данные, посредством групповой политики.
5. Нажмите кнопку **Подключиться**, чтобы создать подключение и установить связь. В большинстве случаев установка связи будет неудачной, т. к. подключение создается для альтернативного размещения, например домашнего подключения пользователя к Интернету, и эти параметры могут не соответствовать требованиям для установки связи через сеть организации. В таком случае нажмите кнопку **Пропустить**, чтобы не активировать подключение на данном этапе. Нажмите кнопку **Закрыть**.

   Совет

   Для проверки широкополосного подключения требуется наличие DSL-маршрутизатора или кабельного модема. Кроме этого, необходимо настроить параметры сетевого адаптера значениями, требуемыми поставщиком Интернета *(см. в разд. "Настройка свойств подключения" далее в этой главе)*.

Создание VPN-подключения

VPN-подключения используются для установки безопасных каналов связи по коммутируемым или широкополосным подключениям. Для подключения к серверу удаленного доступа

необходимо знать его IP-адрес или полное доменное имя. Если имеется необходимое коммутируемое или широкополосное подключение и адрес или имя хоста, VPN-подключение можно создать следующим образом:

1. В Центре управления сетями и общим доступом щелкните по ссылке **Настройка нового подключения или сети**. Будет запущен мастер **Настройка подключения или сети**.
2. Чтобы создать VPN-подключение, выберите опцию **Подключение к рабочему месту**, а затем нажмите кнопку **Далее**.
3. Если уже существует коммутируемое подключение, установите переключатель **Нет, создать новое подключение**, а затем нажмите кнопку **Далее**.
4. На следующей странице, **Как выполнить подключение**, выберите опцию **Использовать мое подключение к Интернету (VPN)** (Use my Internet connection (VPN)).
5. Прежде чем использовать VPN-подключение, пользователю нужно будет установить подключение к Интернету через коммутируемое или широкополосное подключение. Выберите существующее подключение, а затем нажмите кнопку **Далее**.
6. На следующей странице мастера, **Введите адрес в Интернете**, введите в соответствующее поле IPv4- или IPv6-адрес или полное доменное имя компьютера, к которому выполняется подключение, например 157.54.0.1 или **external.microsoft.com**. В большинстве случаев это будет адрес сервера удаленного доступа, настроенного для сети организации.
7. В поле **Имя объекта назначения** (Destination name) введите имя для подключения. Если компьютер настроен на использование смарт-карты для проверки подлинности, установите флажок **Использовать смарт-карту** (Use a smart card).
8. Если подключение требуется сделать доступным для всех пользователей компьютера, установите флажок **Разрешить использовать это подключение другим пользователям**. Эта опция полезна, когда планируется использовать подключение, для которого не предоставлены исходные учетные данные, посредством групповой политики.

> ***Внимание!***
>
> Хотя можно указать, что следует запомнить учетные данные для этого подключения, установив соответствующий флажок, это не безопасно, т. к. позволит использовать данное подключение любому лицу, имеющему доступ к компьютеру. Если этот флажок не установлен, пользователь увидит окно с запросом ввести требуемые учетные данные.

9. Нажмите кнопку **Создать**.

VPN-подключения можно создавать, редактировать и удалять посредством предпочтений групповой политики. Настроить параметры сетевых предпочтений групповой политики можно таким способом:

1. В редакторе управления групповыми политиками откройте для редактирования требуемый объект групповой политики. Для настройки предпочтений для компьютеров разверните узел **Конфигурация компьютера\Настройка\Параметры панели управления** и выберите в нем подузел **Сетевые параметры**. Для настройки параметров для пользователей разверните узел **Конфигурация пользователя\Настройка\Параметры панели управления** и выберите в нем подузел **Сетевые параметры**.
2. Щелкните на этом узле правой кнопкой мыши, в контекстном меню выберите команду **Создать**, а во вложенном меню — команду **VPN-подключение** (VPN Connection). Откроется диалоговое окно **Новые свойства VPN** (New VPN Properties).

3. В списке **Действие** выберите требуемую опцию: **Создать**, **Обновить** или **Заменить**.
4. Если подключение нужно сделать доступным для всех пользователей компьютера, установите переключатель **Подключения всех пользователей**. В противном случае установите переключатель **Подключение пользователя**, чтобы применить подключение только для пользователя, для которого обрабатывается политика.
5. Введите имя и IP-адрес подключения. Либо установите флажок **Использовать DNS имя** (Use DNS name), а затем введите требуемое полное доменное имя.
6. На вкладке **Безопасность** установите переключатель **Дополнительные** (Advanced) и в списке **Шифрование данных** выберите метод шифрования данных. В большинстве случаев желательно использовать шифрование. В разделе **Безопасный вход** (Logon security) укажите требуемые параметры безопасности.
7. Для управления способом применения настройки служат опции на вкладке **Общие параметры**. Как правило, политику требуется применять только один раз. В таких случаях устанавливается флажок **Применить один раз и не применять повторно**.
8. Нажмите кнопку **OK**. При следующем обновлении групповой политики элемент настройки будет применен должным образом к объекту групповой политики, для которого он был определен.

Настройка свойств подключений

При работе с коммутируемыми, широкополосными или VPN-подключениями часто требуется задать дополнительные свойства подключения после его создания. В этом разделе мы рассмотрим ключевые свойства подключений, которые можно настраивать.

Примечание

При работе со свойствами подключения следует иметь в виду, что VPN-подключения используют существующие интернет-подключения (коммутируемые или широкополосные) и каждый тип подключения настраивается отдельно. Для VPN-подключения сначала устанавливается основное подключение с помощью параметров этого подключения, после чего предпринимается попытка установления VPN-подключения посредством его параметров. Имея это в виду, следует сначала настроить основное подключение, а затем настраивать параметры VPN-подключения. Этот подход нужно изменить только при диагностировании проблем с VPN-подключением. В таком случае следует начинать с VPN-конфигурации и двигаться по направлению к параметрам основного подключения.

Настройка автоматических и ручных подключений

Операционную систему Windows 8 можно настроить на автоматическое установление коммутируемого, широкополосного или VPN-подключения, когда пользователь обращается к программе, которой требуется доступ к Интернету, например веб-браузеру. Способ работы автоматических подключений зависит от параметров, установленных в диалоговом окне **Свойства: Интернет**. Для коммутируемых подключений доступны следующие опции:

- **Никогда не использовать коммутируемые подключения** (Never dial a connection) — пользователи должны устанавливать подключение вручную;
- **Использовать при отсутствии подключения к сети** (Dial whenever a network connection is not present) — подключение устанавливается автоматически, когда требуется, но лишь в случаях неработающего сетевого подключения;

- **Всегда использовать принятое по умолчанию подключение** (Always dial my default connection) — подключение по умолчанию всегда создается, когда требуется подключение к Интернету (даже если другие подключения уже созданы).

> ***Совет***
>
> Выбор опции автоматического подключения зависит от особенностей работы организации. У администраторов бытует ошибочное мнение, что пользователям мобильных устройств удобнее работать, когда среди их настроенных подключений нет коммутируемого подключения. У пользователя может отсутствовать доступ к телефонной линии, когда он находится за пределами офиса, и попытка компьютера набрать номер для установления подключения, когда пользователь, например, дает презентацию или проводит встречу с клиентами, может вызвать определенные неудобства или даже проблемы. С другой стороны, пользователи настольных компьютеров в главном офисе или филиале, скорее всего, захотят использовать автоматические подключения.

Настройка ручного подключения выполняется следующим образом:

1. В Панели управления щелкните по ссылке **Сеть и Интернет** и в открывшемся одноименном окне щелкните по ссылке **Свойства обозревателя** (Internet Options). В диалоговом окне **Свойства: Интернет** (Internet Properties) перейдите на вкладку **Подключения** (рис. 16.8).
2. Установите переключатель **Никогда не использовать коммутируемые подключения** (Never dial a connection) и нажмите кнопку **OK**.

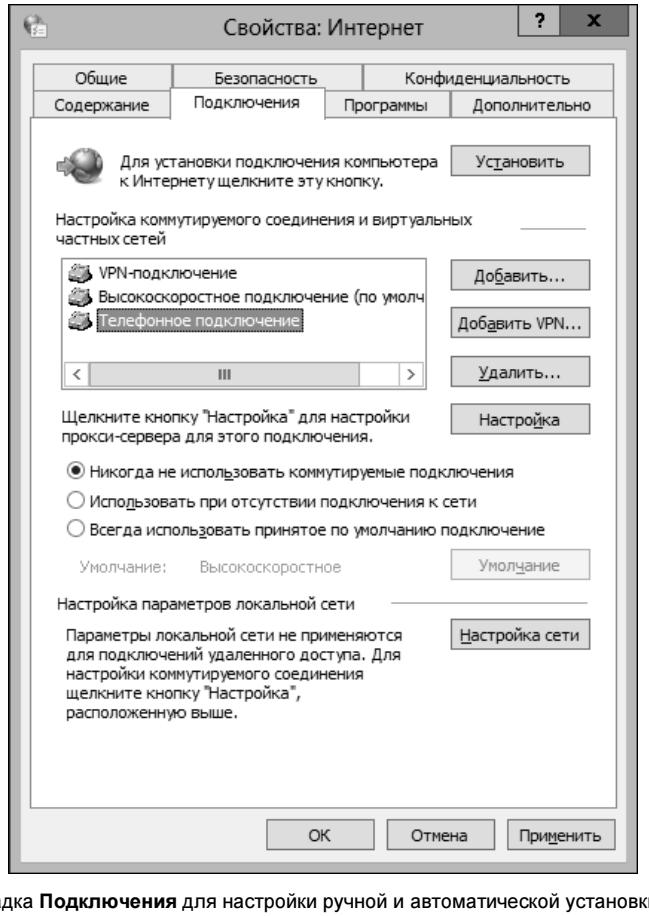


Рис. 16.8. Вкладка **Подключения** для настройки ручной и автоматической установки подключения

Настройка автоматической установки подключения выполняется следующим образом:

1. В Панели управления щелкните по ссылке **Сеть и Интернет** и в открывшемся одноименном окне щелкните по ссылке **Свойства обозревателя**. В диалоговом окне **Свойства: Интернет** перейдите на вкладку **Подключения** (см. рис. 16.8).
2. Установите переключатель **Использовать при отсутствии подключения к сети**, чтобы автоматически устанавливать подключение при отсутствии сетевого подключения, или переключатель **Всегда использовать принятое по умолчанию подключение**, чтобы всегда пытаться установить подключение.
3. Поле **Настройка коммутируемого подключения и виртуальных частных сетей** (Dial-up and virtual private network settings) содержит список коммутируемых, широкополосных и VPN-подключений, настроенных на компьютере в данный момент. Выберите в этом списке подключение, которое требуется использовать по умолчанию для установления подключения, а затем нажмите кнопку **Умолчание** (Set default).
4. Нажмите кнопку **OK**, чтобы сохранить настройки и закрыть окно.

Настройка параметров прокси-сервера для мобильных подключений

Как и в случае с самими подключениями, параметры прокси-сервера можно устанавливать вручную или автоматически. При ручной установке необходимо пошагово настроить каждое свойство. При автоматической настройке компьютер пытается определить параметры прокси-сервера, а затем настроить соответствующие параметры подключения; или же компьютер считывает конфигурационный сценарий, который используется для настройки прокси-сервера.

> ***Примечание***
>
> Посредством групповой политики параметры прокси-сервера можно настроить для множественных систем. Если групповая политика не используется для настройки параметров прокси-сервера, их можно настроить для каждого отдельного подключения, как рассматривается в этом разделе.

Файлы конфигурационных сценариев можно хранить на локальном компьютере или в Интернете. Использование конфигурационных сценариев может сэкономить значительное время, особенно если учитывать то обстоятельство, что все созданные подключения настраиваются по отдельности. Кроме этого, так как VPN-подключения устанавливаются поверх существующих интернет-подключений, параметры прокси-серверов для них могут быть другими, чем для используемых ими интернет-подключений.

Задать автоматическую настройку параметров прокси-сервера для подключения можно следующим образом:

1. В Панели управления щелкните по ссылке **Сеть и Интернет** и в открывшемся одноименном окне щелкните по ссылке **Свойства обозревателя**. В диалоговом окне **Свойства: Интернет** перейдите на вкладку **Подключения** (см. рис. 16.8).
2. В списке **Настройка коммутируемого соединения и виртуальных частных сетей** выберите коммутируемое подключение, которое требуется настроить, и нажмите кнопку **Настройка** (Settings). Откроется диалоговое окно **Телефонное подключение — параметры** (Dial-up Connection settings) (рис. 16.9).
3. Чтобы попытаться автоматически определить параметры прокси-сервера при установлении подключения, отметьте флажок **Автоматическое определение параметров** (Automatically detect settings).

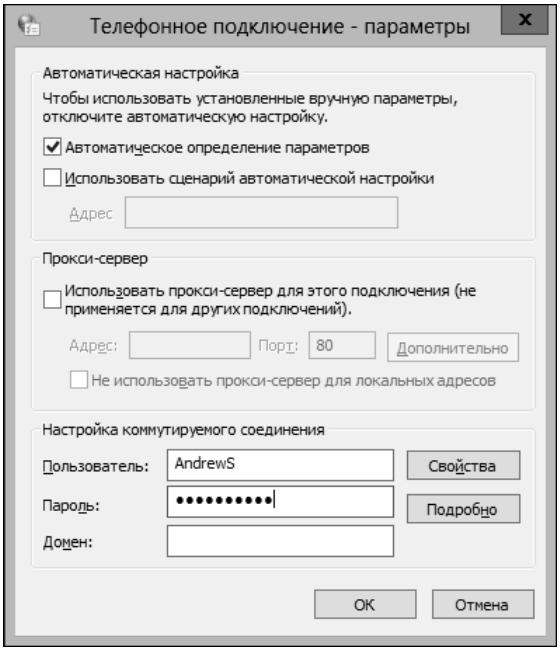


Рис. 16.9. Диалоговое окно для настройки параметров прокси-сервера подключения

4. Чтобы использовать конфигурационный сценарий, установите флажок **Использовать сценарий автоматической настройки** (Use automatic configuration script) и введите путь или URL к файлу сценария. При указании пути к файлу можно использовать переменные среды, например, `%UserProfile%\PROXY.VBS`. При использовании URL файла следует задать URL компьютера, например, **http://proxy.microsoft.com/proxy.vbs**.
5. Чтобы обеспечить использование только автоматических параметров, снимите флажок **Использовать прокси-сервер для этого подключения** (Use a proxy server for this connection).
6. Последовательно нажмите кнопку **OK**, чтобы закрыть все окна.

Настроить параметры прокси-сервера для подключения вручную можно следующим образом:

1. В Панели управления щелкните по ссылке **Сеть и Интернет** и в открывшемся одноименном окне щелкните по ссылке **Свойства обозревателя**. В диалоговом окне **Свойства: Интернет** перейдите на вкладку **Подключения** (см. рис. 16.8).
2. В списке **Настройка коммутируемого соединения и виртуальных частных сетей** выберите коммутируемое подключение, которое требуется настроить, и нажмите кнопку **Настройка**.
3. В открывшемся диалоговом окне **Телефонное подключение — параметры** (см. рис. 16.9) снимите флажки **Автоматическое определение параметров** и **Использовать сценарий автоматической настройки** (если они установлены) и установите флажок **Использовать прокси-сервер для этого подключения**.
4. По умолчанию флажок **Не использовать прокси-сервер для локальных адресов** (Bypass proxy server for local addresses) сброшен. Но в большинстве случаев нежелательно использовать прокси-сервер для запросов к серверам, находящимся в том же самом сегменте сети, что и запрашивающий компьютер, поэтому данный флажок следует уста-

новить. Важно отметить то обстоятельство, что если флажок **Не использовать прокси-сервер для локальных адресов** не установлен, пользователям могут потребоваться дополнительные полномочия для доступа к серверам внутренней сети организации через прокси-серверы.

5. Нажмите кнопку **Дополнительно** (Advanced), чтобы открыть диалоговое окно **Параметры прокси-сервера** (Proxy Settings) (рис. 16.10).

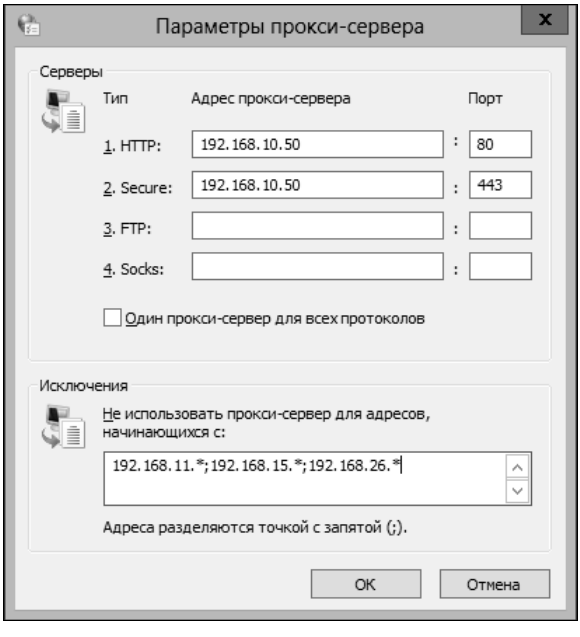


Рис. 16.10. Диалоговое окно для настройки параметров прокси-сервера

6. Введите адреса разных прокси-серверов разных типов в соответствующие поля в группе **Серверы**. Для каждого прокси-сервера необходимо предоставить два типа информации.
   - **Адрес прокси-сервера** (Proxy address to use). Определяет IP-адрес соответствующего прокси-сервера или серверов. Введите IP-адрес для каждого требуемого сервиса. Если для определенного сервиса настраивается несколько прокси-серверов, введите их в том порядке, в каком веб-клиенты должны пытаться использовать их. Адреса в списке разделяются точкой с запятой. Если для службы не требуется прокси-сервер, не заполняйте соответствующее текстовое поле.
   - **Порт** (Port). Задает номер порта, по которому прокси-сервер отвечает на запросы. Большинство прокси-серверов отвечает на все запросы по порту 80. Для протокола HTTP используется стандартный порт 80, для протокола SSL[1] (обозначен, как Secure) — порт 443, для протокола FTP — порт 21, а для протокола Socks — порт 1081. Для точного значения номеров портов обратитесь к своему веб-администратору.
7. Установка флажка **Один прокси-сервер для всех протоколов** (Use the same proxy server for all protocols) позволяет использовать один и тот же IP-адрес и порт для всех четырех протоколов.

[1] Secure Sockets Layer — протокол защищенных сокетов.

В данном отношении доступны следующие опции:

- если организация использует один прокси-сервер для обработки всех запросов, установите этот флажок и введите соответствующий IP-адрес и номер порта;
- если для каждого протокола используется отдельный прокси-сервер или серверы, снимите этот флажок и введите необходимые IP-адреса и номера портов в соответствующие текстовые поля.

8. Если сеть состоит из нескольких сегментов или имеются определенные серверы, которые не должны использовать прокси-серверы, введите соответствующие IP-адреса или диапазоны IP-адресов в поле **Исключения** (Exceptions). Адреса в списке разделяются точкой с запятой. Для указания любой цифры или группы цифр адреса можно использовать подстановочный знак звездочки (*). Например, 192.*.*.*, 192.168.*.* или 192.168.10*.
9. Завершив настройку параметров прокси-серверов, последовательно нажмите кнопку **OK** три раза, чтобы сохранить настройки и закрыть все окна.

Настройка учетных данных подключения

Каждое созданное подключение имеет свой отдельный набор учетных данных: имя пользователя, пароль и домен. Задать эти параметры для подключения можно следующим образом:

1. В Панели управления щелкните по ссылке **Сеть и Интернет** и в открывшемся одноименном окне щелкните по ссылке **Свойства обозревателя**. В диалоговом окне **Свойства: Интернет** перейдите на вкладку **Подключения**.
2. В списке **Настройка коммутируемого подключения и виртуальных частных сетей** выберите подключение, которое требуется настроить, и нажмите кнопку **Настройка**.
3. В открывшемся окне параметров подключения введите имя пользователя и пароль в соответствующие текстовые поля.
4. Если требуется имя домена, введите его в поле **Домен**.
5. Последовательно нажмите кнопку **OK** два раза, чтобы сохранить настройки и закрыть все окна.

Установкой требуемых учетных данных процесс настройки параметров подключения не завершается. Нужно еще установить параметры, указывающие, запрашивать ли при установке подключения ввод пользователем учетных данных и/или номера телефона. Кроме этого, если для установления подключения требуется предоставить сведения о домене, необходимо обеспечить передачу этих сведений вместе с другими параметрами учетных данных. По умолчанию имя домена не предоставляется.

Настройка этих дополнительных параметров подключения выполняется следующим образом:

1. В Панели управления щелкните по ссылке **Сеть и Интернет** и в открывшемся одноименном окне щелкните по ссылке **Свойства обозревателя**. В диалоговом окне **Свойства: Интернет** перейдите на вкладку **Подключения**.
2. В списке **Настройка коммутируемого подключения и виртуальных частных сетей** выберите подключение, которое требуется настроить, и нажмите кнопку **Настройка**.
3. В открывшемся диалоговом окне параметров подключения нажмите кнопку **Свойства**.

4. В окне свойств подключения перейдите на вкладку **Параметры**. Теперь можно настроить следующие параметры подключения:
   - отображение сообщений состояния в процессе подключения, установив флажок **Отображать ход подключения** (Display progress while connecting);
   - запрос ввода пользователями учетных данных подключения, установив флажок **Запрашивать имя, пароль, сертификат и т. д.** (Prompt for name and password, certificate, etc.);
   - включение домена входа, установив флажок **Включать домен входа в Windows** (Include Windows logon domain);
   - запрос номера телефона, установив флажок **Запрашивать номер телефона** (Prompt for phone number).
5. Завершив настройку дополнительных параметров подключения, последовательно нажмите кнопку **OK** три раза, чтобы сохранить настройки и закрыть все окна.

Настройка автоматического отключения

Для коммутируемых подключений можно указать, чтобы Windows 8 отключала телефонную линию при простаивании подключения в течение определенного периода времени или в ситуации, когда подключение больше не требуется. Настройка параметров автоматического отсоединения подключения выполняется следующим образом:

1. В Панели управления щелкните по ссылке **Сеть и Интернет** и в открывшемся одноименном окне щелкните по ссылке **Свойства обозревателя**. В диалоговом окне **Свойства: Интернет** перейдите на вкладку **Подключения**.
2. В списке **Настройка коммутируемого подключения и виртуальных частных сетей** выберите подключение, которое требуется настроить, и нажмите кнопку **Настройка**.
3. В открывшемся диалоговом окне параметров подключения нажмите кнопку **Свойства**. В окне свойств подключения перейдите на вкладку **Параметры**. Чтобы задать отключение после определенного периода неактивности подключения, установите длительность такого периода в раскрывающемся списке **Время простоя до отключения** (Idle time before hanging up). Доступны предопределенные значения **никогда**, **1 минута**, **5 минут**, **10 минут**, **20 минут** (значение по умолчанию), **30 минут**, **1 час**, **2 часа**, **4 часа**, **8 часов** и **24 часа**.
4. Нажмите кнопку **OK**, чтобы возвратиться в диалоговое окно параметров подключения. В этом окне нажмите кнопку **Подробно** (Advanced) в разделе **Настройка коммутируемого соединения** (Dial-up connection settings). В открывшемся диалоговом окне **Дополнительная настройка** для данного подключения установите флажок **Отсоединяться, когда не требуется подключение к Интернету** (Disconnect when connection may be no longer needed)
5. Завершив настройку отсоединения подключения, последовательно нажмите кнопку **OK** три раза, чтобы сохранить настройки и закрыть все окна.

> ***Совет***
>
> Если пользователи жалуются на отключения в процессе сеанса коммутируемого подключения, причиной таких отключений может быть настройка параметров автоматического отключения. Расспросите пользователей, как они работают в Интернете, а затем решите, следует ли изменить настройку этих параметров, чтобы они лучше отвечали требованиям пользователей. Но обычно простаивающее подключение следует все-таки отключать.

Настройка правил набора номера

Коммутируемые подключения можно настраивать с правилами набора номера или без них. Если для подключения не используются правила набора номера, всегда набирается только номер, присвоенный подключению. Когда подключению присваиваются правила набора номера, тип исходящего звонка — локальный или междугородний — определяется текущим расположением вызова.

Просмотреть или установить правила набора номера для коммутируемого подключения можно следующим образом:

1. В Панели управления щелкните по ссылке **Сеть и Интернет** и в открывшемся одноименном окне щелкните по ссылке **Свойства обозревателя**. В диалоговом окне **Свойства: Интернет** перейдите на вкладку **Подключения**.
2. В списке **Настройка коммутируемого подключения и виртуальных частных сетей** выберите коммутируемое подключение, которое требуется настроить, и нажмите кнопку **Настройка**.
3. В открывшемся диалоговом окне параметров коммутируемого подключения нажмите кнопку **Свойства**. Откроется диалоговое окно свойств коммутируемого подключения.
4. Чтобы обеспечить использование подключением нужных правил набора номера, на вкладке **Общие** установите флажок **Использовать правила набора номера** (Use dialing rules), а затем введите код города и выберите код страны или региона.
5. Если правила набора номера использовать не требуется, снимите соответствующий флажок.
6. Завершив настройку правил набора номера, последовательно нажмите кнопку **OK** три раза, чтобы сохранить настройки и закрыть все окна.

Настройка основного и альтернативного номеров телефона

Для коммутируемых подключений можно настроить два типа номера телефона: основной номер, который набирается по умолчанию при каждой попытке установки подключения, и альтернативные номера, которые набираются, когда по основному номеру нельзя дозвониться. Настройка телефонных номеров подключения выполняется следующим образом:

1. В Панели управления щелкните по ссылке **Сеть и Интернет** и в открывшемся одноименном окне щелкните по ссылке **Свойства обозревателя**. В диалоговом окне **Свойства: Интернет** перейдите на вкладку **Подключения**.
2. В списке **Настройка коммутируемого подключения и виртуальных частных сетей** выберите коммутируемое подключение, которое требуется настроить, и нажмите кнопку **Настройка**.
3. В открывшемся диалоговом окне параметров коммутируемого подключения нажмите кнопку **Свойства**. Откроется диалоговое окно свойств коммутируемого подключения.
4. Основной номер телефона задается в поле **Номер телефона**. Если необходимо, введите новый основной номер.
5. Для просмотра и/или настройки альтернативных номеров дозвона нажмите кнопку **Другие** (Alternates) справа от поля основного номера. Откроется диалоговое окно **Дополни-**

тельные номера телефонов (Alternate phone numbers). Настройка основного и альтернативных номеров дозвона для подключения выполняется следующим образом.

- Чтобы добавить номер телефона, нажмите кнопку **Добавить**, в результате чего откроется диалоговое окно **Добавить дополнительный номер телефона** (Add alternate phone number). В поле **Номер телефона** этого окна введите альтернативный номер телефона в требуемом формате. При желании группы цифр можно разделять дефисами, например — 555-1234. Если нужно использовать правила набора номера, установите соответствующий флажок, а затем введите код города и выберите код страны или региона. Нажмите кнопку **OK**.
- Чтобы изменить порядок набора номера в списке, выберите в нем требуемый номер телефона и с помощью кнопок-стрелок вверх/вниз, расположенных справа от списка, переместите номер в требуемую позицию. Первый номер в списке станет основным номером набора.
- Для редактирования номера телефона выберите требуемый номер в списке и нажмите кнопку **Изменить**. В открывшемся диалоговом окне **Изменение дополнительного номера телефона** (Edit alternate phone number) выполните требуемые изменения номера и нажмите кнопку **OK**.
- Чтобы удалить номер телефона, выберите требуемый номер в списке и нажмите кнопку **Удалить**.

6. Чтобы автоматически использовать альтернативные номера, установите флажок **При отказе, пытаться соединиться по следующему номеру** (If a number fails, try the next number). Также номер, успешно набранный после отказа предыдущего номера, можно переместить в начало списка, сделав его основным номером. Для этого нужно установить флажок **Переносить успешно набранный номер в начало списка** (Move successful number to top of the list).
7. Завершив настройку номеров телефона подключения, последовательно нажмите кнопку **OK** четыре раза, чтобы сохранить настройки и закрыть все окна.

Настройка проверки подлинности

Должная проверка подлинности является важным фактором в поддержании целостности сети организации. Когда пользователи подключаются к сети организации по коммутируемым подключениям, необходимо обеспечить безопасную проверку подлинности, если это вообще возможно. Но такую проверку нельзя обеспечить посредством настроек по умолчанию коммутируемого подключения. В случае большинства подключений, учетные данные пользователей могут передаваться по каналу связи открытым текстом. Если использование незашифрованных паролей не разрешается, то Windows 8 пытается передавать учетные данные для входа в систему, используя безопасный метод, например протокол MS-CHAPv2 или протокол CHAP[1]. Подключение также можно настроить на использование протокола EAP[2].

Для коммутируемых и широкополосных подключений можно использовать любую из этих опций, но для VPN-подключений можно использовать только безопасные методы. Когда требуется использовать защищенный пароль, подключение можно настроить на автомати-

[1] Challenge Handshake Authentication Protocol — протокол аутентификации по квотированию вызова.

[2] Extensible Authentication Protocol — расширяемый протокол аутентификации.

ческую передачу имени входа и пароля Windows (и домена, если существует), указанных в конфигурации подключения. Использовать автоматическую передачу учетных данных Windows обычно полезно в тех случаях, когда пользователи удаленно подключаются к сети организации и нужно выполнить проверку их подлинности в домене Windows. Для обоих методов защищенной проверки подлинности можно требовать шифрования данных и выполнять отключение, если шифрование не применяется. Шифрование данных используется автоматически с проверкой подлинности Windows как для защищенных паролей, так и для смарт-карт.

Настройка проверки подлинности выполняется следующим образом:

1. В Панели управления щелкните по ссылке **Сеть и Интернет** и в открывшемся одноименном окне щелкните по ссылке **Свойства обозревателя**. В диалоговом окне **Свойства: Интернет** перейдите на вкладку **Подключения**.
2. В списке **Настройка коммутируемого подключения и виртуальных частных сетей** выберите подключение, которое требуется настроить, и нажмите кнопку **Настройка**.
3. В открывшемся диалоговом окне параметров подключения нажмите кнопку **Свойства**.
4. В окне свойств подключения перейдите на вкладку **Безопасность**. Для VPN-подключений можно указать, что следует использовать определенный протокол или же определять протокол автоматически. Если требуется использовать защищенные пароли, можно также задать автоматический вход в систему и требовать шифрования данных. Обе опции полезны при входе в домен Windows. Но эти параметры должны поддерживаться; если они не поддерживаются, выполнение проверки подлинности пользователей будет невозможно и подключения не будут устанавливаться.

   При использовании смарт-карт также следует использовать шифрование данных, которое является необходимым для обеспечения целостности и безопасности данных, передаваемых между исходным компьютером и компьютером, выполняющим проверку подлинности. Если потребовать шифрование, но при этом подключение не защищено шифрованием, клиентский компьютер отключится.
5. Установите разрешенные протоколы проверки подлинности и нажмите кнопку **OK**, чтобы сохранить настройки.

Настройка сетевых протоколов и компонентов

Способ настройки сетевых протоколов и компонентов зависит от типа подключения. Как показано в табл. 16.1, для коммутируемых подключений в качестве протокола соединения можно использовать протокол PPP[1] или SLIP[2]. Для широкополосных подключений применяется протокол PPPoE[3]. Большинство VPN-подключений использует протокол PPTP или L2TP. Но для более новых реализаций VPN-подключений может использоваться протокол SSTP[4] или IKEv2[5]. По протоколу IKEv2 подключения при проверке подлинности могут использовать сертификаты компьютеров.

---

[1] Point-to-Point Protocol — протокол соединения "точка—точка".

[2] Serial Line Internet Protocol — межсетевой протокол для последовательного канала.

[3] Point-to-Point Protocol over Ethernet — протокол двухточечного соединения через Ethernet.

[4] Secure Sockets Tunneling Protocol — туннелирующий протокол защищенных сокетов.

[5] Internet Key Exchange — обмен ключами по Интернету.

Таблица 16.1. *Протоколы соединения, применяемые с определенными типами подключений*

Тип подключения	Протокол соединения	Описание
Коммутируемое	PPP	Используется для установки подключения к серверам Windows по коммутируемым каналам связи
Коммутируемое	SLIP	Используется для установки подключения к серверам UNIX по коммутируемым каналам связи; доступен при условии установки программного обеспечения сторонних разработчиков
Широкополосное	PPPoE	Используется для установки широкополосного соединения типа "точка—точка" по Ethernet
VPN	Автоматический выбор	Применяется для автоматического определения доступного VPN-протокола и установки виртуального канала связи с помощью этого протокола
VPN	PPTP VPN	Устанавливает протокол PPTP для VPN. Протокол PPTP является расширением протокола PPP
VPN	L2TP IPSec VPN	Устанавливает протокол L2TP для VPN. Протокол L2TP использует набор IPSec для повышения безопасности
VPN	IKEv2	Устанавливает протокол IKEv2 для VPN. Протокол IKEv2 использует режим туннелирования набора IPSec для повышения безопасности
VPN	SSTP	Устанавливает протокол SSTP для VPN. Протокол SSTP передает трафик PPP или L2TP через SSL-туннель
DirectAccess	IPv6 через IPSec	Используется для установки защищенного туннеля к сети организации через существующее подключение

В мобильных сетях используются три сетевых компонента: стек протоколов TCP/IP, общий доступ к файлам и принтерам для сетей Microsoft и клиент для сетей Microsoft. Как показано в табл. 16.2, настройка по умолчанию этих компонентов зависит от исходного подключения. Эти параметры можно настраивать под свои требования. Также, если необходимо, можно устанавливать дополнительные сетевые компоненты.

Таблица 16.2. *Конфигурация компонентов по умолчанию по типу подключения*

Компонент	Описание	Широкополосное	Стандартное коммутируемое	Выделенное коммутируемое	VPN
Протокол TCP/IP	Для сетевой связи требуются протоколы TCP/IPv4 и TCP/IPv6. По умолчанию с подключением используется протокол DHCP, если только он не отменен в параметрах свойств	Да	Да	Да	Да
Общий доступ к файлам и принтерам для сетей Microsoft	Разрешает общий доступ к файлам и принтерам через сетевое подключение; позволяет подключать общие принтеры и диски	Нет	Нет	Нет	Да

Таблица 16.2 *(окончание)*

Компонент	Описание	Широкополосное	Стандартное коммутируемое	Выделенное коммутируемое	VPN
Клиент для сетей Microsoft	Разрешает выполнять проверку подлинности Windows в доменах Windows; позволяет компьютеру играть роль клиента домена	Нет	Нет	Да	Да

Просмотреть и/или изменить сетевые параметры подключения можно следующим образом:

1. В Панели управления щелкните по ссылке **Сеть и Интернет** и в открывшемся одноименном окне щелкните по ссылке **Свойства обозревателя**. В диалоговом окне **Свойства: Интернет** перейдите на вкладку **Подключения**.
2. В списке **Настройка коммутируемого подключения и виртуальных частных сетей** выберите подключение, которое требуется настроить, и нажмите кнопку **Настройка**.
3. В открывшемся диалоговом окне параметров подключения нажмите кнопку **Свойства**.
4. В окне свойств подключения перейдите на вкладку **Сеть** (Networking). Здесь можно выполнять следующие настройки подключения:
   - включать сетевые компоненты, установив флажок требуемого компонента в списке **Компоненты, используемые этим подключением** (This connection uses the following items);
   - отключать сетевые компоненты, сняв флажок требуемого компонента в списке **Компоненты, используемые этим подключением**.

   Совет

   В случае отсутствия в списке **Компоненты, используемые этим подключением** какого-либо требуемого подключением сетевого компонента, указанного в табл. 16.2, его можно установить. Для этого на вкладке **Сеть** нажмите кнопку **Установить**, в открывшемся диалоговом окне **Выбор сетевых компонентов** выберите требуемый тип компонента и нажмите кнопку **Добавить**, а затем в следующем окне выберите необходимый компонент.
5. По умолчанию для настройки сетевых параметров, включая IP-адрес подключения, маску подсети и IP-адреса основного шлюза, DNS-сервера и WINS-сервера, используется служба DHCP. Если подключению требуется присвоить статический IP-адрес или заменить другие параметры по умолчанию, выберите в списке опцию **Протокол Интернета версии 4 (TCP/IPv4)** или **Протокол Интернета версии 6 (TCP/IPv6)**, а затем нажмите кнопку **Свойства**. Откроется диалоговое окно свойств выбранного протокола, в котором можно выполнять настройку его параметров, как рассматривается ранее в этой главе.
6. Завершив настройку сетевых компонентов и протоколов, последовательно нажмите кнопку **OK** три раза, чтобы сохранить настройки и закрыть все окна.

Включение и отключение брандмауэра Windows для сетевых соединений

При использовании коммутируемых, широкополосных и VPN-подключений желательно дополнительно защитить компьютер от атак, используя брандмауэр Windows. Этот встроенный в операционную систему брандмауэр защищает Windows 8, ограничивая типы передаваемой информации. Принудительно применяя соответствующие ограничения, можно

понизить вероятность проникновения в систему несанкционированных лиц. А снижение уровня угроз безопасности является очень важным фактором, когда пользователи осуществляют доступ к сети организации извне защитных брандмауэров и прокси-серверов.

Брандмауэр Windows по умолчанию включен для всех подключений; его также можно включить или отключить для каждого типа сети, к которой подключается пользователь. Процедура включения или отключения брандмауэра Windows следующая:

1. В Панели управления щелкните по ссылке категории **Система и безопасность**, а в открывшемся одноименном окне — по ссылке **Брандмауэр Windows**.
2. В левой панели следующей страницы щелкните по ссылке **Включение и отключение брандмауэра Windows** (Turn Windows firewall on or off).
3. Открывшаяся страница **Настройка параметров для каждого типа сети** (Customize Settings) содержит настраиваемые параметры брандмауэра Windows для каждого типа сети, к которой может подключаться пользователь. Включите или отключите брандмауэр Windows для каждого типа сети, установив соответствующий переключатель.
4. Завершив настройку брандмауэра Windows, нажмите кнопку **OK**, чтобы сохранить настройки и закрыть окно.

Установка подключений

Как отмечено в *разд. "Настройка автоматических и ручных подключений" ранее в этой главе*, коммутируемые, широкополосные и VPN-подключения можно устанавливать вручную или автоматически. Ручной способ предоставляет пользователям возможность выбора, когда устанавливать подключение. Автоматическое установление подключения осуществляется, когда пользователь запускает программу, для которой требуется доступ к сети (например, веб-браузер).

Установка коммутируемого подключения

Коммутируемое подключение использует телефонную линию для установки связи между двумя модемами. Процесс установки коммутируемого подключения следующий:

1. Откройте панель **Сеть**, щелкнув по значку **Сеть** в области уведомлений панели задач. На мобильных устройствах эту панель можно открыть, проведя пальцем от правого края экрана к центру, нажав опцию **Параметры**, а затем нажав значок **Сеть**.
2. В панели **Сеть** щелкните на требуемом подключении, а затем нажмите кнопку **Подключить**.
3. Удостоверьтесь в правильности имени пользователя. Если для подключения был предварительно задан и сохранен пароль, можно использовать этот кэшированный пароль без необходимости вводить его снова. В противном случае, введите пароль для подключения.
4. Чтобы не вводить повторно имя пользователя и пароль при следующих установлениях подключения, отметьте флажок **Сохранять имя пользователя и пароль** (Save this user name and password for the following users), а затем выберите **Только для текущего пользователя** (Me only).

Совет

Чтобы любой пользователь мог использовать данное имя и пароль при попытке установить подключение, отметьте флажок **Сохранять имя пользователя и пароль** (Save this user name and

password for the following users), а затем выберите **Для любого пользователя** (Anyone who uses this computer). Но не задавайте эту опцию, если планируется распределять данное подключение через групповую политику, т. к. не следует разглашать пароль подключения.

5. В раскрывающемся списке **Набор номера** отображаются телефонные номера, по которым можно осуществлять дозвон. По умолчанию в этом списке выбран основной номер. Чтобы делать вызов по другому номеру, выберите в списке необходимый номер.
6. Нажмите кнопку **Вызов**. Когда модем установит соединение с поставщиком Интернета или сетью организации, в состоянии подключения будет отображена скорость соединения. Скорость соединения может быть разной для каждой установки соединения и зависит от максимальной скорости вызывающего и отвечающего модемов, доступных алгоритмов сжатия и качества линии связи.

Просмотреть свойства подключения можно, щелкнув правой кнопкой мыши по значку подключения на панели **Сети** и выбрав команду **Просмотр свойств подключения** (View connection properties). В случае проблем с установлением коммутируемого подключения, следующие советы будут полезными в их диагностировании и устранении.

- **Проблема:** модем успешно набирает номер, получает ответ от модема на другом конце, но не может подключиться. Модем просто издает звуки подключения, пока операция не будет прервана пользователем.

  Решение: обычно причиной такой проблемы является некачественная телефонная линия, в частности электростатические шумы на линии. Проверьте качество подключения кабеля к разъему модема и разъему телефонной линии. Узнайте в телефонной компании, могут ли ее сотрудники проверить линию и устранить проблему.

- **Проблема:** модем успешно набирает номер и вроде бы подключается к другому модему, но затем подключение резко обрывается. Подключение не может завершиться успешно.

  Решение: проверьте правильность установки сетевых протоколов и компонентов *(см. разд. "Настройка сетевых протоколов и компонентов" ранее в этой главе)*. Если эти параметры в норме, определите, передаются ли учетные данные Windows и домен, т. к. эта информация может быть необходимой. Подробную информацию *см. в разд. "Настройка учетных данных подключения" ранее в этой главе*.

- **Проблема:** пользователь не может получить доступ к домену Windows.

  Решение: для доступа к ресурсам сети организации может требоваться клиент для сетей Microsoft. Включите этот компонент и проверьте, что передается имя домена, если оно требуется.

- **Проблема:** не получается завершить вызов. Кажется, что модем использует неправильный номер, набирая либо недостаточное, либо слишком большое количество цифр номера.

  Решение: проверьте правила набора номера для подключения, а также текущее установленное расположение. Убедитесь, что эти параметры настроены должным образом для текущего расположения пользователя.

- **Проблема:** выводится сообщение, что нет сигнала в линии, но модем установлен правильно и по всем признакам, кажется, в порядке.

  Решение: проверьте телефонный шнур и правильность его подключения. Некоторые модемы имеют два разъема, один из них обозначен Phone/In[1] (или значком телефона), а

[1] Подключение телефона.

другой Line/Out[1] (или значком телефонного разъема). Телефонная линия должна быть подключена к разъему Line/Out. Некоторые телефонные линии предназначены только для высокоскоростной передачи данных, а не для подключения телефона или модема. Попробуйте подключиться к другой линии.

- **Проблема:** при попытке использовать модем компьютер зависает.

  Решение: наиболее вероятной причиной этой проблемы является конфликт устройств. Следуйте инструкциям, изложенным в *главе 9*, для настройки и диагностирования устройств.

- **Проблема:** некоторые службы зависают или не работают.

  Решение: проверьте настройки прокси-сервера и брандмауэра. Эти настройки могут запрещать требуемые службы.

Установка широкополосного подключения

Широкополосное подключение устанавливается посредством кабельного модема и кабельной линии или DSL-маршрутизатора и телефонной линии. Процесс установки широкополосного подключения следующий:

1. Откройте боковою панель **Сети**, щелкнув по значку **Сеть** в области уведомлений панели задач. На мобильных устройствах эту панель можно открыть, проведя пальцем от правого края экрана к центру, нажав опцию **Параметры**, а затем нажав значок **Сеть**.
2. В панели **Сеть** щелкните на требуемом широкополосном подключении, а затем нажмите кнопку **Подключить**.
3. Если для подключения не были предварительно установлены имя пользователя и пароль, введите эти параметры по запросу, а затем нажмите кнопку **OK**.

Просмотреть свойства подключения можно, щелкнув правой кнопкой мыши по значку широкополосного подключения на боковой панели **Сети** и выбрав опцию **Просмотр свойств подключения**.

Операционная система Windows 8 кэширует учетные данные для широкополосных подключений и использует эти данные для последующих установок подключения. Для удаления кэшированных учетных данных, чтобы можно было предоставить новые, щелкните правой кнопкой мыши на требуемом широкополосном подключении, а затем выберите команду **Очистить кэшированные учетные данные** (Clear cached credentials).

В случае проблем с установлением широкополосного подключения следующие советы будут полезными в их диагностировании и устранении.

- **Проблема:** невозможно установить подключение. Подключение полностью нерабочее.

  Решение: проверьте сетевые подключения. Проверьте правильность и надежность подключения кабеля, соединяющего компьютер и DSL-модем или кабельный модем, а также правильность подключения этих устройств к внешней линии.

- **Проблема:** подключение неожиданно обрывается и не может завершиться успешно.

  Решение: проверьте правильность установки сетевых протоколов и компонентов *(см. разд. "Настройка сетевых протоколов и компонентов" ранее в этой главе)*. Если эти параметры в норме, определите, передаются ли учетные данные Windows и домен,

[1] Подключение телефонной линии.

т. к. эта информация может быть необходимой. Подробную информацию *см. в разд. "Настройка учетных данных подключения" ранее в этой главе*.

- **Проблема:** некоторые службы зависают или не работают.

  Решение: проверьте настройки прокси-сервера и брандмауэра. Эти настройки могут запрещать требуемые службы.

- **Проблема:** невозможно получить доступ к домену Windows.

  Решение: для доступа к ресурсам сети организации может требоваться клиент для сетей Microsoft. Включите этот компонент и проверьте, что передается имя домена, если оно требуется.

Установление VPN-подключения

VPN-подключение можно установить по установленному сетевому, коммутируемому или широкополосному подключению. VPN-подключения отображаются отдельно от коммутируемых, широкополосных или сетевых подключений. Процедура установки VPN-подключения следующая:

1. Откройте боковую панель **Сети**, щелкнув по значку **Сеть** в области уведомлений панели задач. На мобильных устройствах эту панель можно открыть, проведя пальцем от правого края экрана к центру, нажав опцию **Параметры**, а затем нажав значок **Сеть**.
2. В панели **Сети** щелкните на требуемом VPN-подключении, а затем нажмите кнопку **Подключить**.
3. Если для установки VPN-подключения сначала требуется установить базовое подключение, Windows 8 попытается установить это подключение, прежде чем устанавливать VPN-подключение. Если выводится запрос на установку такого базового подключения, нажмите кнопку **Да**, а затем установите коммутируемое подключение, как рассматривается в *разд. "Установка коммутируемого подключения" ранее в этой главе*.
4. После установки необходимого базового подключения выводится диалоговое окно для установки VPN-подключения. Проверьте в нем правильность введенного имени пользователя и введите пароль для сетевой учетной записи (если он не был введен и сохранен при настройке подключения), а затем нажмите кнопку **Подключиться**.

Просмотреть свойства VPN-подключения можно, щелкнув правой кнопкой мыши по значку широкополосного подключения на боковой панели **Сети** и выбрав команду **Просмотр свойств подключения**.

В случае проблем с установлением VPN-подключения следующие советы будут полезными в их диагностировании и устранении.

- **Проблема:** невозможно установить подключение. Подключение полностью нерабочее.

  Решение: проверьте сетевые подключения. Проверьте правильность и надежность подключения кабеля, соединяющего компьютер и DSL-модем или кабельный модем, а также правильность подключения этих устройств к внешней линии. Если используется базовое коммутируемое подключение, проверьте правильность и надежность соединения модема с компьютером и с внешней телефонной линией.

- **Проблема:** выводится сообщение об ошибке в имени хоста.

  Решение: возможно, неправильно указано имя хоста. Проверьте параметры и убедитесь, что указывается полное имя хоста, например, **external01.microsoft**, а не просто **external01**. Также может неправильно работать служба разрешения имен DNS. В таком случае введите IP-адрес хоста вместо его имени.

- **Проблема:** выводится сообщение об ошибке в IP-адресе.

  Решение: проверьте правильность IP-адреса или введите его снова. Если IP-адрес правильный, возможно, неправильно настроено сетевое программное обеспечение TCP/IP. Проверьте правильность установки и настройки сетевых протоколов и компонентов *(см. разд. "Настройка сетевых протоколов и компонентов" ранее в этой главе)*. Также для подключения может потребоваться установить основной шлюз или статический IP-адрес.

- **Проблема:** выводится сообщение об ошибке, что протокол не поддерживается и установка подключения, по всей видимости, не выполняется успешно.

  Решение: вместо указания конкретного протокола — PPTP, L2TP, SSTP или IKEv2 — задайте автоматическое определение протокола. Проверьте параметры безопасного входа в систему. Возможно, что вместо смарт-карты требуется защищенный пароль или наоборот. Если эти параметры в норме, определите, передаются ли учетные данные Windows и домен, т. к. эта информация может быть необходимой. Подробную информацию *см. в разд. "Настройка учетных данных подключения" ранее в этой главе*.

- **Проблема:** не удается подключить сетевые диски или получить доступ к принтерам.

  Решение: для подключения сетевых дисков и принтеров требуется наличие компонента **Общий доступ к файлам и принтерам для сетей Майкрософт**. Включите этот компонент, как рассматривается в *разд. "Настройка сетевых протоколов и компонентов" ранее в этой главе*.

- **Проблема:** некоторые службы зависают или не работают.

  Решение: проверьте настройки прокси-сервера и брандмауэра. Эти настройки могут запрещать требуемые службы.

Беспроводные сети

Чтобы сотрудники могли брать свои мобильные устройства на совещания и на другие мероприятия, проводимые вдали от их обычных рабочих мест, многие организации настраивают в своих офисах беспроводные сети. Существует много разных конфигураций для развертывания и использования беспроводных сетей. В этом разделе мы рассмотрим наиболее распространенные из этих конфигураций.

Устройства и технологии беспроводных сетей

При работе с беспроводными сетями наиболее часто встречаются такие термины, как "адаптер беспроводной сети" и "беспроводная точка доступа". Беспроводные сетевые адаптеры могут быть в виде PC-плат для ноутбуков, PCI-плат для настольных компьютеров или USB-устройств, применяемых как с ноутбуками, так и с настольными системами. Но большинство современных мобильных устройств оснащено встроенными беспроводными сетевыми адаптерами. Для взаимодействия с точкой доступа беспроводный адаптер имеет встроенную антенну. Обычно точка доступа подключается непосредственно к физической сети организации и может также функционировать как сетевой коммутатор или концентратор. Иными словами, кроме беспроводных подключений, она также может обеспечивать кабельные подключения посредством физических разъемов для подключения сетевых кабелей. Точки доступа также называются *беспроводными базовыми станциями* и *беспроводными шлюзами*.

Наиболее широко используются беспроводные сетевые адаптеры и точки доступа на основе стандарта IEEE 802.11. Беспроводные устройства этого типа могут быть сертифицированы "Wi-Fi Certified", т. е. данное устройство соответствует требованиям тестирования на совместимость и может совместно работать с Wi-Fi-сертифицированными изделиями других поставщиков. В табл. 16.3 приводится сравнительный перечень возможностей основных версий стандарта IEEE 802.11. Как видно, существуют четыре версии этого стандарта, каждая из которых имеет свои достоинства и недостатки. Следует отметить, что хотя беспроводные устройства стандарта 802.11a не могут взаимодействовать с устройствами стандарта 802.11b или 802.11g, насыщенность устройствами пятигигагерцевого диапазона более низкая, что понижает вероятность взаимных помех с другими беспроводными устройствами (большинство беспроводных устройств использует диапазон 2,4 ГГц).

Таблица 16.3. *Беспроводные стандарты*

Беспроводной стандарт / Характеристика	802.11a	802.11b	802.11g	802.11n
Скорость	До 54 Мбит/с	До 11 Мбит/с	До 54 Мбит/с	До 540 Мбит/с
Радиочастота	5 ГГц	2,4 ГГц	2,4 ГГц	2,4 ГГц, 5 ГГц или обе
Эффективная дальность действия внутри помещений	Приблизительно 8 до 23 метра	Приблизительно 30 до 45 метров	Приблизительно 30 до 45 метров	Приблизительно 60 до 90 метров
Совместимость	Несовместимы с устройствами стандарта 802.11b и 802.11g	Могут взаимодействовать с устройствами стандарта 802.11g (со скоростью в 11 Мб/с). Беспроводные сетевые адаптеры стандарта 802/11g могут работать с точками доступа стандарта 802.11b (со скоростью в 11 Мб/с)	Могут взаимодействовать с устройствами стандарта 802.11b (со скоростью в 11 Мб/с)	Могут взаимодействовать с устройствами стандарта 802.11b (со скоростью в 11 Мб/с) и с устройствами стандарта 802.11g (со скоростью в 54 Мб/с)

Версия 802.11n является одной из последних версий стандарта 802.11. Она поддерживает скорость передачи данных до 540 Мбит/с, а устройства, поддерживающие ее, могут взаимодействовать с устройствами стандарта 802.11b и 802.11g. Для достижения высокой скорости передачи данных устройства стандарта 802.11n могут использовать несколько приемников и передатчиков. Каждый передатчик способен передавать один или больше потоков данных. Чем больше потоков данных устройство может разместить по всем передатчикам и приемникам, тем выше его пропускная способность. Но многие стандартные устройства типа 802.11n с несколькими приемниками и передатчиками совмещают сильные, слабые и отраженные сигналы в один поток данных, чтобы максимизировать дальность действия.

Для предоставления дополнительной безопасности организация IEEE определила стандарт 802.11i. В отличие от стандартов 802.11a, 802.11b, 802.11g и 802.11n, стандарт 802.11i не определяет скорость и частоту передачи данных. Это стандарт безопасности, который можно использовать совместно с другими стандартами семейства 802.11. В частности, этот стандарт добавляет функциональность безопасности к стандартам 802.11a, 802.11b, 802.11g и 802.11n. Это означает, что беспроводные сетевые адаптеры и точки доступа стандарта

802.11a могут содержать функциональность безопасности стандарта 802.11i, как и беспроводные устройства стандартов 802.11b, 802.11g и 802.11n.

Примечание

Следует помнить, что некоторые компьютеры (в особенности мобильные устройства) могут содержать интегрированные наборы микросхем, которые поддерживают несколько разных беспроводных технологий. Протокол WPA2[1] является одобренной альянсом Wi-Fi Alliance реализацией стандарта 802.11i. Этот протокол реализует все обязательные элементы стандарта 802.11i.

Практический совет

Прежде чем применять беспроводные устройства иного стандарта, чем 802.11, внимательно изучите вопросы совместимости. Все чаще встречаются устройства, поддерживающие высокую скорость передачи данных. Некоторые из этих устройств достигают этого посредством сжатия данных и других подобных технологий, соответствуя при этом основным требованиям спецификации IEEE 802.11. Другие могут использовать проприетарные сетевые технологии, требуя использования как беспроводных сетевых адаптеров, так и точек доступа данной компании для получения повышенной скорости передачи данных. Чтобы получить дополнительную информацию о стандартах беспроводных сетей и сертифицированных устройствах, посетите веб-сайт **www.wi-fi.org**.

Безопасность беспроводных сетей

Задача защиты беспроводной сети существенно отличается от аналогичной задачи для проводной сети. В проводной сети компьютеры подключаются к сети посредством физического кабеля. Кроме физического кабеля, для подключения к проводной сети также используется сетевой коммутатор или концентратор. Попытку несанкционированного подключения компьютера к проводной сети можно довольно легко обнаружить и проследить физический кабель к компьютеру злоумышленника.

Но любой может иметь доступ к беспроводной сети в пределах действия одной из ее беспроводных точек доступа. Злоумышленник может не только перехватывать передаваемые сигналы, но и попробовать подключиться к беспроводной сети. А обнаружение такого злоумышленника является трудной задачей вследствие отсутствия физического кабеля. Ситуация усугубляется, когда злоумышленник, подключившись к беспроводной точке доступа, попадает внутрь зоны, защищаемой брандмауэром организации. Чтобы защитить беспроводную сеть, необходимо настроить ее брандмауэр, если таковой имеется, а также настроить все беспроводные устройства на шифрование всей передаваемой информации.

Самой базовой схемой шифрования является протокол WEP (Wired Equivalency Protection, защита, аналогичная защите проводных сетей). Этот протокол позволяет зашифровывать данные 40-, 128-, 152-битовым личным ключом или ключом более высокой разрядности. Все передаваемые данные шифруются посредством симметричного ключа, производного от ключа WEP или пароля, и для приема этих данных их необходимо расшифровать, используя этот же ключ. В типичной проводной сетевой среде для защиты обмениваемых по сети данных вполне достаточно шифрования с общим ключом. Но большой объем трафика беспроводной сети делает возможным взлом перехваченного общего ключа, и поскольку этот ключ не меняется автоматически по истечении определенного периода времени, злоумышленник может получить доступ к внутренней сети организации.

Так как протокол WEP предоставляет только самую общую защиту, его использование крайне нежелательно за исключением ситуаций с отсутствующей альтернативой. Предпочитаемыми альтернативами протоколу WEP являются стандарты WPA и WPA2. Протокол

[1] Wi-Fi Protected Access Version 2 — защищенный доступ Wi-Fi, вторая версия.

WPA был принять альянсом Wi-Fi Alliance в качестве временного стандарта до утверждения стандарта 802.11i. Протокол WPA2 основан на официальном стандарте 802.11i и полностью обратно совместим с протоколом WPA.

Оба протокола могут периодически менять ключи для повышения безопасности и менять способы получения ключей, что значительно повышает уровень безопасности по сравнению с протоколом WEP. Устройства, поддерживающие протоколы WPA и WPA2, могут работать в режиме предприятия, в личной конфигурации или в конфигурации домашнего или небольшого офиса.

- Режим предприятия обеспечивает проверку подлинности на основе стандарта IEEE 802.1*x* и протокола EAP. В этом режиме беспроводные устройства используют два набора ключей: ключи сеанса и групповые ключи. Ключи сеанса являются уникальными для каждой ассоциации между точкой доступа и беспроводным клиентом. С их помощью создается частный виртуальный порт между точкой доступа и клиентом. Групповые ключи являются общими для всех клиентов, подключенных к одной и той же точке доступа. Оба набора ключей генерируются динамически и периодически меняются, чтобы повысить защиту целостности ключей с течением времени.
- Личный режим обеспечивает проверку подлинности посредством заранее распределенного ключа или пароля. В этом режиме и в режиме домашнего или небольшого офиса вместо изменения ключа шифрования протокол WPA использует заранее распределенный ключ шифрования. В этом режиме главный ключ (ключ группы) вводится в точку доступа, а затем выполняется настройка всех других беспроводных устройств для применения этого главного ключа. Беспроводное устройство использует главный ключ в качестве начальной точки для генерирования по математическому алгоритму ключа сеанса. Ключ сеанса затем регулярно меняется, чтобы один и тот же ключ сеанса никогда не использовался дважды. Так как смена ключей выполняется автоматически, управление ключами осуществляется в фоновом режиме.
- Протоколы WPA и WPA2 полностью совместимы со стандартами 802.11a, 802.11b, 802.11g и 802.11n. Многие беспроводные устройства, выпущенные до появления протоколов WPA и WPA2, можно сделать полностью совместимыми с этими протоколами, выполнив обновление их программного обеспечения. Для совместимости с протоколом WPA никаких других, кроме этой, модификаций выполнять не требуется. Но для совместимости с протоколом WPA2 одного обновления программного обеспечения может быть недостаточно, и может потребоваться обновление процессора или других аппаратных компонентов, чтобы устройство могло справляться с большим объемом вычислений, требуемым для выполнения шифрования AES.

При работе с протоколами WPA и WPA2 нужно иметь в виду следующее:

- все устройства, сертифицированные альянсом Wi-Fi для протокола WPA2, могут взаимодействовать с устройствами, сертифицированными альянсом Wi-Fi для протокола WPA;
- как протокол WPA, так и протокол WPA2 имеют личный режим работы и режим предприятия;
- как протокол WPA, так и протокол WPA2 используют для проверки подлинности стандарт IEEE 802.1*x* и протокол EAP;
- протокол WPA обеспечивает устойчивое шифрование с помощью протокола TKIP[1];

[1] Temporal Key Integrity Protocol — шифрование с использованием временных ключей.

- протокол WPA2 обеспечивает улучшенное шифрование данных посредством стандарта шифрования AES, что позволяет этому протоколу удовлетворять требования FIPS[1] 140-2 некоторых правительственных организаций (США).

> ***Примечание***
>
> Протоколы WPA и WPA2 предоставляют высокий уровень безопасности для повышения защиты конфиденциальных данных и обеспечивают доступ к беспроводным сетям лишь санкционированным пользователям. Но только протокол WPA2 предоставляет устойчивое шифрование с помощью AES, что требуется некоторым корпоративным и государственным (США) организациям.

Другой продвинутой технологией защиты беспроводных сетей является технология RSN[2], которая поддерживается устройствами стандарта 802.11i. Технология RSN позволяет беспроводным устройствам динамически согласовывать алгоритмы шифрования и проверки подлинности. Это означает, что алгоритмы шифрования и проверки подлинности, используемые устройствами RSN, можно изменять. Проблемы безопасности могут решаться добавлением новых методов проверки подлинности и алгоритмов шифрования. Технология RSN основана на протоколе EAP и стандарте AES.

Установка и настройка беспроводного сетевого адаптера

Кроме беспроводных сетевых адаптеров, встроенных в мобильные устройства, наиболее распространенными являются беспроводные адаптеры на PC-платах, используемые в ноутбуках, и на PCI-платах, используемые в настольных системах. Эти адаптеры легче всего настраивать, и автор находит их самыми надежными. Также все большую популярность набирают беспроводные сетевые адаптеры, подключаемые к компьютеру через USB-разъем. И здесь следует иметь в виду, что существует несколько спецификаций USB, включая USB 2.0 и более новую и быструю спецификацию USB 3.0. Беспроводной сетевой адаптер стандарта USB 3.0 надо подключать к порту USB 3.0, чтобы он функционировал должным образом и с ожидаемой от него скоростью.

Большинство программ установки беспроводных устройств помогает выполнить их настройку в процессе установки. При этом может потребоваться указать имя беспроводной сети, к которой требуется подключиться, и режим, в котором будет работать беспроводное устройство. Беспроводные сетевые адаптеры могут быть настроены для работы в режиме одной из двух топологий беспроводной сети.

- **Топология ad hoc.** При этой топологии беспроводной сетевой адаптер подключается напрямую к другим компьютерам, которые также оснащены беспроводными сетевыми адаптерами.
- **Инфраструктурная топология.** При этой топологии беспроводной сетевой адаптер подключается к беспроводной сети через точку доступа, а не непосредственно к другому компьютеру.

Кроме топологии сети для беспроводного адаптера может также потребоваться указать ключ шифрования для защиты обмениваемых адаптером данных. При использовании шифрования WEP в большинстве случаев нужно будет ввести требуемый ключ шифрования, который обычно называется *сетевым ключом*. А при использовании защиты WPA/WPA2

---

[1] Federal Information Processing Standard — федеральный стандарт обработки информации.

[2] Robust Security Network — сеть с повышенной безопасностью.

требуемый ключ шифрования наиболее часто предоставляется посредством смарт-карты или сертификата.

Работа с беспроводными сетями и подключениями

После установки беспроводного сетевого адаптера компьютер должен подключиться к беспроводной сети. Во многом подобно проводному сетевому адаптеру, который подключается к сети посредством технологии Ethernet, беспроводной сетевой адаптер подключается посредством технологии Wi-Fi к общедоступным, частным или доменным сетям. Если компьютер оснащен проводным и беспроводным сетевым адаптером, он может иметь два активных сетевых подключения: к проводной и беспроводной сети соответственно.

Беспроводные подключения предоставляют следующие дополнительные сведения о сети и подключении:

- имя беспроводной сети, указанное в скобках после обозначения типа подключения;
- графическое представление текущего уровня сигнала в виде пяти столбцов возрастающей высоты. Один столбец (самый короткий) означает самое плохое качество сигнала, а все пять столбцов — лучшее;
- ссылку **Отключение** для отключения беспроводного соединения.

Просмотреть параметры беспроводного подключения можно следующим образом:

1. В разделе **Сеть и Интернет** Панели управления щелкните по ссылке **Просмотр состояния сети и задач**.
2. В левой панели Центра управления сетями и общим доступом щелкните по ссылке **Изменение параметров адаптера**.
3. В результате откроется окно **Сетевые подключения**, содержащее список (или значки, в зависимости от выбранного представления) всех сетевых подключений компьютера. Щелкните правой кнопкой мыши по значку требуемого беспроводного подключения и в контекстном меню выберите команду **Состояние**.
4. Откроется диалоговое окно состояния беспроводного подключения, подобное показанному на рис. 16.11.

   Окно состояния беспроводного подключения служит для проверки состояния подключения и его поддержки и во многом подобно окну состояния для других типов подключений. Отображаемая в этом окне информация содержит сведения о длительности и скорости подключения.

Как и Ethernet-подключения, беспроводные подключения имеют настраиваемые свойства. Это означает, что все, что сказано ранее о настройке свойств проводных сетевых подключений, также относится и к беспроводным сетевым подключениям. В частности, можно выполнять следующие настройки подключения:

- устанавливать и удалять сетевые компоненты для клиентов, служб и протоколов. Для этого в диалоговом окне состояния беспроводного подключения нажмите кнопку **Свойства**, а затем нажмите кнопку **Установить** или **Удалить**, в зависимости от требуемого действия;
- устанавливать параметры TCP/IPv6 и TCP/IPv4 для службы DHCP и статическую или динамическую IP-адресацию. Для этого в окне состояния беспроводного подключения нажмите кнопку **Свойства**, а затем в списке компонентов дважды щелкните на компоненте **Протокол Интернета версии 6 (TCP/IPv6)** или **Протокол Интернета версии 4 (TCP/IPv4)**;

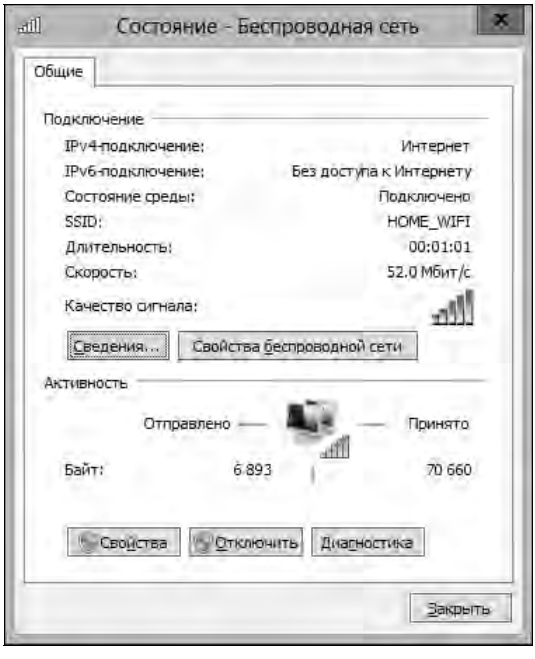


Рис. 16.11. Диалоговое окно состояния беспроводного подключения

- отключать или выполнять диагностику беспроводного подключения. Для этого в окне состояния беспроводного подключения нажмите кнопку **Отключить** или **Диагностика**, в зависимости от требуемого действия.

В случае проблем с установлением беспроводного подключения, которые не могут быть решены с помощью средств автоматической диагностики, следующие советы могут оказаться полезными в их диагностировании и устранении.

- **Проблема:** отсутствует или ограничена связь с беспроводной сетью.

  Решение: проверьте уровень сигнала. При низком уровне сигнала нужно переместить беспроводное устройство ближе к точке доступа или попробовать настроить положение антенны для максимального уровня сигнала. В случае встроенной антенны может потребоваться изменить положение мобильного устройства по отношению к точке доступа. Причиной проблемы может также быть то, что не было выполнено подключение к сети и сетевая адресация не была настроена должным образом. Чтобы проверить состояние подключения, в Центре управления сетями и общим доступом щелкните по ссылке требуемого подключения и в открывшемся окне состояния проверьте уровень сигнала и другие параметры. Если параметр **Состояние среды** (Media State) не отображается как **Подключено**, нажмите кнопку **Диагностика**, чтобы попытаться решить проблему с помощью средств автоматической диагностики.

- **Проблема:** не удается подключиться к беспроводной сети.

  Решение: если компьютер находится вне зоны действия точки доступа, подключение к сети будет невозможным. Щелкните по значку сети в области уведомлений панели задач. В открывшейся боковой панели **Сети** проверьте наличие сетей и уровень их сигналов. Также проверьте, не включен ли режим "в самолете", т. к. включение этого режима отключает все беспроводные подключения. Чтобы подключиться к беспроводной сети, щелкните на требуемом подключении в боковой панели **Сети**, а затем нажмите кнопку

Подключиться. Если не удается подключиться к сети или необходимая сеть отсутствует в списке сетей в боковой панели **Сети**, попробуйте переместить беспроводное устройство ближе к точке доступа или попытаться настроить положение антенны либо компьютера относительно точки доступа для максимального уровня сигнала. Компьютер может быть не настроен должным образом для установления подключения к данной беспроводной сети.

Совет

Чем выше уровень сигнала, тем большая скорость подключения, вплоть до максимальной, поддерживаемой используемой беспроводной технологией. При слабом уровне сигнала скорость подключения может значительно упасть. Чтобы улучшить качество сигнала, попробуйте перемещать антенну беспроводного сетевого адаптера (если она имеется) или же изменять положение компьютера относительно точки доступа.

Подключение к беспроводной сети

Компьютер с беспроводным сетевым подключением должен подключаться к любой беспроводной точке доступа, в пределах зоны покрытия которой он находится. По умолчанию Windows 8 автоматически определяет необходимые для подключения параметры. Если для подключения требуется предоставить пароль или иные учетные данные, при попытке установить подключение к беспроводной сети выводится запрос предоставить эти учетные данные. Также для пользователей можно выполнить предварительную настройку беспроводного подключения, установив разные параметры проверки подлинности, шифрования и режима связи, как требуется.

Выполнить предварительную настройку подключения к беспроводной сети можно следующим образом:

1. В Центре управления сетями и общим доступом щелкните по ссылке **Настройка нового подключения или сети**. Будет запущен мастер **Настройка подключения или сети**.
2. Выберите опцию **Подключение к беспроводной сети вручную** (Manually connect to a wireless network) и нажмите кнопку **Далее**. На следующей странице мастера нужно ввести информацию о беспроводной сети, к которой требуется подключиться. Эти сведения можно получить от сетевого администратора организации.
3. Введите имя сети в соответствующее текстовое поле (имя сети также называется идентификатором SSID сети).
4. В списке **Тип безопасности** (Security type) выберите требуемый тип безопасности, для него автоматически устанавливается тип шифрования.
5. Для типа безопасности WEP и WPA-Personal необходимо ввести соответствующий ключ безопасности или парольную фразу в текстовое поле **Ключ безопасности** (Security key). Ключ безопасности WEP обычно является одним из следующих:
   - пять символов с учетом регистра;
   - 13 символов с учетом регистра;
   - 10 шестнадцатеричных символов без учета регистра;
   - 26 шестнадцатеричных символов без учета регистра.
6. По умолчанию подключение устанавливается автоматически при входе пользователя в систему. Если следует попытаться установить подключение, независимо он наличия доступной сети (например, когда компьютер находится вне зоны покрытия беспроводной точки доступа), установите флажок **Подключаться, даже если сеть не производит**

широковещательную передачу (Connect even if the network is not broadcasting). Если не установить этот флажок, подключение будет отображаться на боковой панели **Сети** только в том случае, если сеть находится в пределах досягаемости и передает свой идентификатор SSID.

7. Нажмите кнопку **OK**, а затем **Закрыть**, чтобы сохранить настройки и закрыть все диалоговые окна.

Обычно, когда компьютер находится в пределах зоны покрытия беспроводной сети, выполнять предварительную настройку подключения не требуется, а можно выполнять автоматическую установку подключения, предоставив Windows определить правильные настройки. Процедура подключения к беспроводной сети следующая:

1. Откройте боковую панель **Сети**, щелкнув по значку **Сеть** в области уведомлений панели задач. На мобильных устройствах эту панель можно открыть, проведя пальцем от правого края экрана к центру, нажав опцию **Параметры**, а затем нажав значок **Сеть**.
2. Раздел **Беспроводная сеть** (Wi-Fi) панели **Сети** содержит список доступных беспроводных сетей, упорядоченных по имени, состоянию и уровню сигнала.
3. С сетями в этом списке можно выполнять следующее:
   - подключаться, выбрав требуемую сеть и нажав кнопку **Подключиться**;
   - отключаться, выбрав требуемую сеть и нажав кнопку **Отключиться**.

Управление беспроводными сетями и их диагностирование

Управление беспроводными сетями осуществляется с помощью боковой панели **Сети**. Щелчок правой кнопкой мыши по беспроводной сети в списке открывает контекстное меню, содержащее следующие команды.

- **Отображать сведения о предполагаемом использовании данных** (Show estimated data usage). Отображает оценочные сведения об объеме данных, обработанных подключением. Щелкните по ссылке **Сброс**, чтобы очистить счетчик.
- **Задать как лимитное подключение** (Set as metered connection). Определяет подключение как тарифицируемое, чтобы к нему применялись правила и политики для тарифицированных подключений.
- **Задать как безлимитное подключение** (Set as non-metered connection). Определяет подключение как нетарифицируемое, чтобы к нему больше не применялись правила и политики для тарифицированных подключений.
- **Забыть эту сеть** (Forget this network). Удаляет подключение из списка доступных подключений. Опция полезна в тех случаях, когда созданное вручную подключение больше не требуется.
- **Включение и отключение общего доступа** (Turn sharing on or off). Позволяет задать или отменить общий доступ к устройствам в данной сети.
- **Просмотреть свойства подключения** (View connection properties). Открывает диалоговое окно свойств данной беспроводной сети на вкладке **Безопасность**. Таким образом можно быстро просмотреть или изменить параметры безопасности подключения.

Операционная система Windows 8 содержит большое количество инструментов для диагностирования и проверки работоспособности сетей. Методы для диагностирования и устранения сетевых проблем рассматриваются в *разд. "Диагностирование и тестирование сетевых*

параметров" главы 15. Подобные проблемы возникают и в беспроводных сетях. Для их диагностирования и устранения, кроме рассмотренных в *главе 15* методов, рекомендуется использовать следующие.

- Проверьте конфигурацию параметров безопасности беспроводной сети и удостоверьтесь в их правильности. Повторно введите ключ безопасности и парольную фразу.
- Проверьте, что расположение беспроводного устройства по отношению к точке доступа обеспечивает максимальный уровень сигнала, а устройство находится в пределах зоны покрытия точки доступа. Может быть, необходимо переместить компьютер ближе к точке доступа.
- Проверьте отсутствие помех от других устройств, которые работают в том же частотном диапазоне, что и ваше беспроводное устройство, или электромагнитных помех от других устройств. Может быть, необходимо переместить или выключить устройства, которые, вероятно, создают помехи.

Предметный указатель

A

B

Б

В

Г

Д

Ж

З

И

К

Л

М

Н

П

P

C

Т

У

Ф

X

Ц

Ш

Э

Я

Microsoft Windows® 8

Справочник администратора

Практическое руководство для администраторов Windows!

Быстро и качественно выполняйте повседневные задачи настройки, оптимизации и обслуживания Windows 8 с помощью справочных таблиц, инструкций и списков параметров, представленных в книге. Вы сэкономите время и справитесь с поставленными задачами.

В этой книге:

- управление установкой и настройкой системы;
- оптимизирование рабочего стола и пользовательского интерфейса;
- настройка предпочтения групповой политики;
- использование модуля TPM и шифрования дисков BitLocker;
- реализация TCP/IP и мобильных сетей;
- настройка учетных записей пользователей, доступ к данным и безопасность;
- управление устройствами, приложениями и виртуализацией;
- администрирование дисков и файловых систем;
- выполнение поиска и устранение неполадок;
- управление обновлениями, резервными копиями и восстановлением системы.

Об авторе

Уильям Р. Станек (William R. Stanek) — обладатель статуса Microsoft MVP, имеет 20-летний опыт в области системного администрирования и продвинутого программирования. Отмечен наградами, написал свыше 100 книг, включая «Microsoft Windows Server 2012. Справочник администратора», «Microsoft SQL Server 2012. Справочник администратора». Редактор серии Справочник администратора.

Издательство
Русская редакция
Москва,
ул. Свободы, д. 17, а/я 14
E-mail: info@rusedit.com
Internet: www.rusedit.com
Тел.: (495) 638-5-638

БХВ-ПЕТЕРБУРГ
191036, Санкт-Петербург,
Гончарная ул., 20
Тел.: (812) 717-10-50,
339-54-17, 339-54-28
E-mail: mail@bhv.ru
Internet: www.bhv.ru

Windows 8

Microsoft

ISBN 978-5-7502-0426-7

bhv®

РУССКАЯ РЕДАКЦИЯ