КОМПЬЮТЕР ГЛАЗАМИ ХАКЕРА

3-е издание

Михаил Флёнов

Модификация операционной системы Windows

Разгон компьютера

Атаки хакеров и защита

Форсирование Интернета

Компьютерные шутки

Материалы на www.bhv.ru

bhv®

Михаил Флёнов

КОМПЬЮТЕР ГЛАЗАМИ ХАКЕРА

3-е издание

Санкт-Петербург
«БХВ-Петербург»
2012

УДК 681.3.06
ББК 32.973.26-018.2
Ф70

Флёнов М. Е.

Ф70 Компьютер глазами хакера. — 3-е изд., перераб. и доп. — СПб.: БХВ-Петербург, 2012. — 272 с.: ил.

ISBN 978-5-9775-0790-5

Рассмотрены компьютер, операционные системы Windows XP/Vista/7 и Интернет с точки зрения организации безопасной и эффективной работы на ПК. Описаны основные методы атак хакеров и рекомендации, которые позволят сделать компьютер быстрее, надежнее и безопаснее. Представлены примеры накручивания счетчиков на интернет-сайтах и методы взлома простых вариантов защиты программ Shareware. Приведены советы хакеров, которые позволят при путешествии по Интернету не заразиться вирусами и не стать добычей сетевых мошенников, владеющих методами социальной инженерии. Показано, как сделать интерфейс Windows более удобным и привлекательным, компьютер — надежнее и быстрее, а работу в сети — более эффективной. В третьем издании добавлены новые примеры для операционной системы Windows 7. На сайте издательства находятся программы, описанные в книге, а также используемые файлы и дополнительные статьи.

Для пользователей ПК

УДК 681.3.06
ББК 32.973.26-018.2

Группа подготовки издания:

Главный редактор	*Екатерина Кондукова*
Зам. главного редактора	*Игорь Шишигин*
Зав. редакцией	*Григорий Добин*
Редактор	*Анна Кузьмина*
Компьютерная верстка	*Ольги Сергиенко*
Корректор	*Наталия Першакова*
Дизайн серии	*Инны Тачиной*
Оформление обложки	*Марины Дамбиевой*
Зав. производством	*Николай Тверских*

Подписано в печать 31.01.12.
Формат 70×100 1/16. Печать офсетная. Усл. печ. л. 21,93.
Тираж 2000 экз. Заказ №
"БХВ-Петербург", 190005, Санкт-Петербург, Измайловский пр., 29.

Отпечатано с готовых диапозитивов
в ГУП "Типография "Наука"
199034, Санкт-Петербург, 9 линия, 12

ISBN 978-5-9775-0790-5

Оглавление

Введение

Первое издание книги я начинал с того, что компьютер становится неотъемлемой частью нашей жизни. Прошло уже несколько лет, и сейчас можно смело говорить, что компьютер уже стал неотъемлемой частью нашего бытия. Лично у меня дома один стационарный компьютер и три ноутбука. Стационарный компьютер у детей, по ноутбуку у меня с женой и один ноутбук с Linux, который используется мною для моих рабочих дел. Вот думаем еще купить один ноутбук дочке, чтобы не дралась с братом за стационарный компьютер.

А ведь в доме есть еще Xbox360, который так же можно назвать полноценным компьютером, просто заточенным под игры, PSP. Ах да, я еще забыл о китайском планшетнике, который тоже является компьютером.

Не забываем и про смартфоны, которые начинают вытеснять простые телефоны. Нынешние смартфоны по своей мощности уже догнали те персональные компьютеры, которые существовали во времена написания первого издания. На моем HTC Surround установлен процессор с одним гигагерцем и видеоускорителем. Я писал первое издание на ноутбуке с процессором Pentium M 1,6 ГГц. Уже появляются смартфоны на процессорах с двумя ядрами, и о такой мощности я мог только мечтать в 90-х годах, а сейчас я эту мощь ношу с собой каждый день в кармане и использую для звонков и серфинга по Интернету.

Каждый день я иду на работу, а за спиной в рюкзаке находится ноутбук HP. Выдалась свободная минутка — так, крышка ноутбука открывается и начинает переливаться разными цветами, показывая загрузку Windows. Теперь творить можно где и когда угодно, лишь бы хватило заряда аккумулятора. Практически каждый день я разбираю почту в метро или работаю над очередной заметкой для своих блогов, а в ближайшие дни собираюсь тратить свое время в пути на работу и домой на написание этой книги.

Темп жизни растет с каждым днем, и постоянного наличия ноутбука под рукой, например мне, уже не хватает. Люди начинают окружать себя дополнительными цифровыми устройствами, такими как планшетники, смартфоны и игровые приставки. Компьютеры внедряются в жизнь все активнее, и их отказы, кража, взлом и другие неприятности могут привести к катастрофе. Именно поэтому все связанное с хакерами все ярче описывается в прессе.

Эта книга полезна абсолютно всем, кто хоть как-то связан с компьютерами. Специалистам некоторые вещи покажутся слишком простыми, хотя мой опыт говорит, что мелочей в нашей жизни не бывает. Но даже если вы хорошо знакомы с компьютером, то данная книга будет вам интересна, как веселое повествование о том, что вы уже знаете. Ну а если вы знакомы с компьютерами и хакерами поверхностно, то помимо хорошего времяпровождения сможете узнать и полезную информацию. Надеюсь, что вы не пожалеете потраченных времени и денег.

Компьютер глазами хакера

Не знаю почему, но у некоторых людей очень странная реакция на слово "хакер", особенно на обложке книги. Некоторые почему-то считают, что в такой книге обязательно должно описываться написание вирусов, другие предполагают, что там должен обсуждаться изощренный взлом сайтов или программ. Но ничего из этого не имеет отношения к книге. Для подобных тем книга называлась бы по-другому. Например, как приемы взлома и защиты от взлома сайтов я описывал в книгах "PHP глазами хакера" [7] и "Web-сервер глазами хакера" [6]. Взломами программ я не интересуюсь, хотя и был опыт много лет назад.

Так о чем же эта книга? Мы будем говорить о компьютере вообще и ОС Windows в частности. И чем же она будет отличаться от других самоучителей/книг по компьютерам? Мы будем говорить о безопасности, о компьютерных приколах и об оптимизации компьютера. Хакерство — это не просто взлом программы или сервера, это образ жизни.

Если вас смущает слово "хакер" в названии книги, то просто проигнорируйте его. Читайте самое важное для себя, и надеюсь, что она будет для вас интересна и познавательна.

Хакеры — это не ботаны, которые сидят с сигаретой в руках по ночам в рваных джинсах в нищих квартирах. Это такие же люди, как мы с вами. Они так же зависимы от общества, в котором живут, и бывают совершенно разными. Бывают хакеры, которые действительно зарабатывают копейки и работают за обеды, устанавливая ОС в школах, а бывают очень богатые и обеспеченные люди. Так что ломайте стереотипы, которые созданы в СМИ.

Мне приходилось общаться в своей жизни с большим количеством людей, которые являются профессионалами в ИТ и которых я бы без проблем называл хакерами. У меня был большой опыт работы в журнале "Хакер", и я могу сказать, что все там достойны, чтобы их называли хакерами. Возможно, не все ломали сайты, возможно, не все ломали программы, но это не является показателем какой-то элитности. И во время общения с этими людьми трудно не заметить одну особенность — они все обладают хорошим чувством юмора. Есть хакеры-ботаники, но такие как раз почему-то не любят журнал "Хакер".

Я никогда не был ботаником и люблю прикалываться, поэтому этой составляющей хакерского мира мы тоже уделим небольшое внимание. Вы увидите, как можно подшутить над друзьями или коллегами, используя компьютер, узнаете некоторые

секреты использования Интернета и сможете повысить эффективность своего пребывания в сети. Помимо этого, вас ждет множество интересных и веселых ситуаций, компьютерных шуток из моей жизни и многое другое.

Возможно, где-то книга даже покажется немного философской, но это только третье издание. Первое было больше практическим. Это во втором издании я решил поговорить чуть больше.

Книга стоит на трех китах: компьютер, ОС Windows и Интернет. Это действительно значимые понятия современной эпохи, и именно их мы будем рассматривать с точки зрения хакера. А если конкретнее, нам предстоит узнать про тюнинг (настройка, оптимизация и ускорение), взлом и защиту компьютера, ОС Windows и Интернета.

Эта книга отличается от других тем, что здесь полезные знания можно приобрести, совмещая процесс познания с отдыхом и развлечением. Вы узнаете, как сделать свою работу за компьютером лучше, интереснее, эффективнее и безопаснее.

Но работа должна приносить удовольствие. Постоянно трудиться за одним и тем же рабочим столом утомляет. Вы же делаете дома перестановку, обновляете интерьер, чтобы четыре стены не докучали своим видом? То же самое и с компьютером. Однообразные окна надоедают, а смена только обоев рабочего стола и окраски окон не приносит нужного эффекта. Хочется чего-то большего.

Компьютер сейчас — не просто дань моде, для меня это источник дохода, средство отдыха и развлечения, инструмент для получения информации и обучения, ну и, конечно же, способ самовыражения. Он позволяет реализовать многие мои желания. В этой книге я поделюсь с вами самым интересным из того, что знаю о "внутренностях" ОС Windows, с точки зрения пользователя. Это поможет придумать новые компьютерные шутки, использовать железо по максимуму или просто разнообразить вашу жизнь.

Вы узнаете, как сделать интерфейс приложений более удобным и изящным. Свои любимые программы я под Новый год раньше украшал гирляндами, а летом на диалоговых окнах рассаживал цветы. Это делает жизнь приятнее и красивее. Почему "раньше"? Сейчас времени как-то нет, а жаль. Это интересное занятие.

Многие люди, покупая новый автомобиль, сразу же приступают к тюнингу. Это позволяет через машину продемонстрировать свою индивидуальность и выделиться среди окружающих. Почему не поступить так и с компьютером? Он ведь тоже является отражением наших характерных особенностей, и мы имеем на это полное право.

Некоторые хакеры занимаются модингом, украшая системный блок, а кто-то предпочитает улучшать ОС. Я больше люблю все же программные украшения, потому что именно с ОС приходится работать чаще, а системный блок больше стоит под столом и никому не виден, но от тюнинга железа все равно не отказываюсь. Именно поэтому первым делом мы будем украшать Windows, а заодно познакомимся с универсальными способами изменения и других программ. Конечно же, эти приемы применимы не ко всем программам, но к большинству — это уж точно.

Я провожу за компьютером по 10—12 часов, а когда еще не было ни жены, ни детей, то у монитора просиживал до 16 часов, в основном ночью, когда тихо и спокойно. Я даже кушал, держась одной рукой за клавиатуру, а отходил от компьютера только, чтобы поспать. Так как в игры я практически не играю, то получалось, что большая часть времени уходила на программирование и изучение системы. Но надо же как-нибудь отдыхать и развлекаться! Вот я и начал создавать маленькие смешные программы, с помощью которых легко подшутить над друзьями и коллегами по работе. Большинство таких программ или трюков рождалось именно на работе, где был "испытательный полигон" для новых идей. Всегда хочется показать свои знания и умения (и даже превосходство), и юмор позволяет это сделать как нельзя лучше. А главное, на работе есть корпоративная сеть, в которой много компьютеров, а значит и потенциальных "жертв". Именно сеть позволяет сделать шутки более интересными.

Мне в те времена повезло с заместителем начальника моего отдела, потому что он тоже был любителем подшутить над ближним. Нужно действовать по великой заповеди хакеров: "Подшути над ближним своим, ибо он подшутит над тобой и возрадуется".

Однажды у меня перестал работать монитор, и я долго не мог понять почему. Оказалось, что монитор работал, просто над ним "поколдовал" мой шеф (про эту шутку читай в *главе 3*). После этого между нами развернулась настоящая война. Мы постоянно искали новые способы "напакостить" друг другу. С каждым днем шутки становились все интереснее и изощреннее.

Некоторые вещи, которые мы будем рассматривать, могут нарушать какое-либо лицензионное соглашение разработчика программы, ОС или компьютера, поэтому прежде чем приступать к действиям, следует внимательно с ним ознакомиться. Например, мы узнаем, как можно изменить ресурсы приложения (окна, меню, значки и т. д.), что противоречит лицензионному соглашению на использование разработок большинства крупных производителей программного обеспечения. Небольшие фирмы или программисты-одиночки делают соглашения более мягкими или вообще не используют их в своей практике, и самое интересное из того, как их можно настроить на свой вкус, я раскрою на страницах этой книги.

Правило использования

Лично я не понимаю, почему нам запрещают изменять что-то в программе, которую мы честно купили. Производители телевизоров не запрещают перекрашивать его в другой цвет, да и с автомобилями можно делать все, что угодно (теряется только гарантия). Так почему же нельзя то же самое сделать с Windows?

Но необходимо отдавать себе отчет в том, что, нарушив лицензию, вы можете лишиться поддержки. Я, да и многие другие, этой поддержкой не пользуюсь, поэтому смело изменяю все, что захочу.

Помните, что большинство примеров приводится только в информационных целях, для лучшего понимания системы и компьютера. За использование этих знаний

в незаконных целях автор и издательство ответственности не несут. Я всегда говорил, что даже безобидный предмет может стать оружием уничтожения или разрушения.

Кто такие хакеры?

Это довольно спорный вопрос, и я достаточно много писал о том, кто такие хакеры и как ими стать. Давайте разберем понятие "хакер" с позиции, с которой я буду рассматривать его в данной книге. Именно из-за того, что у некоторых людей другое понимание слова "хакер", начинаются непонятные вопросы к названию этой книги или к его содержимому.

Но для начала надо углубиться немного в историю. Понятие "хакер" зародилось, когда только начинала распространяться первая сеть ARPANET. Тогда это понятие обозначало человека, хорошо разбирающегося в компьютерах. Некоторые даже подразумевали под хакером человека, "помешанного" на компьютерах. Понятие ассоциировали со свободным компьютерщиком, человеком, стремящимся к свободе во всем, что касалось его любимой "игрушки" — компьютера. Собственно благодаря этому стремлению и тяге к свободному обмену информацией и началось такое бурное развитие всемирной сети. Я считаю, что именно хакеры помогли развитию Интернета и создали FIDO. Благодаря им появились UNIX-подобные системы с открытым исходным кодом, на которых сейчас работает большое количество серверов.

В те далекие времена еще не было вирусов и никто даже не думал о взломе сетей, сайтов или отдельных компьютеров. Образ хакера-взломщика появился немного позже. Но это только образ. Настоящие хакеры никогда не имели никакого отношения к взломам, а если хакер направлял свои действия на разрушение, то это резко осуждалось виртуальным сообществом. Даже самые яркие представители борцов за свободу не любят, когда кто-либо вмешивается в их личную жизнь.

Так что если вы купили книгу в надежде, что тут будет что-то о взломе чего-либо, только из-за слова "хакер" на обложке, вы можете разочароваться. Но я все же постарался сделать книгу как можно интереснее и полезнее, поэтому все же надеюсь, что вы не разочаруетесь.

Настоящий хакер — это творец, а не разрушитель. Так как творцов оказалось больше, чем разрушителей, то истинные хакеры выделили тех, кто занимается взломом, в отдельную группу и назвали их крэкерами (взломщиками) или просто вандалами. И хакеры, и взломщики являются гениями виртуального мира. И те, и другие борются за свободу доступа к информации. Но только крэкеры взламывают сайты, закрытые базы данных и другие источники информации с целью собственной наживы, ради денег или минутной славы, такого человека можно назвать только преступником (кем он по закону и является!).

Если вы взломали программу, чтобы увидеть, как она работает, то вы — хакер, а при намерении ее продать или просто выложить в Интернете crack (крэк) — становитесь преступником. Но если вы взломали сервер/компьютер/веб-сайт и сообщили владельцу ресурса об уязвимости, то вы, несомненно, — хакер.

Жаль, что многие специалисты не видят этой разницы и путают хакерские исследования с правонарушениями. Хакеры интересуются безопасностью систем и серверов для определения ее надежности (или в образовательных целях), а крэкеры — с целью воровства или уничтожения данных.

Итак, к крэкерам относятся:

- вирусописатели — программисты, которые применяют свои знания на то, чтобы написать программу разрушительной направленности;
- вандалы — эти люди стремятся уничтожить систему, удалить все файлы или нарушить работу сервера;
- взломщики компьютеров/серверов — они совершают "кражу со взломом" с целью наживы, выполняя зачастую чьи-либо заказы на получение информации, но очень редко используют свои знания в разрушительных целях;
- взломщики программ — такие крэкеры снимают защиту с программного обеспечения и предоставляют его для всеобщего использования. Этим они приносят ущерб софтверным фирмам и государству. Программисты должны получать зарплату за свой труд.

Чтобы еще раз подчеркнуть разницу между хакером и крэкером, можно сравнить их с взломщиками программ. Все прекрасно понимают, что многие софтверные фирмы завышают цены на свои программные продукты. Крэкер будет бороться с ценами с помощью снятия защиты, а хакер создаст свою программу с аналогичными функциями, но меньшей стоимости или вообще бесплатную. Так, движение Open Source можно причислить к хакерам, а те, кто пишет крэки, относятся к взломщикам, т. е. крэкерам.

Мне кажется, что путаница в понятиях отчасти возникла из-за некомпетентности в этом вопросе средств массовой информации. Журналисты популярных СМИ, не вполне разбираясь в проблеме, приписывают хакерам взломы, делая из них преступников.

Истинные хакеры никогда не используют свои знания во вред другим. Именно к этому я призываю в данной книге, и никакого конкретного взлома или вирусов в ней не будет описано. Вы найдете только полезную и познавательную информацию, которую сможете использовать для умножения своих знаний.

Так как в нашей жизни злостный образ хакера уже устоялся и от него уже не избавиться, то их разделили на White Hat (белые шапки) и Black Hat (черные шапки). К черным шапочкам относятся как раз хакеры, которые все взламывают. К белым шапочкам (почему-то возникает ассоциация с врачами) относятся добрые и пушистые хакеры, которых я уважаю и о которых мы будем говорить.

Есть еще красные шапочки (Red Hat), но это отдельная элитная категория, которая носит бабушкам пирожки, а всем остальным открытый код :). Шутка конечно же. На счет пирожков я не уверен, а вот открытый код Red Hat все же несет миру. С этими шапками связан самый знаменитый дистрибутив Linux, который в свое время наделал много шума.

Хакеры должны очень хорошо знать компьютер и в особенности ОС, а также желательно знание программирования и лучше на нескольких языках. Когда мы будем рассматривать атаки, которые используют хакеры, то вы увидите, что без навыков программирования реализовать большинство из этих приемов будет невозможно. Если вы заинтересовались и решили повысить свой уровень мастерства, то могу посоветовать прочитать мои книги "Программирование в Delphi глазами хакера" [2] и "Программирование на C++ глазами хакера" [1]. Надеюсь, это поможет вам научиться создавать собственные шуточные программы и хакерский софт. Для понимания материала не надо иметь глубоких знаний в программировании. Компьютерные шутки, которые мы будем рассматривать в данной книге, хороши, но не менее интересно самостоятельно сотворить забавную программу и подбросить ее друзьям.

Напоследок я хочу дать вам одну ссылку на одну статью энциклопедии Wiki: **http://ru.wikipedia.org/wiki/%D5%E0%EA%E5%F0**. Выглядит страшно и не понятно, но на самом деле это то же самое, что написать: **http://ru.wikipedia.org/wiki/хакер**. Просто, если ввести этот адрес в браузере, сайт переведет русское слово в URL в закодированный формат (коды букв вместо реальных букв) и загрузит уже эту страницу. В этой статье промотайте немного вниз, и напротив раздела "Известные хакеры" вы должны увидеть фото Линуса Торвальдса (рис. В1).

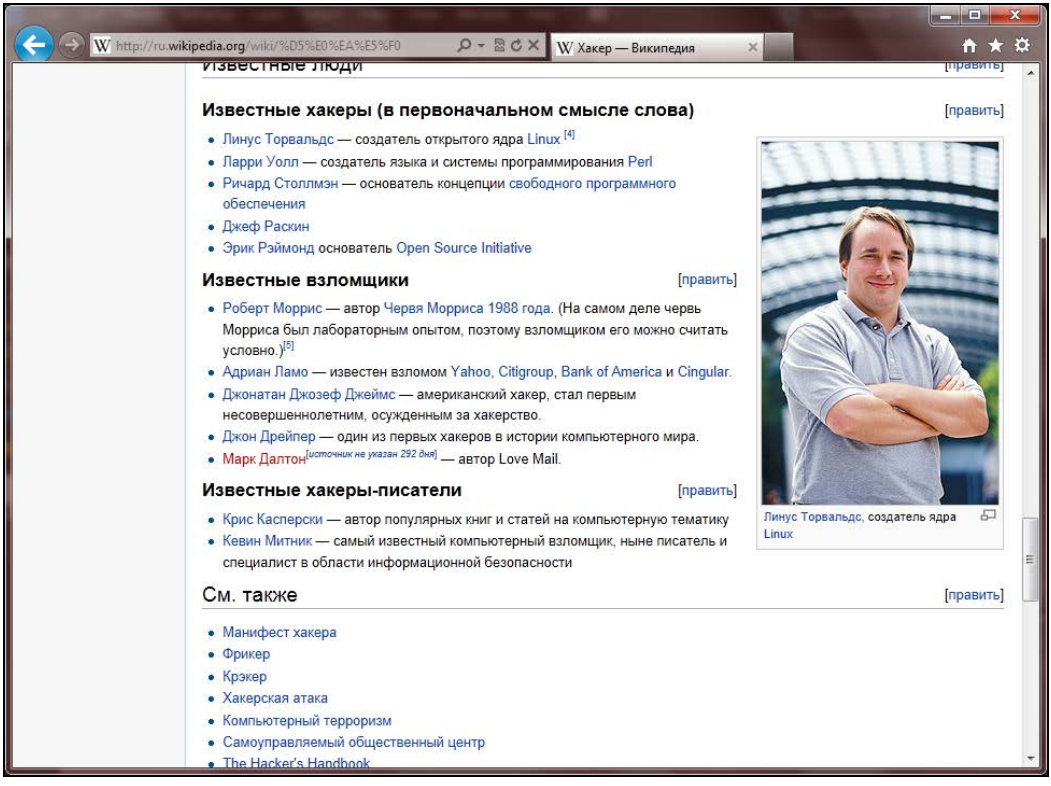


Рис. В1. Известный хакер Линус Тррвальдс

Не думаю, что Линус когда-то и что-то взламывал, но очень много людей, которые разделяют мою точку зрения, без сомнений назовут его хакером. Я понимаю, что энциклопедия Wiki не всегда показательна и тем более, не является законом, потому что ее пишут люди, которые могут ошибаться. Но все же в целом эту энциклопедию рецензирует большое количество людей.

Так, самое главное — существует множество понятий и ни одно из них не является единственным верным. Но я считаю правильной мою точку зрения и именно с этой точки пишу эту книгу. Надеюсь, что мы смотрим на мир с одной и той же позиции, и тогда вам эта книга понравится.

Как стать хакером?

Этот вопрос задают себе многие, но точного ответа вам не даст никто. Есть ответы, которые могут нравиться, но реальность намного более сурова. Данная книга не сделает из вас хакера, как никто не сможет этого сделать. Только труд сотворил из обезьяны человека, и только работа сделает из простого юзера элитного хакера.

Нужно просто как можно больше изучать, читать, пробовать, практиковаться. Желательно общение с другими людьми, потому что обмен опытом — наиболее важный ресурс информации. Не ограничивайтесь только одним автором книг или только одной книгой. Прочитав лишь эту книгу, вы познакомитесь с опытом и узнаете мнение только одного автора, но оно не всегда является лучшим. Аккумулируйте информацию, анализируйте и принимайте решение сами.

Я всегда люблю говорить: "не стоит тупо делать что-то, потому что это тупо". Прежде чем что-то сделать, желательно все же подумать самому, а не доверяться какой-то книжке (даже этой) или автору. Не доверяйте мне, потому что я сам себе не доверяю, пробуйте сами и проверяйте, и тогда вы получите неоценимый опыт, который пригодится в будущем.

В этой главе мы постараемся выделить некоторые общие аспекты, но все зависит от конкретной области, в которой вы хотите стать лучшим. Да, существует множество областей безопасности и хакерства, вот только некоторые:

- сетевой — рассматривает безопасность сетевых протоколов и интернет-приложений;
- кернел (kernel) — ядро ОС, переполнения буфера, ошибки выполнения программ;
- криптография — вопросы и проблемы безопасности шифрования, стойкости и передачи зашифрованных данных;
- веб-сайты — это отдельный класс безопасности, который мне интересен больше всего;
- вирусы — этот класс мне интересен меньше всего. Во времена MS-DOS мне было интересно экспериментировать с системой, и я даже пробовал написать вирус, но дальше размножения дело не дошло, потому что мне это показалось очень скучным и глупым занятием;

- программный — сюда бы я отнес как безопасность программ, так и стойкость ко взлому авторизации/проверки ключей.

Названия и классификацию я придумал сейчас налету, потому что делить области можно как угодно и по какому угодно признаку. Смысл тут в том, что стать специалистом в разных областях одновременно очень и очень сложно. Уж слишком разные нужны тут знания.

Сравним компьютерного специалиста со строителем. В каждой профессии существует некая специализация (разная направленность). Хорошим строителем может быть отличный каменщик или штукатур. Точно также и хакером может быть специалист по операционным системам (например, UNIX) или программист (приложений или веб-сайтов). Все зависит от ваших интересов и потребностей.

После выхода первого издания книги ко мне пришло несколько писем, в которых читатели были недовольны тем, что я в своей книге не уделил внимание вирусам/взлому программ или чему-то еще, и поэтому слово "хакер" на обложке не должно находиться. Видимо, авторы писем ограничены только одной областью хакерства, но тут все намного сложнее.

Итак, вот некоторые рекомендации, которые помогут вам стать настоящим хакером и добиться признания со стороны друзей и коллег.

1. Вы должны знать свой компьютер и научиться эффективно им управлять. Если вы будете еще и знать в нем каждую железку, то это только добавит к вашей оценке большой и жирный плюс.

   Что я подразумеваю под умением эффективно управлять своим компьютером? Это значит знать все возможные способы для выполнения каждого действия и в каждой ситуации уметь использовать наиболее оптимальный из них. В частности вы должны научиться пользоваться "горячими" клавишами и не дергать мышь по любому пустяку. Нажатие клавиши выполняется быстрее, чем любое, даже маленькое перемещение мыши. Просто приучите себя к этому, и вы увидите все прелести работы с клавиатурой.

   Лично я использую мышь очень редко и стараюсь всегда применять клавиатуру. Если быть точнее, то дома я вообще не использую мышь, потому что у меня ее нет. Дома я использую ноутбук и touch pad.

   Маленький пример на эту тему. У меня был один начальник, который всегда копировал и вставлял данные из буфера обмена с помощью кнопок на панели инструментов или команд контекстного меню, которое появляется при щелчке правой кнопкой мыши. Но если вы делаете так же, то, наверное, знаете, что не везде есть кнопки **Копировать**, **Вставить** или соответствующие пункты в контекстном меню. В таких случаях мой начальник набирает текст вручную. А ведь можно было бы воспользоваться копированием/вставкой с помощью "горячих" клавиш <Ctrl>+<C>/<Ctrl>+<V> или <Ctrl>+<Ins>/<Shift>+<Ins>, которые достаточно универсальны, а их работа реализована практически во всех современных приложениях (даже там, где не предусмотрены кнопки и меню).

   За копирование и вставку в стандартных компонентах Windows (строки ввода, текстовые поля) отвечает сама операционная система, и тут не нужен дополни-

тельный код, чтобы данные операции заработали. Если программист не предусмотрел кнопку, то это не значит, что данное действие не предусмотрено вовсе. Оно есть, но доступно через "горячую" клавишу. Если соответствующие "горячие" клавиши не переопределены в программе (им не даны другие действия), то команды будут работать.

Еще один пример. Я работал программистом на крупном предприятии (более 20 000 работников). Моей задачей было создать программу ведения базы данных для автоматизированного формирования отчетности. Большое количество параметров набиралось вручную, и для этого использовались операторы. Первый вариант программы работал без "горячих" клавиш, и для ввода данных требовалось 25 операторов. После внедрения "горячих" клавиш производительность возросла, и с программой работало уже менее 20 операторов. Экономия заметна даже без увеличительного стекла.

2. Вы должны досконально изучать все, что вам интересно о компьютерах. Если вас интересует графика, то вы должны освоить лучшие графические пакеты, научиться рисовать в них любые сцены и создавать самые сложные миры. Если вас интересуют сети, то старайтесь узнать о них все. Если вы считаете, что познали уже все, то купите более толстую книгу по данной теме, и вы поймете, что сильно ошибались. Компьютеры — это такая сфера, в которой невозможно знать все!!! Даже в отдельно взятой области очень тяжело быть всезнающим специалистом.

   Хакеры — это, прежде всего, профессионалы в каком-нибудь деле. И тут даже не обязательно должен быть компьютер или какой-то определенный язык программирования. Хакером можно стать в любой области, но мы в данной книге будем рассматривать только компьютерных хакеров.

3. Желательно уметь программировать. Любой хакер должен знать как минимум один язык программирования. А лучше даже несколько языков. Лично я рекомендую всем изучить для начала Borland Delphi или C++. Borland Delphi достаточно прост, быстр, эффективен, а главное, это очень мощный язык. C++ — признанный стандарт во всем мире, но немного сложнее в обучении. Но это не означает, что не надо знать другие языки. Вы можете научиться программировать на чем угодно, даже на языке Basic (хотя использовать его не советую, но знать не помешало бы).

   По ходу изучения книги вы увидите, что без навыков программирования некоторые приемы были бы невозможны. Используя готовые программы, написанные другими хакерами, вы можете стать только взломщиком, а для того чтобы стать хакером, нужно научиться создавать свой код.

   Хакер — это творец, человек, который что-то создает. В большинстве случаев это касается кода программы, но можно создавать и графику, и музыку, что тоже относится к искусству хакера.

4. Не тормозите прогресс. Хакеры всегда боролись за свободу информации. Если вы хотите быть хакером, то тоже должны помогать другим. Хакеры обязаны способствовать прогрессу. Некоторые делают это через написание программ с открытым кодом, а кто-то просто делится своими знаниями.

Открытость информации не означает, что вы не можете зарабатывать деньги. Это никогда не возбранялось, потому что хакеры тоже люди, хотят кушать и должны содержать свою семью. Самое главное — это созидание. Вот тут проявляется еще одно отличие хакеров от крэкеров: хакеры "создают", а крэкеры "уничтожают" информацию. Если вы написали какую-нибудь уникальную шуточную программу, то это вас делает хакером. Но если вы изобрели вирус, который с улыбкой на экране уничтожает диск, то вы — крэкер-преступник.

В борьбе за свободу информации может применяться даже взлом, но только не в разрушительных целях. Вы можете взломать какую-либо программу, чтобы посмотреть, как она работает, но не убирать с нее систем защиты. Нужно уважать труд других программистов, не нарушать их авторские права, потому что защита программ — это их хлеб.

Представьте себе ситуацию, если бы вы украли телевизор. Это было бы воровство и преследовалось бы по закону. Многие люди это понимают и не идут на преступления из-за боязни наказания. Почему же тогда крэкеры спокойно ломают программы, не боясь закона? Ведь это тоже воровство. Лично я приравниваю взлом программы к воровству телевизора с полки магазина и считаю это таким же правонарушением.

При этом вы должны иметь право посмотреть на код купленной программы. Ведь вы же можете вскрыть свой телевизор, и никто не будет вас преследовать по лицензионным соглашениям. Кроме того, вас же не заставляют регистрироваться, когда вы честно приобрели товар, как делают это сейчас с активацией.

Когда я говорю, что вы должны иметь право посмотреть на код, я не призываю писать и использовать только проекты с открытым исходным кодом. Ни в коем случае. Можно смотреть во внутренности программ с помощью дизассемблеров. На ассемблере читать код программ намного сложнее, но тут будет самое настоящее соединение с хакерской культурой (как красиво сказал, аж сам не верю).

Я понимаю разработчиков программ, которые пытаются защитить свой труд. Я сам программист и продаю свои программы. Но я никогда не делаю сложных систем защиты, потому что любые попытки "предохранения" усложняют жизнь законопослушным пользователям, а крэкеры все равно их обойдут. Какие только "замки" не придумывали крупные корпорации, чтобы защитить свою собственность, но crack существует на любые программы, и большинство из них взломано еще до официального выхода на рынок. С нелегальным распространением программ нужно бороться другими методами, а системы активации или ключей бесполезны.

В цивилизованном мире программа должна иметь только простое поле для ввода некоего кода, подтверждающего оплату, и ничего больше. Не должно быть никаких активаций и сложных регистраций. Но для этого и пользователи должны быть честными, потому что любой труд должен оплачиваться. А то, что какой-то товар (программный продукт) можно получить бесплатно, это не значит, что вы должны это делать.

5. Знайте меру. Честно сказать, я уважаю Билла Гейтса за то, что он создал Windows и благодаря этой операционной системе сделал компьютер доступным для каждого в этом мире. Если раньше пользоваться компьютерами могли только люди с высшим образованием и математическими способностями, то теперь он доступен каждому ребенку.

   Единственное, что я не приветствую, — это методы, которыми продвигается Windows на компьютеры пользователей. Мне кажется, что уже давно пора ослабить давление, и Windows наоборот станет более популярной, а у многих пропадет ненависть к корпорации и ее руководству. Хотя судя по последним тенденциям именно это и происходит.

   Нельзя просто так лишать денег другие фирмы только из-за того, что ты проиграл конкуренцию, как это произошло с Netscape Navigator. Тогда Microsoft не удалось победить фирму Netscape в честной борьбе, и Microsoft сделала свой браузер бесплатным, потому что у корпорации достаточно денег, и она может себе это позволить. Но почему нельзя было просто уйти от борьбы и достойно принять проигрыш? Ведь доходы фирмы от перевода браузера на бесплатную основу не сильно увеличились, а интеграция Internet Explorer в ОС — чистый фарс.

6. Не изобретайте велосипед. Тут опять действует созидательная функция хакеров. Они не должны стоять на месте и обязаны делиться своими знаниями. Например, если вы написали какой-то уникальный код, то поделитесь им с ближними, чтобы людям не пришлось создавать то же самое. Вы можете не выдавать все секреты, но должны помогать другим.

   Ну а если вам попал чужой код, то не стесняйтесь его использовать (с согласия хозяина!). Не выдумывайте то, что уже сделано и обкатано другими пользователями. Если каждый будет изобретать колесо, то никто и никогда не создаст повозку, и тем более автомобиль.

7. Хакеры — не просто отдельные личности, а целая культура с собственными магическими заклинаниями и танцами с бубнами, которые позволяют добиться нужного результата (например, заставить программу работать). Но это не значит, что все хакеры одеваются одинаково и выглядят на одно лицо. Каждый из них — отдельный индивидуум, и не похож на других. Не надо копировать другого человека. Удачное копирование не сделает вас продвинутым хакером. Только ваша индивидуальность может сделать вам имя.

   Если вы известны в каких-либо кругах, то это считается очень почетным. Хакеры — это люди, добывающие себе славу своими познаниями и добрыми делами. Поэтому любого хакера должны знать.

   Как определить, являетесь ли вы хакером? Очень просто, если о вас говорят, как о хакере, то вы один из них. Жаль, что этого добиться очень сложно, потому что большинство считает хакерами взломщиков. Поэтому, чтобы о вас заговорили как о хакере, нужно что-то взломать или уничтожить. Но это неправильно, и не надо поддаваться на этот соблазн. Старайтесь держать себя в рамках дозволен-

ного и добиться славы только хорошими делами. Это намного сложнее, но что поделаешь... Никто и не обещал, что будет просто.

8. Чем отличаются друг от друга программист, пользователь и хакер? Программист, когда пишет программу, видит, какой она должна быть, и делает на свое усмотрение. Пользователь не всегда знает, что задумал программист, и использует программу так, как понимает.

   Программист не всегда может предугадать действия своих клиентов, да и приложения не всегда тщательно оттестированы. Пользователи имеют возможность ввести параметры, которые приводят к неустойчивой работе программ.

   Хакеры намеренно ищут в программе лазейки, чтобы заставить ее работать неправильно, нестабильно или необычно. Для этого требуется воображение и нестандартное мышление. Вы должны чувствовать исполняемый код и видеть то, чего не видят другие.

   Если вы нашли какую-то уязвимость, то необязательно ее использовать. Об ошибках лучше сообщать владельцу системы (например, администрации сайта). Это весьма благородно, а главное, — создаст вам имя, и при этом можно не опасаться оказаться в зале суда. Хотя, те, кто оказываются в суде, быстрее получают популярность, потому что о таких людях пишут в газетах и им начинают подражать "чайники". Но кому в тюрьме нужно признание общественности? Мне оно абсолютно не нужно. Тем более что после отбывания срока очень часто тяжело найти себе работу. Мало кто захочет содержать в штате бывшего преступника, да и после пребывания в местах не столь отдаленных могут еще долго не разрешать пользоваться любимыми компьютерами. Лучше быть здоровым и богатым, т. е. пусть не знаменитым, но на свободе.

Некоторые считают, что правильно надо произносить "хэкер", а не "хакер". Это так, но только для английского языка. У нас в стране оно обрусело и стало "хакером". Мы — русские люди, и давайте будем любить свой язык и признавать его правила. Хотя, некоторые читатели могут быть и с Украины, Белоруссии и других стран бывшего СНГ, и тогда произносите это слово так, как уже устоялось в вашем языке, и не копируйте с американцев.

Тут же возникает вопрос: "Почему же автор относит к хакерскому искусству компьютерные шутки и сетевые программы?" Попробую ответить на этот вопрос. Во-первых, хакеры всегда пытались доказать свою силу и знания методом написания каких-либо интересных, веселых программ. К этой категории я не отношу вирусы, потому что они несут в себе разрушение, хотя они тоже бывают с изюминкой и юмором. Зато простые и безобидные шутки всегда ценились в узких кругах.

Мне кажется, что в ИТ-областях вообще очень хорошо с чувством юмора, и хакеры — не исключение, чтобы писать только серьезные вещи. Поэтому не будем ботаниками, а будем чаще улыбаться, это полезно для кожи лица, чтобы не было морщин.

Таким способом хакер демонстрирует не только знания особенностей операционной системы, но и старается заставить ближнего своего улыбнуться. Так как многие

хакеры обладают хорошим чувством юмора, и он поневоле ищет своего воплощения во всем. Я советую шутить с помощью безобидных программ, потому что юмор должен быть здоровым.

Пользуйтесь собственным умом

Читать чужие идеи и мысли очень хорошо и полезно, потому что, изучая опыт других людей, можно узнать много нового. Но с другой стороны, не стоит принимать все на веру без самостоятельного анализа. Даже эту книгу нужно профильтровать через собственный мозг, потому что я где-то могу ошибаться или заблуждаться.

Вы также должны понимать необходимость использования различных технологий. Я по образованию экономист-менеджер и 6 лет проучился в институте по этой специальности. Но даже до этого я знал, что заказчик всегда прав. Почему-то в компьютерной области стараются избавиться от этого понятия. Например, Microsoft пытается заставить программистов писать определенные программы, не объясняя, зачем это нужно пользователям. Многие тупо следуют этим рекомендациям и не задумываются о необходимости того, что они делают.

Тут же приведу простейший пример. Совсем недавно все программисты вставляли в свои продукты поддержку XML, и при этом никто из них не задумывается о целесообразности этого. А ведь не всем пользователям этот формат нужен, и не во всех программах он востребован. Следование рекомендациям не означает правильность действий, потому что заказчик — не Билл Гейтс, а ваш потребитель. Поэтому надо всегда делать то, что требуется конечному пользователю. А если заказчику не нужен XML, то не надо и внедрять его поддержку в программу.

Сейчас нас зомбируют с экранов телевизоров и интернет-сайтов облачными технологиями и тучами. А оно вам нужно? Придумали какие-то красивые слова, а все это как было клиент-серверной технологией, так и осталось. Если нужны интернет-вычисления, то используйте интернет-серверы, а как вы их назовете — облако, туча или мясорубка, клиенту все равно. Не обязательно задействовать сложные системы, которые строят Amazon и Microsoft, когда нужен всего лишь веб-сайт или небольшой веб-сервис.

Я рекомендую не обращать особого внимания на корпорацию Microsoft (хотя некоторые ее разработки гениальны), потому что считаю определенные ее действия тормозом прогресса. И это тоже можно доказать на примере. Сколько технологий доступа к данным придумала Microsoft? Просто диву даешься: DAO, RDO, ODBC, ADO, ADO.NET, и это еще не полный список. Корпорация Microsoft регулярно выкидывает на рынок что-то новое, но при этом сама этим не пользуется. При появлении новой технологии все программисты кидаются переделывать свои программы под новоиспеченный стандарт и в результате тратят громадные ресурсы на постоянные переделки. Таким образом, конкуренты сильно отстают, а Microsoft движется вперед, потому что не следует своим собственным рекомендациям и ничего не переделывает. Если программа при создании использовала для доступа к данным DAO, то можно спокойно оставить ее работать через DAO, а не переделывать на

ADO, потому что пользователю все равно, каким образом программа получает данные из базы, главное, чтобы данные были вовремя и качественно.

Могу привести более яркий пример — интерфейс. В программах, входящих в пакет MS Office, постоянно меняется интерфейс, и при этом всем говорят, что именно он самый удобный для пользователя и именно за ним будущее. Все бегут переводить свои программы на новый внешний вид меню и панелей, а тот же Internet Explorer и многие другие программы выглядят, как 10 лет назад, в них практически ничего не меняется. Microsoft не тратит на это время, а конкуренты месяцами переписывают множество строчек кода.

Да, следование моде придает вашим программам эффектность, но при этом вы должны суметь сохранить индивидуальность.

Компания Microsoft постоянно что-то переписывает и переделывает в спецификациях, но при этом сама очень сильно топчется на месте и программы меняет только по мере необходимости. В этом смысле Apple поступила мудрее и постоянно движется вперед. Если на настольных системах яблочный гигант пока отстает, но на мобильном рынке он с большим отрывом обошел Microsoft и заставил конкурента шагнуть не то, что на шаг назад, а отступить к самому началу. Мобильная платформа MS была практически полностью переписана и запущена с нуля под новым именем Windows Phone без совместимости с предыдущей платформой Windows Mobile.

Возможно, сложилось впечатление, что я противник Microsoft, но это не так. Мне очень нравятся некоторые ее продукты, например Windows, Office, C#, Visual Studio или MS SQL Server, но я не всегда согласен с ее методами борьбы с конкурентами. Это жестокий бизнес, но не до такой же степени.

Программисты и хакеры навязывают другим свое мнение о любимом языке программирования, как о единственно приемлемом, обычно добиваясь успеха, потому что заказчик часто не разбирается в программировании. На самом же деле заказчику все равно, на каком языке вы напишете программу, его интересуют только сроки и качество.

Если я могу обеспечить минимальные сроки написания приложения, сохраняя хорошее качество, работая на Borland Delphi, то я буду использовать его. Такое же качество на C++ я (да и любой другой программист) смогу обеспечить только в значительно большие сроки. Правда сейчас я нашел для себя другой язык программирования, который мне больше подходит — C#, и с его помощью я пишу свои нынешние проекты.

Вот когда заказчик требует минимальный размер или наивысшую скорость работы программы, тогда я берусь за C (не путать с C++) и ASM (встроенный ассемблер). Но это бывает очень редко (последний раз было, наверное, лет 6 назад), потому что сейчас носители информации уже практически не испытывают недостатка в размерах, и современные компьютеры работают в миллионы раз быстрее своих предшественников. Таким образом, размер и скорость программы уже не являются критичными, и на первый план выдвигаются скорость получения готового продукта и качество выполнения заказа.

Какие требования перед вами ставят, такие требования и выполняйте. Не пытайтесь забивать гвозди отверткой, используйте молоток. Точно так же и при выборе программных продуктов, с помощью которых вы будете реализовывать задачу — нужно выбирать то, что подходит лучше, а не то, что круче.

Предыстория

Чтобы лучше понимать мир хакера, нужно оглянуться назад и увидеть, как все развивалось, начиная с зарождения Интернета и появления первых хакерских программ, первых взломов и т. д.

В 1962-м году директор агентства ARPA (Advanced Research Projects Agency, Управление передовых исследовательских проектов) Дж. С. Р. Ликлидер (J. C. R. Licklider) предложил в качестве военного применения компьютерных технологий использовать имеющиеся компьютеры, взаимосвязанные выделенной линией. Целью такого применения компьютеров стало создание распределенных коммуникаций. А в основу ноу-хау был положен принцип функционирования системы, устойчивой к отказам линий связи. Благодаря этому ключевым направлением исследований агентства стали компьютерные сети. Это время можно назвать началом появления сети ARPANET (Advanced Research Projects Agency NETwork, сеть коммутации пакетов).

С этой ошибки и началось развитие Интернета. Почему ошибки? В основу был положен принцип функционирования системы при отказе отдельных ее блоков, т. е. уже в самом начале заложили вероятность отказа отдельных компонентов!!! Во главу угла должна была стать безопасность системы, ведь она разрабатывалась для военных нужд США. Но как раз на этот аспект никто не обращал внимания. И это понятно, ведь компьютеры были доступны только профессионалам, о домашних компьютерах только мечтали. А о том, чтобы подключить домашний компьютер к сети, использовавшейся для военных и исследовательских целей, никто и не задумывался. Дальше еще хуже.

Разные специалисты признают различные события как рождение сети. В различных источниках можно найти даты, начиная с 1965 до 1970 года. Но многие признали 1969 год — период появления ARPANET, и именно тогда зарождается ОС UNIX, на основе которой и создавался Интернет в ближайшие десятилетия.

В начале 70-х годов ARPANET стала расширяться и объединять различные исследовательские институты. Сеть вышла за пределы одного здания и начала опутывать США. Изначально никто даже не предполагал, что рост пойдет такими быстрыми темпами и сеть объединит такое большое количество компьютеров. Поэтому первые технологии, которые использовались для связи и обмена данными, устарели в течение первых 10 лет.

С 1970 года начинается десятилетие фрикеров. Их тоже относят к категории хакеров, хотя они напрямую не связаны с компьютерами. Основное направление их деятельности — телефоны, услуги по использованию которых стоили дорого, поэтому молодые ребята (и не очень молодые, и иногда не очень ребята :)) старались

снизить эти затраты. Не знаю, какие расценки сейчас в США, а в Канаде до сих пор цены на телефонную связь очень высокие. Домашняя линия стоит минимум 10 долларов, а хороший безлимитный тариф — 30 долларов. Сотовая связь так же очень дорогая. Средняя стоимость разговора в месяц обходится в 70 долларов на одну телефонную линию.

Эпоху фрикеров начинают отсчитывать с момента, когда компания Bell опубликовала в журнале "Technical Assistance Program" частоты тональных сигналов, которыми управляется телефонная сеть. В 1971 году появилась "синяя коробка" (Blue Box), с помощью которой можно было генерировать сигналы нужных тонов. Следующие 10 лет такие коробки позволили экономить людям немалые деньги на телефонных разговорах, телефонные компании стали терять деньги. После 1980 года эта болезнь начинает проходить, потому что фрикеров начали активно ловить, и это стало небезопасно.

Среди фрикеров были замечены достаточно знаменитые личности, например основатели Apple Computers. Они продавали студентам электронные приборы, среди которых были и "синие коробки".

В 1972 году появилось первое приложение для передачи электронных сообщений, а через год сеть вышла за пределы США, и к ней подключились компьютеры из Англии. В том же году начались первые разговоры и предложения по построению международной сети.

Только в 1981 году был создан Defence Security Center (DSC, центр компьютерной безопасности министерства обороны США). Этот центр должен был определить степень пригодности предлагаемых систем для их ведомства.

16 декабря 1981 года начался судебный процесс против самого знаменитого фрикера Льюиса де Пейна, более известного под кличкой Роско. В этом же деле участвовал и известный хакер Кевин Митник, но ему повезло, — тогда он проходил в качестве свидетеля. Не прошло и года, как знаменитый хакер попался на другом деле и все же сел в тюрьму для подростков.

В 1982 году в основу Интернета был положен протокол передачи данных TCP/IP (Transmission Control Protocol/Internet Protocol). Количество хостов росло, а для обращения к компьютерам использовались их адреса. С появлением TCP/IP началась разработка DNS (Domain Name System, система доменных имен), что позволило обращаться к компьютерам по именам, а система сама переводила их в адреса компьютеров.

Несмотря на то, что к этому времени мир уже узнал о том, что компьютерные технологии могут быть опасны, протокол TCP разрабатывался как открытый и с большим количеством недостатков с точки зрения безопасности. И только при разработке IPv6 безопасности было уделено достаточно много внимания.

1983 год возвращает Кевину Митнику свободу. Но ненадолго, потому что руки хакера тянутся к взлому, и он снова попадается, из-за чего ему приходится скрываться вплоть до 1985 года.

В 1984 году система DNS вводится в эксплуатацию. Проходит еще четыре года, и весь мир узнает, что существует угроза червя. В 1988 году происходит одно из са-

мых масштабных заражений "червем" компьютеров, подключенных к Интернету. Молодой выпускник Корнельского университета по имени Роберт Моррис, являющийся сотрудником фирмы Digital, пишет программу-"червя", которая должна была самостоятельно перемещаться по сети и заражать файлы всех взломанных компьютеров.

Для внедрения на чужой компьютер "червь" использовал подбор пароля. В теле программы находилось несколько наиболее часто употребляемых паролей, и именно они применялись для проникновения в другой компьютер. Если напрямую пароль не удавалось подобрать, то подключался системный словарь слов. Таким простым способом было взломано более 7% всех компьютеров в сети. Это достаточно большая цифра. "Червь" был запущен по случайной ошибке, и его код еще не был закончен. Трудно предположить последствия, если бы Роберт Моррис смог дописать программу до конца.

Но и это еще не все. 1988 год оказался самым продуктивным с точки зрения взлома и громких судебных дел. Именно в этом году в очередной раз был пойман Кевин Митник, и на этот раз он уже надолго был отлучен от компьютеров.

Начиная с 1990 года, сеть ARPANET перестает существовать, потому что ее просто съедает Интернет. Всемирная сеть начинает поглощать все отдельные сети.

В 1991 году мир первый раз увидел веб-страницы, без которых сейчас уже никто не может себе представить Всемирную сеть. Интернет-сообщество начинает смотреть на сеть по-новому. В том же году появляется одна из самых мощных систем шифрования — PGP (Pretty Good Privacy, набор алгоритмов и программ для высоконадежного шифрования сообщений с использованием открытых ключей), которая постепенно становится стандартом в большинстве областей, в том числе и в шифровании электронных сообщений e-mail.

В 1994 году количество пользователей Интернета уже исчисляется миллионами. Чтобы народ не просиживал за монитором зря, предпринимаются первые попытки полноценной коммерческой деятельности через сеть, которая постепенно перестает быть исключительно инструментом для обмена информацией, теперь это еще и средство рекламы и способ продвижения товара в массы.

В 1995 году регистрация доменных имен перестает быть бесплатной, и начинается эра войны за домены. Хакеры стремятся скупить все доменные имена, похожие на торговые марки, или просто легко запоминающиеся слова. Компании, которые хотят, чтобы доменное имя совпадало с их торговой маркой, тратят большие деньги для их выкупа.

Этот же год стал знаменит и тем, что я купил себе модем и влился в Интернет. До этого я появлялся в сети очень редко и ненадолго, потому что для меня это было слишком дорогое удовольствие.

Итак, на такой деловой ноте мы закончим вводную лекцию и перейдем к практическим упражнениям по воинскому искусству, где часто главное — это скрытность и победа минимальными силами.

ГЛАВА 1

Интересные настройки Windows

Будем двигаться от очень простого к простому, ведь все на самом деле очень примитивно, если не усложнять себе жизнь. Поэтому после прочтения книги даже на те вопросы, на которые вы не знали ответа, вы сможете воскликнуть: "Как же это было просто!" Я ничего особого изобретать не намерен, а просто соберу интересные (на мой взгляд) темы относительно компьютера в одной книге. И начнем мы с интерфейса ОС Windows и его программ.

Когда я первый раз познакомился с Windows 95, то понял, что полюбил эту ОС по самые иконки. Несмотря на то, что она была нестабильна и выдавала синие экраны, да и переустанавливать ее приходилось раз в пару месяцев, в ней было очень много удобных для простого пользователя и заядлого хакера вещей.

С появлением следующих версий, таких как Windows 98, 2000, моя любовь только укреплялась. С каждой новой версией система усложнялась, и появлялись новые, интересные возможности для выражения своей индивидуальности. Нестабильность и проблемы иногда склоняли меня установить Linux и работать в нем, но с появлением Windows XP я понял, что ни о каком дистрибутиве в "красной шапке" можно больше и не думать. Лучше заплатить подороже, но получить отличную, удобную и стабильную систему. Главное — подойти с правильной стороны и все строго настроить. А тут есть где "разгуляться", и не только для повышения надежности, но и с целью улучшения внешнего вида.

Начиная с Windows Vista, количество интересных изменений, которые можно выполнить в визуальном интерфейсе, сильно сократилось, поэтому и эта глава сильно изменилась по сравнению с предыдущими изданиями. На момент написания этих строк во всем мире семимильными шагами идет переход на Windows 7, а через год нам обещают еще одну новую версию — Windows 8. Архитектурно Windows уже не должна так сильно меняться, как это произошло при переходе с Windows XP на Vista, поэтому бóльшая часть описываемого здесь может быть применима и в ближайших будущих версиях ОС от Microsoft.

Но вернемся к Linux, который я только что упомянул. Если честно, то в Linux я иногда посиживаю, но в последнее время все реже и реже. Процентов 90 своего

компьютерного времени я провожу непосредственно в Windows, и только 10 процентов уходит на Linux в его различных проявлениях.

В предыдущем издании эта глава содержала много информации, касающейся Windows XP и IE версии 6.0, которые сейчас используются все меньше и меньше. Я думаю, что к моменту выхода книги на полки магазинов количество компьютеров на Windows XP сократится еще сильнее, поэтому оставлять устаревшую информацию не имеет смысла. Но чтобы не терять ее вовсе, я вынес все, что касается Windows XP и Internet Explorer до версии 7, в архив, который можно найти на FTP-сервере издательства (см. **ftp://85.249.45.166/9785977507905.zip**, ссылка доступна также со страницы книги на сайте **www.bhv.ru**). Ищите там множество дополнительной информации в папке Doc.

В этом издании я решил значительно сократить этот раздел, потому что параметры постоянно изменяются, и не хотелось бы, чтобы большая часть книги устарела уже завтра. Вместо этого мы рассмотрим наиболее интересные настройки системы.

1.1. Internet Explorer

Большинство программ устанавливается с настройками по умолчанию. И если в основном производители программного обеспечения предоставляют к своим настройками полный визуальный интерфейс, то Microsoft почему-то решила не делать этого. Не все настройки можно изменить визуально в окне параметров, иногда приходится изменять что-то напрямую в реестре. Как любит говорить qa (quality assurance), с которым я сотрудничаю сейчас на работе: "Don’t ask me why it works this way". Реально, иногда очень сложно объяснить, почему менеджеры проектов или разработчики приняли именно такое решение.

Популярный (пока еще) в Windows-мире браузер Internet Explorer, который устанавливается с ОС по умолчанию, грешит такой же проблемой. У него далеко не все параметры можно изменять в окне настроек. Некоторые (иногда очень интересные и полезные параметры) доступны для изменения только напрямую в реестре.

1.1.1. Убить нельзя, помиловать

Среди настроек есть такой параметр, который запрещает пользователю закрывать окна Internet Explorer. Во время путешествия в сети на многих сайтах выскакивает масса всплывающих окон, которые засоряют экран. Если использовать возможность такой настройки, то окна будут только плодиться, а при попытке закрытия появится окно с предупреждением, как на рис. 1.1.

Чтобы сделать Internet Explorer незакрываемым, нужно перейти в реестре в раздел **HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Restrictions**. Этот путь может отсутствовать, и нужно будет добавить недостающие разделы. Для этого достаточно щелкнуть правой кнопкой мыши на нужном разделе и в появившемся меню выбрать **Создать | Раздел** (New | Key). Например, если у вас существует только путь **HKEY_CURRENT_USER\Software**

Policies\Microsoft, то щелкните правой кнопкой на строке **Microsoft** и создайте раздел **Internet Explorer**, а затем в нем — **Restrictions**. Когда все разделы будут существовать, создайте параметр **NoBrowserClose** типа `DWORD` и со значением `1`.

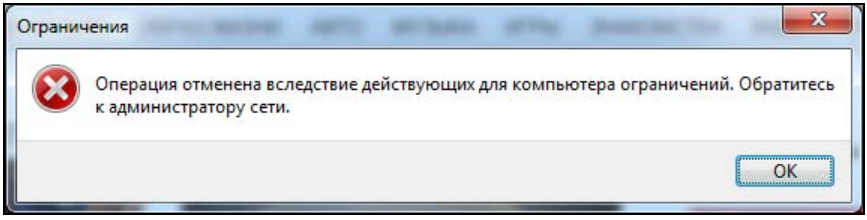


Рис. 1.1. Предупреждение о невозможности закрытия окна IE

Все эти действия можно проделать на компьютере своего друга и посмотреть за его реакцией, когда он попытается закрыть окно. Я однажды подшутил так над своими коллегами по работе. Реакция их была разнообразной. Большинство посчитало, что это было вмешательство вируса.

Чтобы внести все эти изменения на компьютере пользователя, нужно достаточно много времени, а его может и не быть. Чтобы сделать все быстро и незаметно, можно поступить следующим образом:

1. Внести изменения сначала в свой компьютер.
2. Выполнить экспорт файла реестра с опцией **Выбранная ветвь** (в данном случае ветвь **HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Restrictions**).
3. Записать получившийся файл на флешку.

Теперь идите к компьютеру пользователя, над которым вы намереваетесь подшутить, и говорите, что хотите что-то показать. Вставляете флешку и запускаете файл с расширением reg. Вся необходимая информация будет автоматически добавлена. Не надо больше ничего делать, даже запускать Internet Explorer. Просто скажите, что это не та флешка, и уходите. Ждите, пока пользователь сам не запустит браузер и не встретится с проблемой закрытия программы.

Мне интересно узнать, чем руководствовался тот человек, который придумал ограничение, запрещающее закрывать IE? Я бы с удовольствием поговорил бы с этим человеком, чтобы узнать, для чего это было сделано. А те, над кем подшутили подобным образом, наверно открутили бы нерадивому разработчику голову.

Этот параметр существовал в IE6, и я думал, что его добавили по глупости и уберут из Internet Explorer уже в 7-й версии. Сегодня я проверил 9-ю версию и трюк все еще работает. Немного странно он начинает работать, совсем не сразу. Видимо, браузер кеширует свои параметры и не читает их каждые пять минут или при каждом запуске. Я даже сначала подумал, что параметр не работает, и уже собирался удалить этот раздел из книги. Но прошло некоторое время и я не смог закрыть браузер, а раздел вернулся в книгу.

1.1.2. Количество потоков для скачивания

По умолчанию Internet Explorer очень сильно ограничен в выборе максимального количества подключений из одного процесса к серверу. В зависимости от протокола, версии браузера и подключения это значение может быть от 2 до 6. Конечно же, чем больше установить одновременных подключений между сервером и клиентом, тем лучше и, может быть, даже быстрее. Сервер так же может быть ограничен по скорости на каждое подключение и качать в два и более потока, что способно принести выгоду.

Но если вам значения по умолчанию не достаточно, то его легко можно увеличить и до 10 всего лишь небольшим изменением в реестре.

Открываем редактор реестра regedit и в **HKEY_LOCAL_MACHINE** переходим в ветку **SOFTWARE\Microsoft\InternetExplorer\MAIN\FeatureControl**. Здесь есть два подраздела, которые могут нас заинтересовать:

- **FEATURE_MAXCONNECTIONSPERSERVER** — максимальное количество подключений к серверу по протоколу HTTP 1.1;
- **FEATURE_MAXCONNECTIONSPER1_0SERVER** — максимальное количество подключений к серверу по протоколу HTTP 1.0.

В обоих разделах есть параметр с именем **explorer.exe**, который задает количество одновременных подключений из одного процесса к серверу. Интересно, что для более старого протокола 1.0 это значение равно `4`, а для более нового протокола это значение равняется всего лишь `2`. Почему такая несправедливость? Она связана с тем, что для протокола 1.0 значение выбиралось опытным путем по поведению браузеров. А вот для версии 1.1 количество потоков в 2 было обусловлено стандартом, только вот стандарт разрабатывался в 1997-м году, когда большинство пользователей Интернета работало с сетью через медленные модемы.

В настоящее время большинство работает в Интернете через более скоростные подключения. У меня лично в данный момент два варианта выхода в сеть:

- кабельный Интернет. Коаксиальный кабель подключен к Wi-Fi-роутеру, который может работать на стандартах до 802.11n (150 Мбит/с), а провайдер обещает, что его кабель может обеспечить передачу до 10 Мбит/с в мою сторону и до 512 Кбит/с от меня. Так как скорость определяется самым слабым звеном, то больше 10 Мбит/с на скачивание не будет;
- 3G-модем с Wi-Fi-маршрутизатором в одной коробке (я описывал его здесь **http://www.funniestworld.com/Review.aspx?id=781**) и по заявлениям провайдера он должен работать на скорости до 5,76 Мбит/с.

Даже при самых слабых показателях скорость передачи достаточно высокая, чтобы без проблем качать данные даже в 10 потоков. Именно поэтому Internet Explorer 8 сделали чуть более интеллектуально развитым, и он уже определяет максимальное количество потоков в зависимости от соединения. Если это коммутируемое подключение, то количество подключений определяется в зависимости от протокола — 4 или 2 (не забываем, что это значения по умолчанию в реестре и их можно

изменить). Ну а если это высокоскоростное подключение типа интернет-кабеля или Wi-Fi, то браузер будет использовать значение 6.

Чем больше доступно подключений, тем лучше для таких современных технологий как AJAX, но хуже для сервера. Дело в том, что количество подключений на стороне сервера не безгранично. Все имеет свои пределы, просто они иногда очень большие. Но благодаря современным методам кэширования, использования proxy-серверов и современных веб-серверов этим фактором начинают пренебрегать. Особенно клиенты. Мне как пользователю все равно, какие лимиты на сервере, я хочу получать информацию быстрее.

Обратите внимание, что ключ реестра, который мы сейчас рассматриваем, находится в **HKEY_LOCAL_MACHINE**, и это значит, что его изменение отразится на всех пользователях компьютера. Если вы хотите установить для каждого пользователя отдельные настройки, то можно без проблем создать описанные ранее параметры в ветке **SOFTWARE\Microsoft\InternetExplorer\MAIN\FeatureControl**, но только в **HKEY_CURRENT_USER** для текущего пользователя.

Увеличить количество одновременных подключений можно и с помощью групповых политик. Но это отдельная история, да и управление политиками может отсутствовать на компьютере. Просто они ставятся далеко не со всеми редакциями. Поэтому редактирование параметров реестра напрямую намного эффективнее.

На моей практике 6 является вполне достойным значением. Если сервер работает в нормальном режиме, то он будет обрабатывать и более 6 подключений сам. Ну а если сервер слабый, то изменение параметров не поможет.

Сейчас мы отойдем немного от темы и рассмотрим эту проблему с другой стороны — со стороны веб-сервера. Хотя программирование выходит за рамки книги, информация может быть очень полезной.

Итак, мы уже знаем, что Internet Explorer по умолчанию скачивает максимум 6 файлов одновременно. Если на веб-странице 30 и более картинок, то скачивание может быть достаточно долгим, особенно в браузерах IE до версии 8, если качать максимум две картинки. Если тратить на загрузку каждой пары картинок хотя бы 1 секунду, загрузка 30 будет происходить 15 секунд. Это очень много, потому что пользователи не любят ждать столько времени.

Страница должна появляться максимум через 5 секунд, иначе сайт теряет клиентов. Пять секунд — это максимум, где-то я читал, что пользователи не любят ждать и две секунды, а уходят к конкуренту. Лично я сам тоже не люблю медленные сайты.

Разработчики веб-сайтов используют различные ухищрения для того, чтобы оптимизировать загрузку своих сайтов. Можно создать одну большую картинку, на которой будут находиться все необходимые ресурсы в виде маленьких картинок, а потом с помощью CSS отображать только отдельные части большого холста. Но одна большая картинка неудобна с точки зрения сопровождения. 30 маленьких все же удобнее.

Чтобы браузер смог грузить сразу 20 картинок одновременно, проще использовать следующий трюк: разместить картинки на разных доменах. Каждый хост определя-

ется не адресом (IP), а доменным именем сайта. Например, для веб-страницы **www.flenov.info/blog.php** браузер сможет открыть *X* подключений к домену **www.flenov.info** (где *X* зависит от настроек системы и браузера). Но если половину картинок поместить на **image.flenov.info/images/**, то браузер уже будет думать, что перед ним совершенно другой сервер, и сможет открыть еще *X* соединений к домену **image.flenov.info**, а это значит, что можно качать в два раза больше ресурсов.

Такую оптимизацию очень легко реализовать с помощью DNS. Достаточно только настроить его так, чтобы любые поддомены ***.flenov.info** загружали один и тот же сайт. Что бы вы ни набрали вместо звездочки, на моем сайте все это будет загружать один и тот же мой блог. Я подумываю о том, чтобы использовать поддомены, но на данный момент все работает именно так.

Попробуйте загрузить сайт **www.sonyrewards.com** в FireFox и откройте надстройку FireBug. Эта надстройка позволяет показывать, какие сайты и как загружаются (рис. 1.2). Обратите внимание, что картинки грузятся не с **sonyrewards.com**, а с доменов **image1.sonyrewards.com**, **image2.sonyrewards.com** или **image3.sonyrewards.com**. Ресурсов у сайта много, но за счет того, что практически все браузер может грузить одновременно, сайт грузится достаточно быстро даже у тех, кто использует параметры по умолчанию.

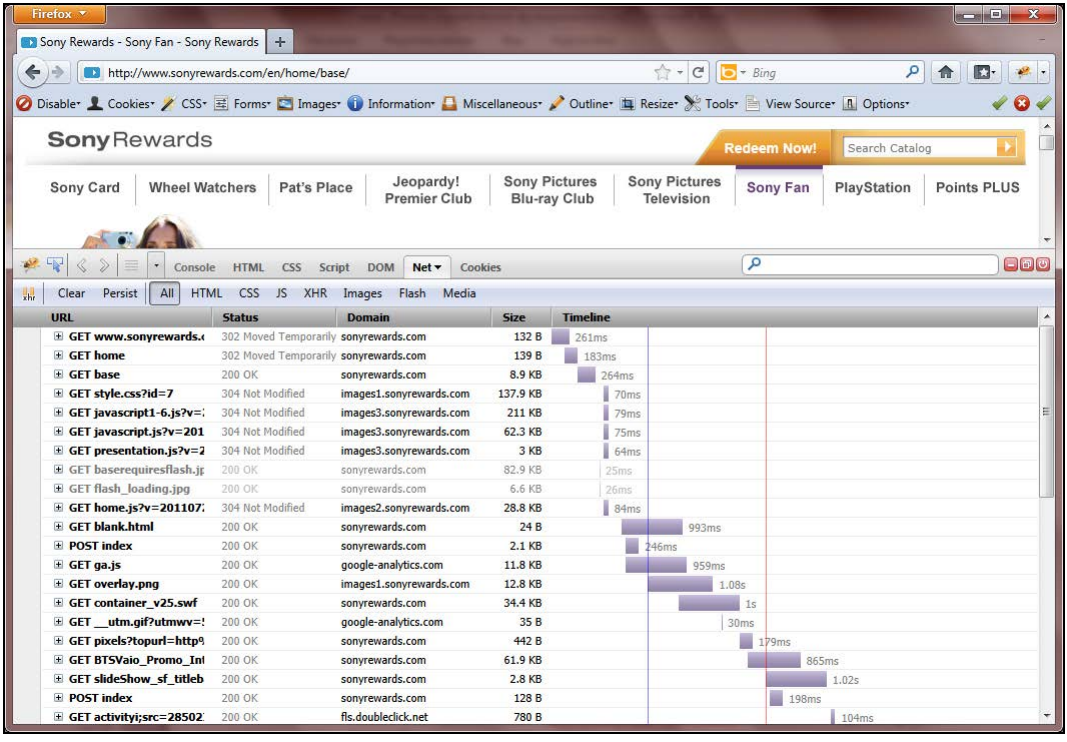


Рис. 1.2. Оптимизация загрузки на стороне сервера

1.2. Windows 7

Не знаю почему, но Microsoft постоянно изменяет методы, которыми она использует различные элементы оформления в своих ОС. Руководству компании наверно нравится менять все каждые 5—7 лет. Но вот в последней версии Windows 7 графическая оболочка вроде бы достигла своего идеала и почти не отличается от Windows Vista.

По сравнению с Windows 8 графическая система снова претерпит изменения, но уже похоже не так сильно. То, что касается оформления Windows XP, и было описано в предыдущих изданиях книги, вы можете найти в электронном архиве на FTP-сервере в каталоге Doc\Windows.

1.2.1. Окно входа в систему

Не знаю почему, но Microsoft зачем-то усложнила смену фонового рисунка загрузки компьютера и окна входа в систему. В Windows 9*x* окно менялось банальным изменением графического файла в корне загрузочного диска, хотя и расширение файла было изменено (если мне не изменяет память, то расширение было dat вместо bmp). В Windows XP спрятали в файл ресурсов, и изменение картинок достаточно сильно усложнилось.

В Windows 7 компания Microsoft (или кто там отвечает за подобные вещи) снова упростила процесс смены картинки, хотя он все равно остался скрытым. Не знаю, почему компания не предоставила нормальной утилиты.

Итак, чтобы изменить фон картинки, которую вы видите при входе в систему, нужно для начала загрузить редактор реестра и перейти в следующий раздел:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Authentication\LogonUI\Background

Тут должен быть параметр **OEMBackground**, который по умолчанию равен `0`. Если какой-то из параметров или разделов не существует, то их можно без проблем создать. Если параметр **OEMBackground** изменить на `1`, то в качестве картинки для окна входа в систему будет использоваться файл:

C:\Windows\System32\oobe\Info\backgrounds\backgroundDefault.jpg

Тут есть одна интересная особенность — этот путь может быть недоступен в некоторых файловых менеджерах. Например, я люблю использовать Total Commander, и если в этом редакторе перейти в папку c:\Windows\System32\oobe\, то в ней будут только два файла и одна папка, но папки info не будет (рис. 1.3).

Ну а если ту же папку открыть в Проводнике Windows, то она заметно преображается и появляется нужная папка info, в которой и следует искать подпапку backgrounds (рис. 1.4).

Имя файла backgroundDefault.jpg используется по умолчанию, если файл для вашего разрешения не найден. Так как вы знаете разрешение своего экрана, то можете поместить туда соответствующую картинку. Но для более универсального решения

можно создать файлы в следующем формате background*XXX*x*XXX*.jpg, где *XXX*x*XXX* — это разрешение экрана. Например, если у вас экран размером в 1280×960 пикселов, то имя файла должно быть background1280x960.jpg.

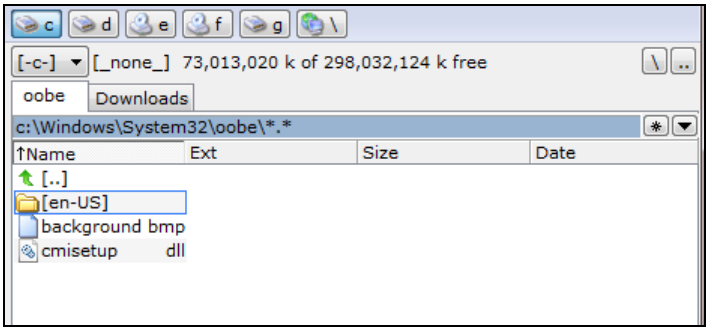


Рис. 1.3. Папка oobe в Total Commander

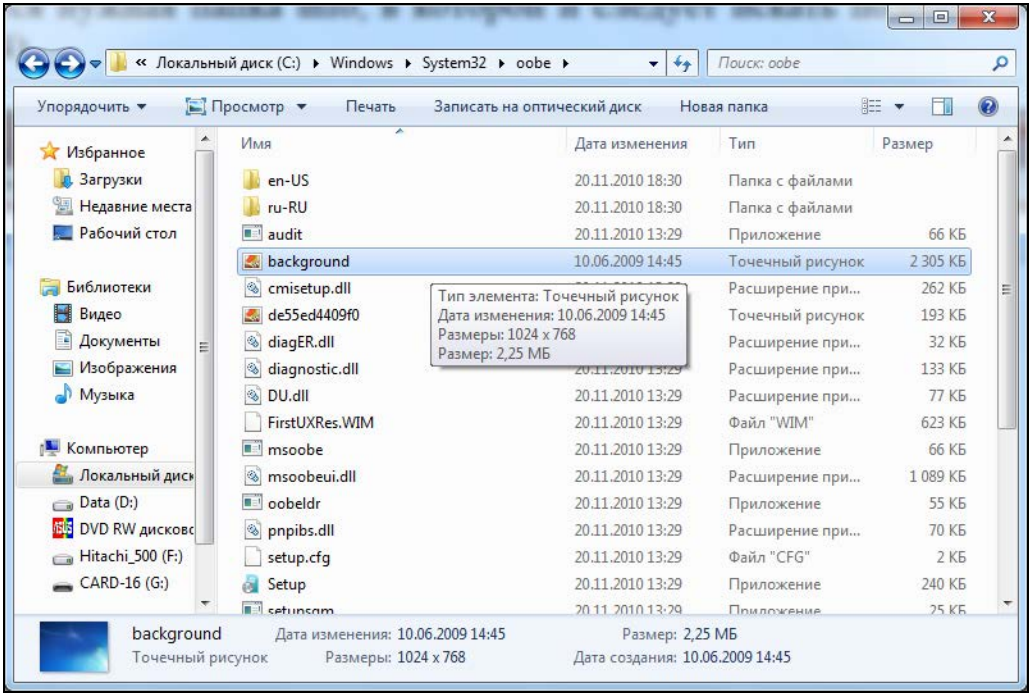


Рис. 1.4. Папка oobe в Проводнике Windows

1.2.2. Рабочий стол

Лично я люблю чистый рабочий стол, на котором нет ничего лишнего. На данный момент у меня на нем расположены только один ярлык Корзины (Recycle Bin) и один ярлык документа, с которым я работаю.

Если посмотреть на рабочий стол компьютера моей жены, то там файлу приземлиться негде. Весь рабочий стол заполнен ярлыками.

Есть несколько способов убрать все с рабочего стола. Самый жестокий — это удалить ярлыки. Хотя нет, все ярлыки удалить не получится. Есть один, который не удаляется — Корзина. Если щелкнуть по ней правой кнопкой мыши, то там вы не найдете пункта удаления. Чтобы удалить Корзину, переходим в реестре к разделу:

HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\Desktop\NameSpace

Здесь ищем подраздел, у которого значение по умолчанию равно `Recycle Bin` (рис. 1.5). У меня таким оказался **{645FF040-5081-101B-9F08-00AA002F954E}**. Я тут не могу утверждать, но опыты показывают, что на всех системах Windows Vista и Windows 7 Корзина имеет этот код. Но просто на всякий случай убедитесь, что именно она перед вами.

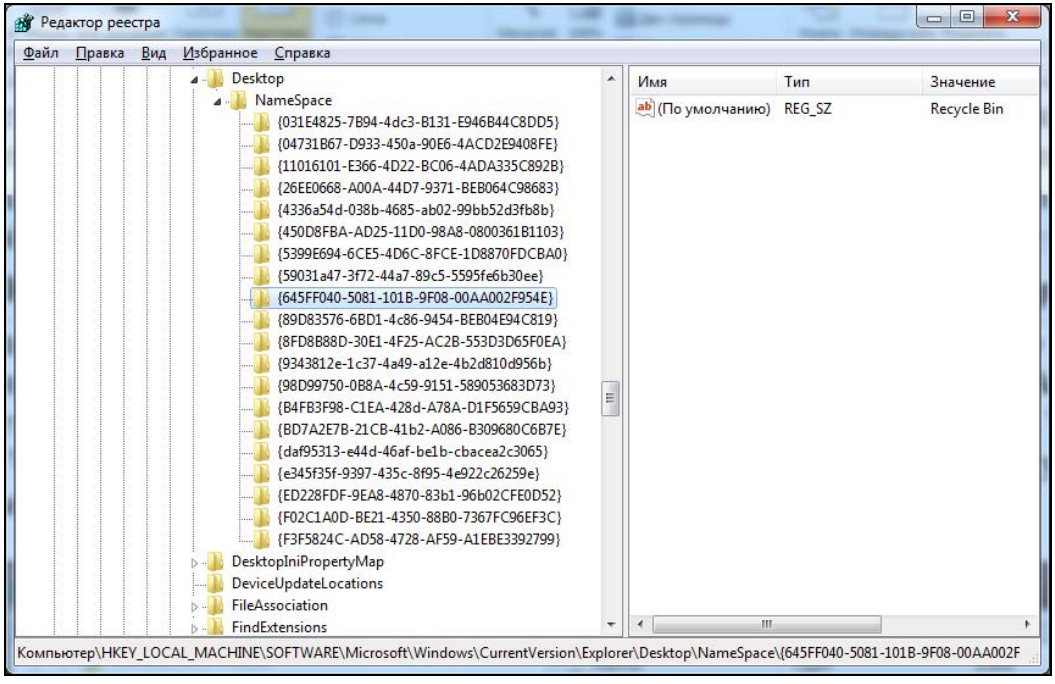


Рис. 1.5. Раздел реестра, отвечающий за Корзину на рабочем столе

Так как мы удалили Корзину, ее нужно как-то чистить. Ее все еще можно очистить, например, вручную. Для этого в своем менеджере файлов сделайте так, чтобы отображались скрытые файлы. На каждом диске вы сможете увидеть скрытую папку с именем $Recycle.Bin (рис. 1.6). Внутри этой папки будет еще несколько папок, но для доступа к ним нужны права администратора, и там ничего интересного нет. Вас больше должна интересовать папка, у которой даже ярлык — корзина. У меня это S-1-5-21-4060577442-2030883239-2705281912-1000. Если зайти в эту папку, то вы увидите удаленные вами файлы, и очистка Корзины в принципе заключается в удалении этих файлов с диска.

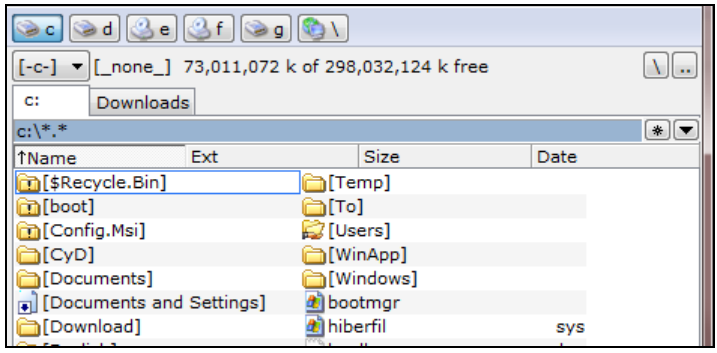


Рис. 1.6. Корзина — это просто скрытая папка в корне диска

Получается, что для доступа к Корзине достаточно в файловом менеджере перейти в папку c:\$Recycle.Bin\S-1-5-21-4060577442-2030883239-2705281912-1000\. Но это не всегда удобно, и у каждого диска своя папка для Корзины. Это сделано для того, чтобы проще было удалять. Дело в том, что если перемещать файл из реальной папки в папку Корзины внутри одного диска, достаточно пользоваться операцией переименования. Вы как бы переименовываете путь к файлу, перемещая его в новое место, и это происходит мгновенно. Если же источник и приемник на разных дисках, то тут уже придется копировать файл с одного места в другое и потом удалять из источника.

Но Корзине можно найти вполне удобное и полезное место для жизни — окно **Компьютер** (Computer). Тут располагаются все диски и сюда же можно добавить Корзину. Для этого переходим в раздел реестра:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\MyComputer\NameSpace

И добавляем уже знакомый нам магический ключик **{645FF040-5081-101B-9F08-00AA002F954E}**. Теперь ваше окно **Компьютер** будет содержать и Корзину — рис. 1.7.

Но если вы хотите убрать значки просто ради шутки (а шутки мы будем рассматривать отдельно), то не обязательно прибегать к жестокому методу удаления этих самых значков. Я не настолько жестокий, поэтому предлагаю воспользоваться более простым способом. В реестре переходим в следующий раздел:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer

И здесь создаем `DWORD`-параметр **NoDesktop** (он, скорее всего, не будет существовать). Если этому параметру установить значение `1`, то все ярлыки исчезнут с рабочего стола. Чтобы вернуть все значки на их место, просто изменяем на `0`.

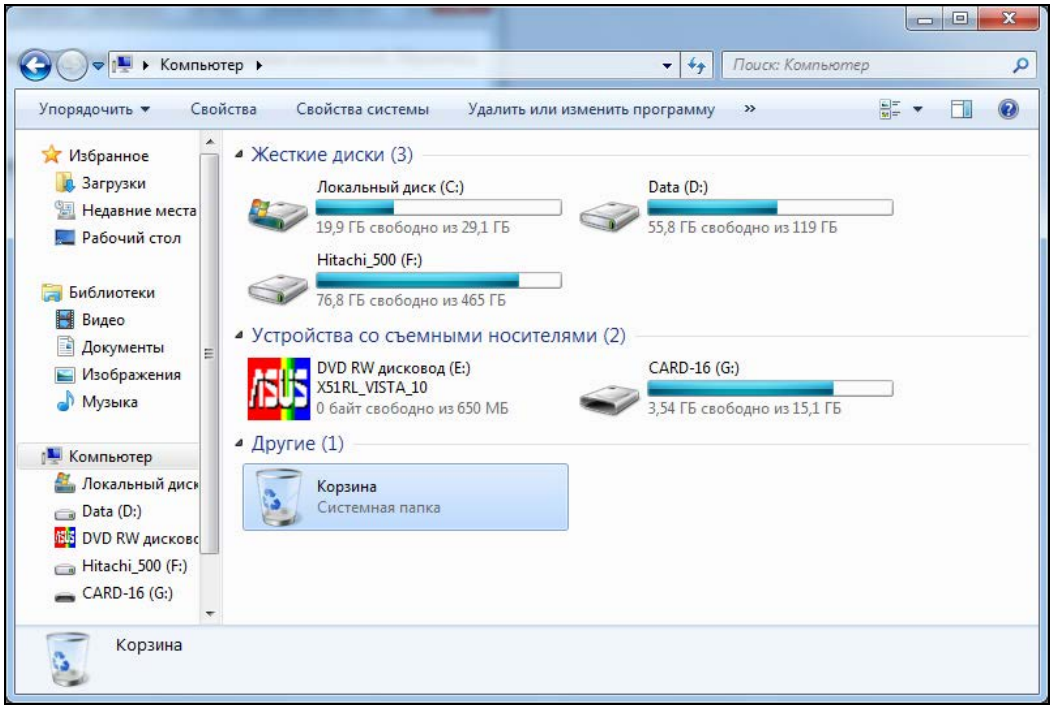


Рис. 1.7. Корзина в вашем компьютере

ГЛАВА 2

Внутренний мир Windows

Если в предыдущей главе мы обсуждали Windows весьма поверхностно, то здесь мы рассмотрим проблемы настройки глубже и детальнее. Вы узнаете, из чего состоят программы, и это позволит вам изменять практически любой софт по собственному усмотрению.

В этой главе нам предстоит познакомиться с великолепной программой Restorator, с помощью которой вы сможете редактировать ресурсы исполняемых файлов и динамических библиотек. В качестве практических примеров мы отредактируем загрузчики Windows XP и программы входа в систему.

Изменение ресурсов, которое мы будем рассматривать в данной главе, применимо в равной степени к любой версии ОС. Но я затрону только загрузчики Windows XP/Vista/7, которые имеют новый формат и содержат намного больше интересных для хакера настроек. Однотипные же ресурсы в Windows 9*x* реализованы проще, и о них уже много сказано в Интернете, так что нет смысла повторяться. (Да и есть ли у кого еще эта ОС?)

2.1. Ресурсы Windows

Прежде чем приступать к серьезным изменениям системы, мы должны немного познакомиться с теорией. Основой этого раздела будет работа с ресурсами программ, и именно о них мы сейчас поговорим с научной точки зрения.

Что такое ресурсы и для чего они нужны? Чтобы понять это, достаточно увидеть, что может быть в ресурсах, а это картинки, значки, строки и внешний вид диалоговых окон. Программа использует ресурсы в своей работе, а мы можем получить к ним доступ и изменить, а значит, повлиять на внешний вид и даже на поведение программы.

Классические исполняемые файлы Windows имеют расширение exe. В общем виде они состоят из следующих частей:

- заголовок;
- исполняемый код;
- ресурсы.

Существуют еще и .NET-сборки, но это уже отдельная история.

Заголовок содержит служебную информацию, которую ОС использует при запуске файла. Например, здесь записана точка, начиная с которой должен выполняться исполняемый код. Это очень важная информация для любой программы. Помимо этого, можно узнать, где размещаются ресурсы программы (чаще всего — после исполняемого кода, но возможны и исключения).

Исполняемый код мы изменять не будем, это достаточно сложно и нужны знания Ассемблера и сложных программ отладки приложений. Ну а с ресурсами познакомимся достаточно подробно, потому что здесь для настоящего хакера кроется много интересного.

Все ресурсы разбиты по разделам:

- Bitmap — картинки, высвечиваются в окнах программы;
- Menu — меню, обеспечивают удобный доступ к функциям приложения, структурируя их в однородные группы;
- Dialog — всевозможные окна диалогов;
- Stringtable — таблица с сообщениями, которые используются в строках состояния или в окнах диалогов;
- Accelerator — сочетания клавиш для быстрого вызова каких-либо команд;
- Cursor — различные курсоры;
- Icon — рисунки определенного размера, чаще используются для отображения в виде значка формы в свернутом состоянии;
- Versioninfo — информация о версии. В дальнейшем мы этот раздел использовать не будем, поэтому забудьте о его существовании и то, что я о нем упоминал :).

Все ресурсы хранятся в открытом виде и доступны для редактирования. Ресурсы могут быть не только в исполняемых файлах, но и в динамических библиотеках (dll), программах-заставках (scr), отдельных файлах ресурсов (res) и в некоторых других типах файлов.

Руками какой-либо из ресурсов изменить невозможно, но программ для их редактирования великое множество. Практически в каждом языке программирования есть утилита или встроенный модуль, который позволяет изменять ресурсы:

- Borland Resource Workshop — поставляется с некоторыми средствами разработки фирмы Borland;
- Microsoft Visual Studio — среда разработки от Microsoft, которая может открывать исполняемые файлы для редактирования ресурсов.

Тут надо заметить, что модули, написанные на разных языках программирования, могут иметь разные типы ресурсов. Например, компилятор Visual C++ создает про-

граммы, в которых все визуально созданные диалоговые окна хранятся в ресурсах в стандартном виде. Borland Delphi использует для этих целей собственный формат, который обладает более мощными визуальными возможностями. Поэтому не помешает научиться определять язык, на котором написана программа.

Самыми распространенными языками программирования для платформы Windows на данный момент являются C++ и C#, а значит уникальный ресурс файлов Borland Delphi можно проигнорировать.

2.2. Программа Restorator

Для редактирования ресурсов лучше всего использовать такую утилиту, которая одинаково хорошо работала бы с программами, написанными на разных языках программирования.

Мне больше других нравится утилита Restorator, которую можно скачать на сайте **http://www.bome.com/Restorator/**. Она позволяет редактировать запускаемые файлы и обладает гораздо большими возможностями, чем другие программы, которые я видел. Именно ее мы и будем рассматривать.

Прежде чем продолжить чтение, я советую установить эту программу на свой компьютер, чтобы она была под рукой, и вы в любой момент могли проверить описываемые действия. Так лучше всего будет запоминаться описываемый здесь материал. Данная книга не является файлом помощи по программе, поэтому мы рассмотрим только основы, которые касаются взлома программ и придания им симпатичного вида.

Итак, на рис. 2.1 представлено главное окно программы Restorator 2007. Что мне нравится в ней, так это стабильность. В первом издании книги была описана версия 2004, и ее главное окно практически не отличается от 2007-й версии. Основное окно программы разбито на три части:

- **Resource Tree** — панель для отображения всех ресурсов открытого файла по категориям в виде дерева;
- **Resource View** — вкладка для просмотра выделенного ресурса;
- **File Browser** — вкладка с браузером (в стиле программы Проводник), в котором можно обозревать содержимое компьютера. Это очень удобно для открытия ресурсов.

Давайте откроем какую-нибудь программу и на ее примере увидим, как можно изменять ресурсы. Для примера я взял программу dialer.exe, которая устанавливается вместе с Windows. Если у вас ОС установлена на диске C:, то путь к файлу будет C:\Windows. В Windows XP SP2 эта программа изменилась, находится в другом месте и выглядит по-новому. Нам же нужен сам факт примера редактирования, а какая программа — не имеет значения, поэтому я оставил в качестве примера звонилку из первой версии XP (она же была и в Windows 9*x*/NT/2000).

Выберите в программе Restorator меню **File | Open** (Файл | Открыть). Перед вами появится стандартный диалог открытия файла. Найдите файл dialer.exe. Программа

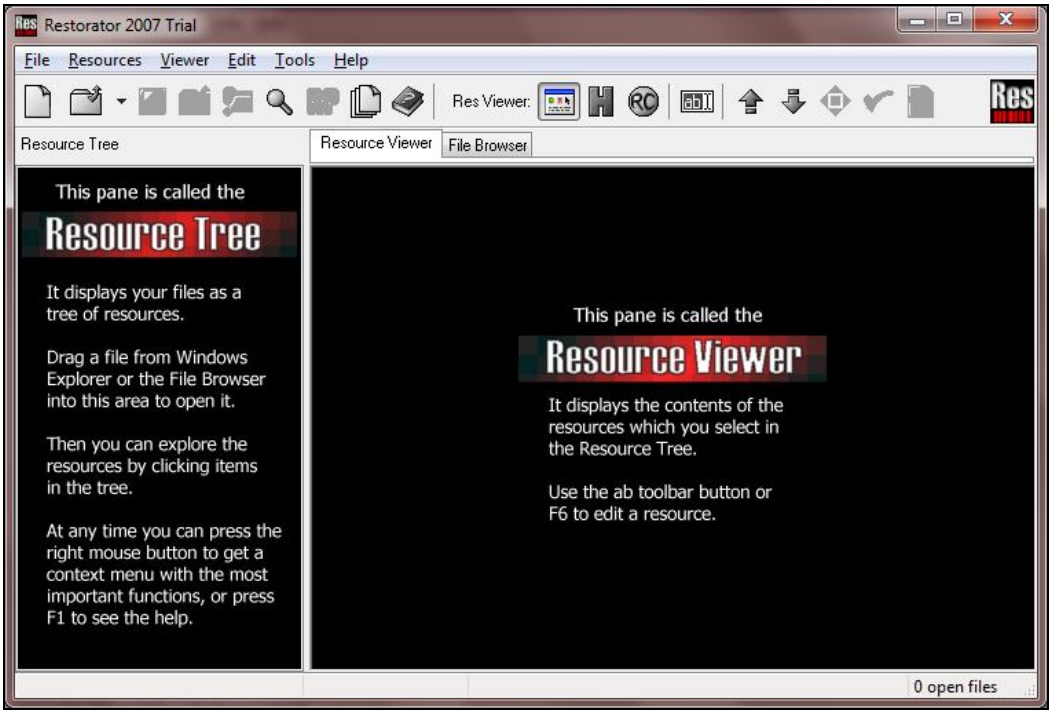


Рис. 2.1. Главное окно программы Restorator

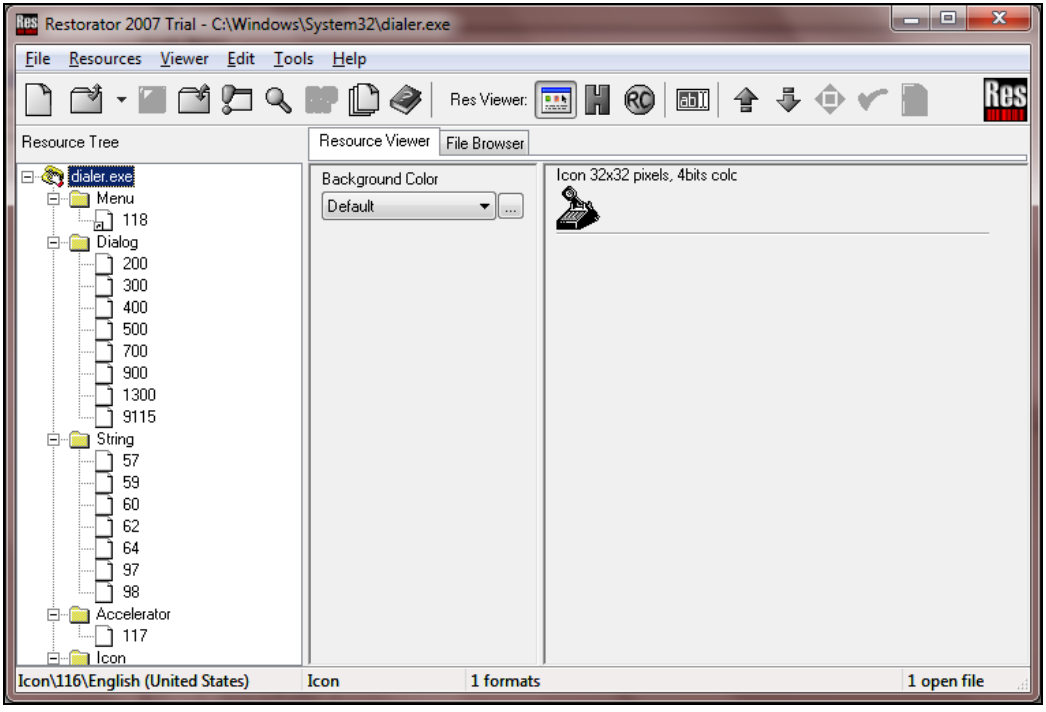


Рис. 2.2. Окно программы Restorator с открытым файлом

загрузит названия его ресурсов в панель **Resource Tree**. Чтобы раскрыть все дерево ресурсов, выделите название файла (оно должно быть в корне дерева) и нажмите знак умножения (*) в дополнительной секции клавиатуры. Результат этих действий показан на рис. 2.2.

Я специально выбрал программу, в которой присутствуют практически все типы ресурсов, и сейчас нам предстоит рассмотреть, как их можно редактировать.

2.2.1. Редактирование меню

На рис. 2.2 в дереве ресурсов в разделе **Menu** вы увидите только один пункт под номером 118. Выделите его, и на вкладке **Resource Viewer** появится исходное меню, для редактирования которого нужно выбрать в главном меню опцию **Viewer | Edit Mode**, это заставит отображать ресурс в виде команд. Кроме того, появится окно для просмотра изменений (рис. 2.3).

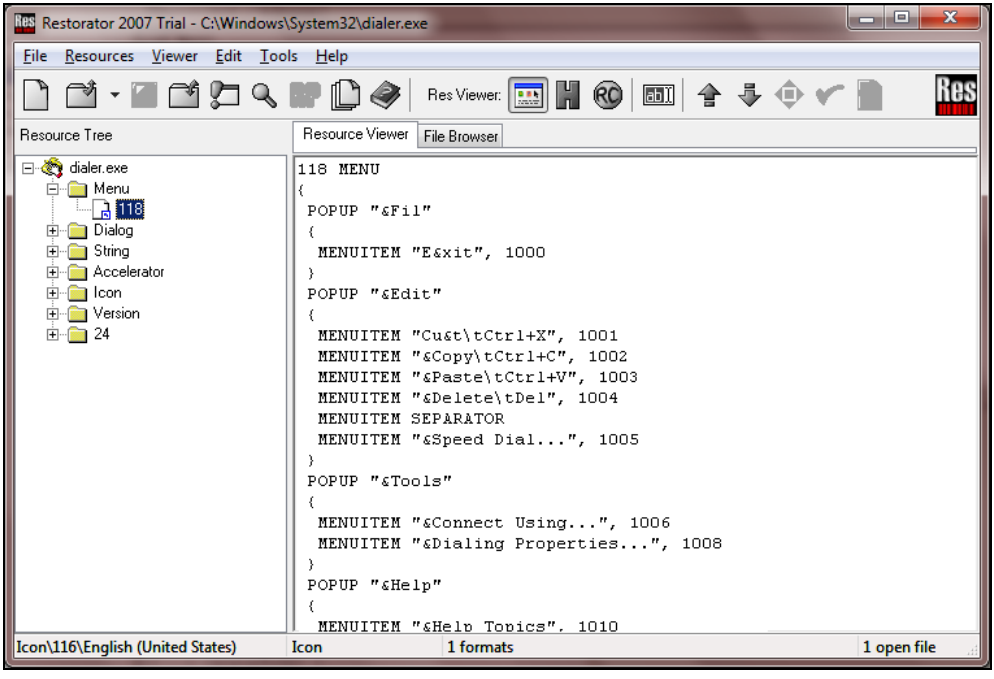


Рис. 2.3. Редактирование меню

В листинге 2.1 приведен полный код (исключены только комментарии) меню программы Dialer в командах ресурсов. Этот код достаточно прост для понимания, и сейчас мы его рассмотрим.

Листинг 2.1. Исходный код меню

```
118 MENU
{
 POPUP "&File"
```

```
 {
  MENUITEM "E&xit", 1000
 }
 POPUP "&Edit"
 {
  MENUITEM "Cu&t\tCtrl+X", 1001
  MENUITEM "&Copy\tCtrl+C", 1002
  MENUITEM "&Paste\tCtrl+V", 1003
  MENUITEM "&Delete\tDel", 1004
  MENUITEM SEPARATOR
  MENUITEM "&Speed Dial...", 1005
 }
 POPUP "&Tools"
 {
  MENUITEM "&Connect Using...", 1006
  MENUITEM "&Dialing Properties...", 1008
 }
 POPUP "&Help"
 {
  MENUITEM "&Help Topics", 1010
  MENUITEM "&What's This?", 1015
  MENUITEM SEPARATOR
  MENUITEM "&About Phone Dialer", 1011
 }
}
```

Прежде чем рассматривать код из листинга 2.1, познакомимся с комментариями. Это произвольный текст, который никак не влияет на ресурс, но позволяет добавлять какие-либо собственные описания или примечания. Когда компилятор ресурса встречает двойной слеш (`//`), весь последующий текст в этой строке воспринимается в качестве комментария. Итак, я буду вставлять пояснения к рассматриваемому коду, а вы можете использовать комментарии для того, чтобы помечать места, в которых производили изменения.

Меню начинается с номера, который определяет имя ресурса (в данном случае 118). После этого следует ключевое слово `MENU`. Начало и конец меню обозначаются фигурными скобками `{}`:

```
118 MENU
{
 // Здесь идет описание меню
}
```

Если у вас есть опыт программирования на языках C/C++, то для вас такая структура будет знакома.

Между фигурными скобками, ограничивающими меню, располагаются выпадающие меню и их элементы. Описание выпадающего меню начинается с ключевого слова `POPUP`, после чего в двойных кавычках идет имя, которое вы хотите увидеть в

самом меню. При создании имени перед любой буквой можно поставить знак &. Следующий за этим знаком символ будет ключевым для меню, и если нажать клавишу <Alt> вместе с ним, то будет вызвано это меню, а при отображении данная буква в названии будет подчеркнута.

Таким образом, выпадающее меню File будет иметь такую структуру:

```
POPUP "&File"
{
}
```

После описания выпадающего меню снова идут фигурные скобки, внутри которых можно создавать вложенные элементы:

```
MENUITEM "Имя", Код
```

При написании имени работают те же правила, что и для выпадающего меню, т. е. можно использовать знак &. Помимо этого, после знаков \t можно добавлять "горячие" клавиши. Например, сочетанию клавиш <Ctrl>+<X> соответствует "Ctrl+X".

Код — это идентификатор (число), по которому программа определяет меню и реагирует на него. Таким образом, с помощью редактора ресурсов можно изменять имена, и программа будет работать корректно. Но если поменять код, то работа программы в данном месте будет нарушена.

Допустим, что вы хотите откорректировать следующие пункты меню:

```
MENUITEM "Cu&t\tCtrl+X", 1001
MENUITEM "&Copy\tCtrl+C", 1002
MENUITEM "&Paste\tCtrl+V", 1003
```

С помощью редактора ресурсов попробуйте изменить идентификаторы, просто поменяв их местами:

```
MENUITEM "Cu&t\tCtrl+X", 1002
MENUITEM "&Copy\tCtrl+C", 1003
MENUITEM "&Paste\tCtrl+V", 1001
```

Теперь при попытке вырезать выделенную часть текста (команда Cut) будет происходить копирование данных в буфер обмена, при копировании (Copy) — вставка, а при вставке (Paste) программа вырежет данные и поместит в буфер. Но это уже из серии шуток. А это отдельная история, о которой мы будем говорить на протяжении всей *главы 3*.

Итак, номера можно только менять местами. Выдумывать что-то свое бесполезно, потому что такой пункт меню работать просто не будет.

Для создания полосы разделителя между меню нужно написать:

```
MENUITEM SEPARATOR
```

После внесения изменений в код меню их можно просмотреть в окне предварительного просмотра, которое появилось во время перехода в режим редактирования. Но чтобы отобразить изменения меню в этом окне, нужно обновить информацию. Для этого нажмите клавишу <F5>.

Теперь вы без проблем сможете создавать собственные меню любой сложности.

2.2.2. Редактирование диалоговых окон

Отдельная песня — это редактирование диалоговых окон. Тут много команд, и описать их все просто невозможно. Откройте раздел **Dialog** в дереве ресурсов и выделите ресурс под номером **200**. Вы должны увидеть диалоговое окно в визуальном представлении (рис. 2.4).

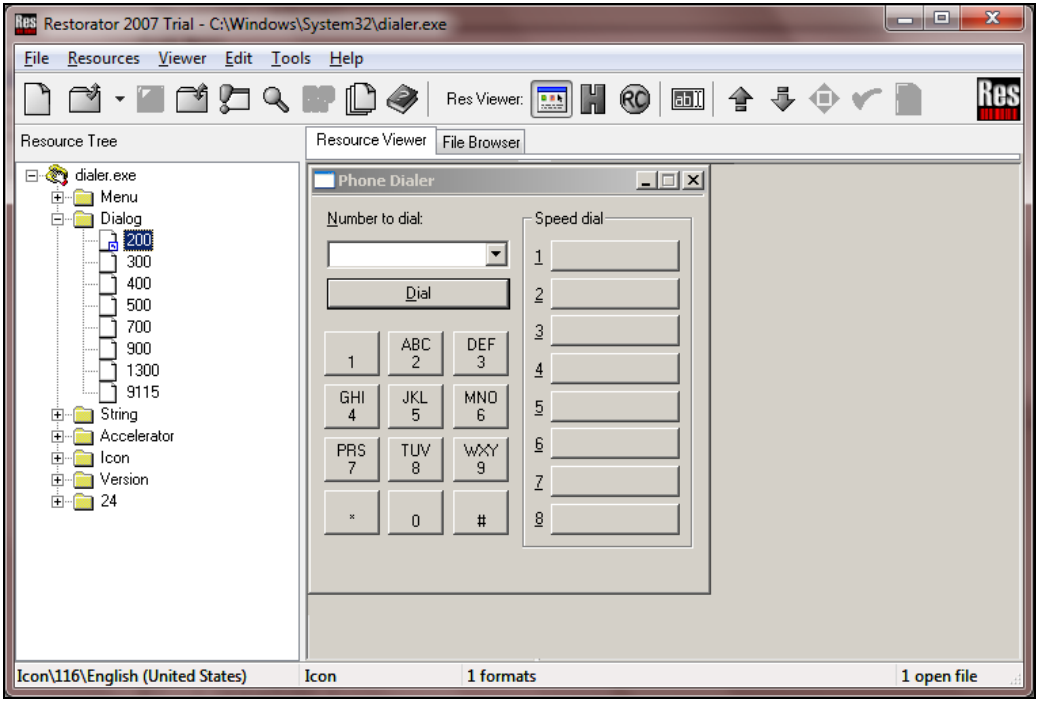


Рис. 2.4. Просмотр диалогового окна

Для перехода в режим редактирования нужно выбрать меню **Viewer | Edit Mode**. Код диалогового окна под номером 200 представлен в листинге 2.2.

Листинг 2.2. Исходный код диалогового окна

```
200 DIALOG 50, 50, 194, 168
STYLE DS_SETFONT | DS_3DLOOK | WS_MINIMIZEBOX | WS_CAPTION | WS_SYSMENU
MENU 118
CAPTION "Phone Dialer"
FONT 8, "MS Shell Dlg"
{
 CONTROL "", 224, "STATIC", SS_ETCHEDHORZ | WS_DISABLED, 0, 0, 194, 1
 LTEXT "&Number to dial:", 223, 7, 7, 90, 10
 COMBOBOX 201, 7, 21, 90, 104, CBS_DROPDOWN | CBS_AUTOHSCROLL | CBS_SORT
   | WS_VSCROLL | WS_GROUP
```

```
 DEFPUSHBUTTON "&Dial", 1, 7, 38, 90, 14, WS_DISABLED | WS_GROUP
 PUSHBUTTON "\n1", 202, 6, 62, 27, 20, BS_CENTER | BS_MULTILINE |
   NOT WS_TABSTOP
 PUSHBUTTON "ABC\n2", 203, 37, 62, 27, 20, BS_CENTER | BS_MULTILINE |
   NOT WS_TABSTOP
 PUSHBUTTON "DEF\n3", 204, 69, 62, 27, 20, BS_MULTILINE | NOT WS_TABSTOP
 PUSHBUTTON "GHI\n4", 205, 6, 86, 27, 20, BS_CENTER | BS_MULTILINE |
   NOT WS_TABSTOP
 PUSHBUTTON "JKL\n5", 206, 37, 86, 27, 20, BS_CENTER | BS_MULTILINE |
   NOT WS_TABSTOP
 PUSHBUTTON "MNO\n6", 207, 69, 86, 27, 20, BS_CENTER | BS_MULTILINE |
   NOT WS_TABSTOP
 PUSHBUTTON "PRS\n7", 208, 6, 110, 27, 20, BS_CENTER | BS_MULTILINE |
   NOT WS_TABSTOP
 PUSHBUTTON "TUV\n8", 209, 37, 110, 27, 20, BS_CENTER | BS_MULTILINE |
   NOT WS_TABSTOP
 PUSHBUTTON "WXY\n9", 210, 69, 110, 27, 20, BS_CENTER | BS_MULTILINE |
   NOT WS_TABSTOP
 PUSHBUTTON "\n*", 212, 6, 134, 27, 20, BS_CENTER | BS_MULTILINE |
   NOT WS_TABSTOP
 PUSHBUTTON "\n0", 211, 37, 134, 27, 20, BS_CENTER | BS_MULTILINE |
   NOT WS_TABSTOP
 PUSHBUTTON "\n#", 213, 69, 134, 27, 20, BS_CENTER | BS_MULTILINE |
   NOT WS_TABSTOP
 GROUPBOX "Speed dial", 222, 103, 7, 84, 154
 LTEXT "&1", 225, 109, 24, 7, 10
 PUSHBUTTON "", 214, 117, 21, 63, 14, BS_LEFT | WS_GROUP
 LTEXT "&2", 226, 109, 41, 7, 10
 PUSHBUTTON "", 215, 117, 38, 63, 14, BS_LEFT | WS_GROUP
 LTEXT "&3", 227, 109, 58, 7, 10
 PUSHBUTTON "", 216, 117, 55, 63, 14, BS_LEFT | WS_GROUP
 LTEXT "&4", 228, 109, 75, 7, 10
 PUSHBUTTON "", 217, 117, 72, 63, 14, BS_LEFT | WS_GROUP
 LTEXT "&5", 229, 109, 92, 7, 10
 PUSHBUTTON "", 218, 117, 89, 63, 14, BS_LEFT | WS_GROUP
 LTEXT "&6", 230, 109, 109, 7, 10
 PUSHBUTTON "", 219, 117, 106, 63, 14, BS_LEFT | WS_GROUP
 LTEXT "&7", 231, 109, 126, 7, 10
 PUSHBUTTON "", 220, 117, 123, 63, 14, BS_LEFT | WS_GROUP
 LTEXT "&8", 232, 109, 143, 7, 10
 PUSHBUTTON "", 221, 117, 140, 63, 14, BS_LEFT | WS_GROUP
}
```

Объявление диалогового окна в общем виде выглядит следующим образом:

```
n DIALOG x, y, w, h
STYLE Флаги стилей
MENU Номер меню
```

```
CAPTION "Заголовок"
FONT размер, "Название шрифта"
{
 // Здесь идет описание элементов окна
}
```

Здесь:

- `n` — номер ресурса;
- `x` — левая позиция окна;
- `y` — верхняя позиция окна;
- `w` — ширина окна;
- `h` — высота окна.

Далее идет описание стилей окна (`STYLE`). Если окно имеет меню, то оно указывается в следующей строке командой `MENU Номер меню`. Заголовок окна задается командой `CAPTION "Текст заголовка"`. Затем следует описание используемого шрифта (размер/имя) и фигурные скобки, внутри которых перечисляются элементы окна. Давайте рассмотрим описание основных элементов, которые вы можете вставлять в текст окна.

Начиная с третьей версии программы, появилась возможность визуального редактирования диалоговых окон. Для этого нужно сначала выбрать режим просмотра ресурса по умолчанию (меню **Viewer | Default view mode**), а затем перейти в режим редактирования (меню **Viewer | Edit Mode**). В этом случае в окне просмотра ресурсов появится панель свойств выбранного элемента окна. Вы можете мышью двигать любые элементы, изменять их размеры и просматривать сделанные изменения (в той же панели свойств).

Единственный недостаток визуального редактора — нельзя добавлять компоненты. В этом случае придется писать код вручную (для чего надо выбрать режим **Viewer | RC Mode**). Это не страшно, если нужно добавить всего один рисунок. При значительном количестве новых элементов проще воспользоваться программой Resource Workshop или средой разработки Visual Studio.

Значки

Этот тип ресурсов позволяет добавлять графические изображения в диалоговые окна. В принципе, эффективность окна не улучшается, но красоту навести можно. Значки добавляются следующей командой:

```
ICON n, i, x, y, w, h
```

Необходимо задать такие параметры:

- `n` — номер картинки в файле ресурсов. Изображение с таким номером уже должно существовать. Например, в программе Dialer есть два значка с номерами 1 и 116, и любой из этих номеров можно здесь использовать. Добавьте новые значки под своими номерами и потом используйте в диалоговых окнах;

- `i` — индекс, по которому программа сможет обращаться к значку. Не изменяйте этот индекс при редактировании уже существующей картинки. Если вы добавляете новый значок, то можно указывать любое значение (желательно, чтобы оно не конфликтовало с другими элементами в окне), все равно программа не знает о существовании нового значка и не будет к нему обращаться;
- `x` — левая позиция значка;
- `y` — верхняя позиция значка;
- `w` — ширина значка;
- `h` — высота значка.

Надписи

Надписи существуют для добавления текстовых пояснений к каким-либо элементам управления. Они объявляются следующим образом:

```
LTEXT "Текст", i, x, y, w, h
```

Здесь:

- `Текст` — текст подписи (указывается в кавычках);
- `i` — индекс, по которому программа сможет обращаться к подписи. Если вы редактируете уже существующую надпись, то не изменяйте этот индекс. При добавлении новой подписи можно указывать любое значение (желательно, чтобы оно не конфликтовало с другими элементами в окне), все равно программа не знает о существовании новой надписи и не будет к ней обращаться;
- `x` — левая позиция надписи;
- `y` — верхняя позиция надписи;
- `w` — ширина надписи;
- `h` — высота надписи.

Кнопки

По нажатию кнопок выполняются какие-либо команды. Чаще всего мы их видим в диалоговых окнах (в виде **Да** и **Отмена**), но бывают кнопки для вызова специализированных команд. Их объявление выглядит следующим образом:

```
PUSHBUTTON "Текст", i, x, y, w, h, Флаги
```

Необходимо задать:

- `Текст` — подпись на кнопке (указывается в кавычках);
- `i` — индекс, по которому программа сможет обращаться к кнопке. Правила его задания такие же, как для значков и надписей;
- `x` — левая позиция кнопки;

- y — верхняя позиция кнопки;
- w — ширина кнопки;
- h — высота кнопки;
- Флаги — описывают свойства кнопки, их может быть много и они перечисляются через разделитель |. Вот основные:
  - BS_CENTER — надпись располагается по центру;
  - BS_LEFT — текст будет прижат к левому краю;
  - BS_RIGHT — надпись выравнивается по правому краю;
  - BS_MULTILINE — текст может быть многострочным;
  - WS_DISABLED — кнопка отключена;
  - WS_GROUP — кнопка сгруппирована с другими кнопками на окне.

Косметика

Давайте попробуем воспользоваться полученными знаниями на практике и произведем несколько косметических операций над окном диалога. Во-первых, расширим его. Для этого в первой строке объявления окна нужно изменить третий числовой параметр, например, на 225:

```
200 DIALOG 50, 50, 225, 168
```

Теперь поменяем заголовок — третью строку:

```
CAPTION "Horrific Dialer"
```

После этого изменения в заголовке окна будет отображаться надпись "Horrific Dialer".

Теперь добавим в окно диалога значок и подпись. Для этого вслед за открывающей фигурной скобкой поместим следующие строки:

```
FONT 8, "MS Shell Dlg"
{
 ICON 1, 0, 195, 5, 18, 20
 LTEXT "Copyright: Horrific", 223, 40, 1, 90, 10

 //Остальное без изменений
}
```

Нажмите клавишу <F5>. Если в описании окна есть команда CLASS, то при обновлении очень часто возникают ошибки. Просто удалите всю эту строку. В большинстве случаев на работу программы это не повлияет.

Если вас устраивает результат вашего творчества (рис. 2.5), то можно нажать клавишу <F8>, чтобы окончательно записать ресурс, а потом комбинацию клавиш <Ctrl>+<S>, чтобы сохранить весь файл.

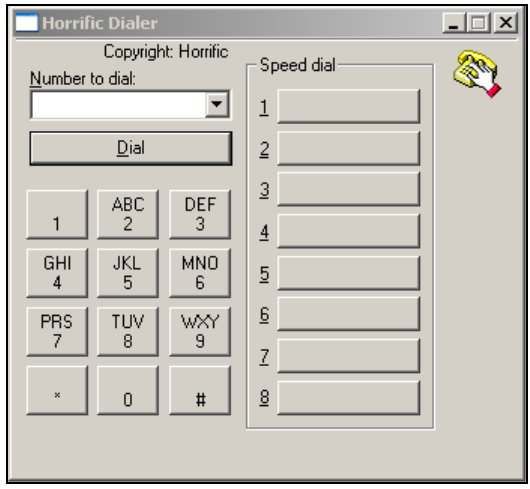


Рис. 2.5. Результат редактирования окна

2.2.3. Редактирование строк и акселераторов

В разделе **String** (см. рис. 2.2) хранятся строки. Это могут быть различные сообщения, названия или просто текст, используемый программой. Выделите любой ресурс в этом разделе и перейдите в режим редактирования (меню **Viewer | Edit Mode**). Рассмотрим на примере ресурса 57, как выглядит его исходный код:

```
STRINGTABLE
{
 901, "Dialer"
 902, "Phone Dialer"
}
```

Все начинается с ключевого слова `STRINGTABLE`. После него идут фигурные скобки, в теле которых описываются строки в виде:

```
Номер, "Строка"
```

`Номер` — это число, по которому программа находит нужную строку. Его изменять не рекомендуется, т. к. это может сказаться на стабильности программы. Сам же текст задается после запятой в кавычках, и его можно без проблем менять, как угодно.

Акселераторы (раздел **Accelerator**) — это "горячие" клавиши, которые используются в программе. Если вас что-то не устраивает, то можно легко изменить на более удобный вариант, даже если смена клавиш не предусмотрена в программе.

В программе dialer.exe только один набор акселераторов под номером 117. Выделите его, и в окне редактирования увидите следующий код:

```
214: "Alt+1"
215: "Alt+2"
```

```
216: "Alt+3"
...
...
1003: "Shift+Ins"
1001: "Ctrl+X"
```

Описание акселераторов похоже на описание строк. Вначале идет код, по которому программа находит нужное сочетание клавиш, а после двоеточия в кавычках указывается сам акселератор.

2.2.4. Редактирование изображений

В ресурсах могут храниться два типа изображений — значки (раздел **Icon**) и картинки (раздел **Bitmap**). Работа с обоими форматами происходит одинаково, посему и рассматривать их будем, как один.

В программе Restorator нет встроенного графического редактора, поэтому приходится использовать любой другой, имеющийся на компьютере. Но для начала нужно сохранить ресурс в отдельном файле. Для этого щелкните по графическому ресурсу правой кнопкой мыши и в появившемся меню выберите пункт **Extract | Extract as *"Имя файла"***. Вместо строки "Имя файла" будет стоять реальное имя ресурса. Перейдите на вкладку **File Browser**, и здесь вы увидите созданный файл.

Теперь вы можете подкорректировать его, а затем подключить обратно к ресурсу, для чего надо снова щелкнуть правой кнопкой мыши и в появившемся меню выбрать **Assign | Assign to**. Далее в стандартном диалоге открытия файла вы должны найти и выбрать отредактированную версию графического файла.

Для редактирования изображений из раздела **Bitmap** подойдет любая графическая утилита, в том числе и входящая в поставку Windows программа Paint. Для работы со значками в ОС Windows ничего нет, поэтому здесь можно выбрать один из следующих способов:

- ❒ найти хорошую программу для редактирования значков;
- ❒ просто заменять значки программы своими.

Я чаще использую второй способ, потому что рисовать не умею, и даже лучший редактор значков не поможет мне создать что-либо красивое. Хорошо, что в Интернете сейчас много готовых и профессионально сделанных значков. Какие-то из них платные, а часть — нет, но даже бесплатные варианты бывают очень хорошего качества.

2.3. Темы Windows

Я хотел назвать этот раздел "Темы Windows 7. Кто следующий?", но потом решил все же, что так будет слишком длинно. Начиная с Windows XP, в Microsoft полностью изменили графическую оболочку ОС и то, как хранятся для нее ресурсы. При переходе на Windows Vista произошли достаточно серьезные архитектурные изме-

нения в ОС, в том числе и в графической части. Но представление ресурсов практически не изменилось, поэтому если вы читали первое издание, бóльшая часть вам будет уже знакома. Думаю, что в Windows 8 серьезных изменений не должно произойти.

Даже если вы не будете менять свои темы, прочитать эту главу будет интересно, потому что вы сможете познакомиться с некоторыми внутренностями ОС. Лично я не меняю темы и использую стандартные настройки. Все, что я изменил на своем домашнем компьютере, — это фон экрана загрузчика, а на работе компьютер стоит с настройками по умолчанию и без изменений. Но каждый раз при выходе новой системы я изучаю ее внутренности и начинаю с графической части. У меня есть своеобразная страсть к графике, и просто это интересно.

Темы ОС Windows хранятся в папке C:\Windows\Resources\Themes. Откройте ее и посмотрите на содержимое. На первый взгляд папка выглядит так же, как и в старых версиях Windows. Все те же бесполезные файлы с расширением theme, и в зависимости от ОС там могут быть еще и папки. В Windows XP каждая тема могла находиться в своей папке и была уникальной. В Windows 7 осталась только одна папка Aero, которая хранит ресурсы для единственной графической оболочки Windows.

В каталоге \Aero находятся все необходимые файлы для стандартной темы Windows — Aero. В Windows XP стандартной темой была Luna, и вы могли увидеть соответствующую папку. Давайте глянем на нее... А это что за "чудо в перьях" — aero.msstyles? Что-то я такого расширения в старой Windows не видел. Надо познакомиться с этим файлом поближе. Когда я первый раз заметил подобный файл (это был luna.msstyles) в Windows XP, то сразу проглядел содержимое в режиме просмотра (в Windows Commander я нажал клавишу <F3>). Сразу бросилось в глаза, что первые два символа в файле — это "MZ". Такое начало говорит о том, что этот файл, скорее всего, имеет байт-код, как у исполняемых файлов. Опускаю взгляд чуть ниже и вижу заветную надпись: "This program cannot be run in DOS mode." Значит файл luna.msstyles не просто содержит байт-код, но и может выполняться или, по крайней мере, имеет схожую структуру.

Как известно, любой исполняемый файл или DLL-библиотека могут содержать ресурсы. Я понадеялся на это и попытался открыть файл в программе Borland Resource Workshop. Меня ждало разочарование, потому что BRW просто "выбило из колеи", и он выдал системную ошибку. Сказывается допотопность и запущенность программы, ведь ее не обновляли уже долгие годы.

Повторяю попытку с помощью программы Restorator, "полет прошел нормально". Единственное, что надо сделать, — в окне открытия файла, в поле **Files of type** выбрать из выпадающего списка **All files**. Просто программа не знает расширения msstyles и не отобразит необходимый файл, поэтому нужно попросить показывать все.

Я не ошибся. В этом файле действительно полно ресурсов. Посмотрите на рис. 2.6, где представлена структура файла luna.msstyles из Windows XP и aero.msstyles из Windows 7. Глядя только на ее заголовки, можно понять: это то, что мы искали.

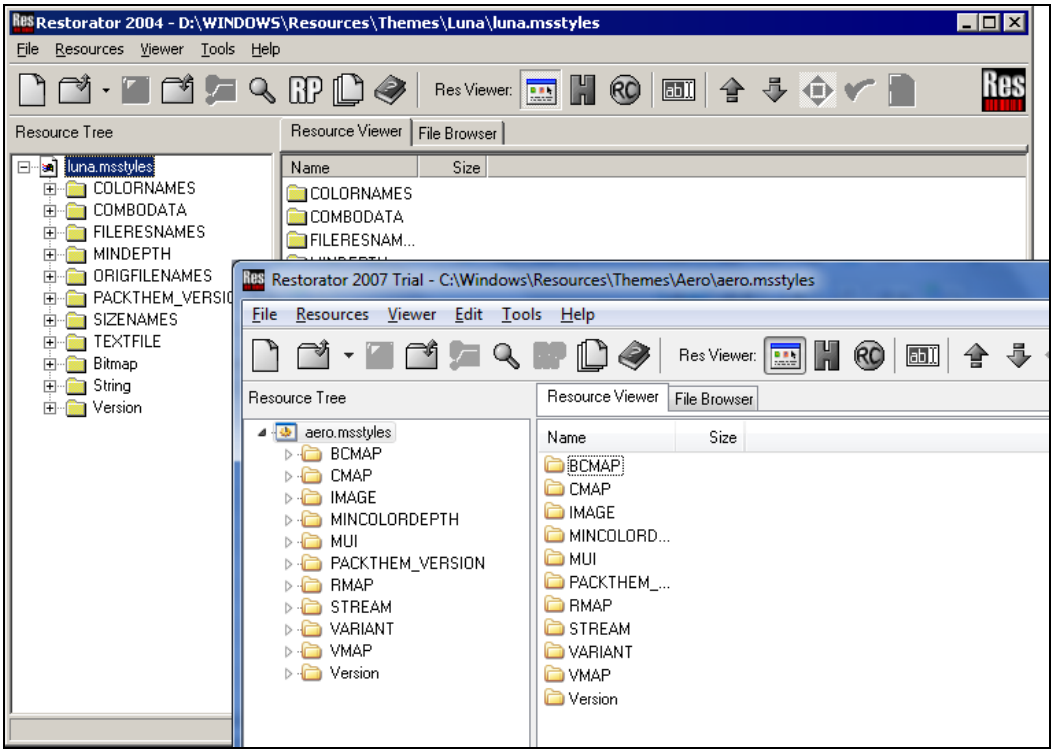


Рис. 2.6. Структура файла luna.msstyles и aero.msstyles

Откройте ветку **Bitmap** и посмотрите на ее содержимое. На рис. 2.7 показан один из пунктов этой ветки, где находятся рисунки, которые используются для отображения элемента управления **CheckBox** (флажок).

Глядя на ресурсы файла, можно представить себе, как Windows может создавать графический интерфейс программ, с которыми мы работаем каждый день. Скорее всего, она просто рисует на поверхностях окон картинки в зависимости от состояния. У меня других предположений нет.

Давайте поработаем, например, над элементом управления **CheckBox**. Для этого в разделе **Bitmap** нам понадобятся ресурсы BLUE_CHECKBOX13_BMP, BLUE_CHECKBOX16_BMP, BLUE_CHECKBOX25_BMP. Это группы изображений данного компонента разного размера.

Теперь правой кнопкой мыши щелкните по первому из этих пунктов и выберите в появившемся меню пункт **Extraxt | Extract as "BLUE_CHECKBOX13_BMP.bmp"**. Найдите этот файл в области **File Browser** и измените в любом графическом редакторе. Я для простоты нарисовал вертикальную линию вдоль всего рисунка. Для загрузки отредактированного файла снова щелкните правой кнопкой по соответствующему ресурсу и выберите пункт **Assign to**, после чего укажите на отредактированный файл. Аналогичным образом можно поступить и с двумя другими рисунками для этого компонента.

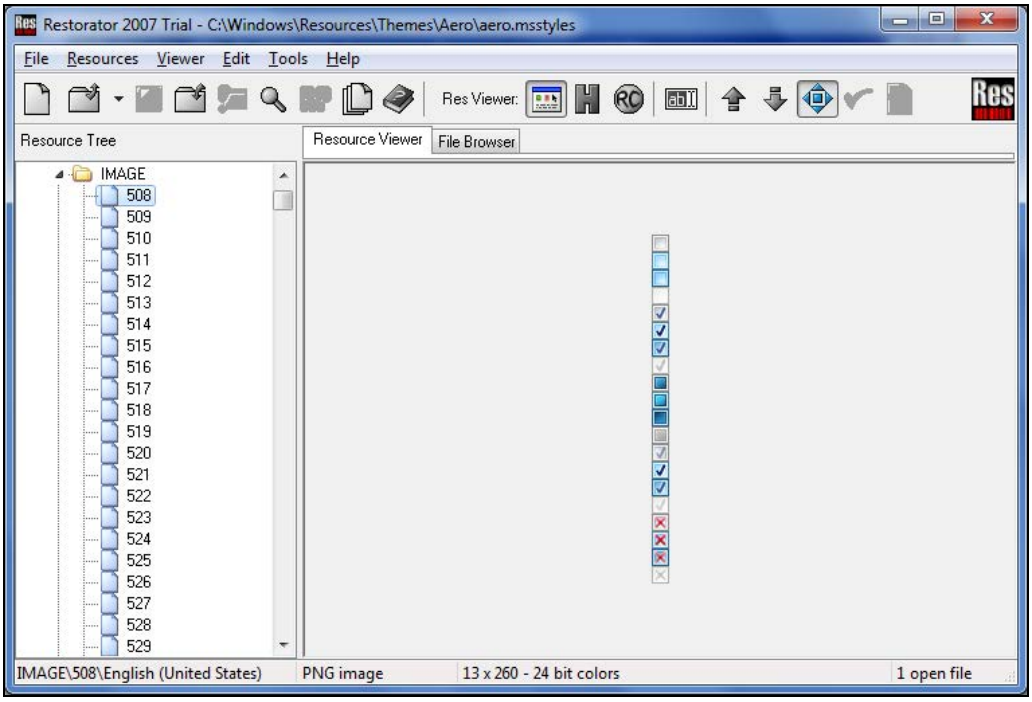


Рис. 2.7. Вот из чего реально состоит компонент **CheckBox**

Как только закончите редактирование, в случае с Windows XP сохраните файл luna.msstyles под новым именем (меню **File | Save as**) и скопируйте новый файл в папку C:\Windows\Resources\Themes. Чтобы установить его в системе, достаточно просто запустить файл luna.msstyles, как любую другую программу, и применить новую тему. Если возникнут проблемы с запуском, то войдите в свойства дисплея и на вкладке **Themes** (Темы) выберите в выпадающем списке **Theme** пункт **Browse** (Обзор). В появившемся окне выберите отредактированный файл и нажмите кнопку **Открыть**.

На рис. 2.8 показано окно свойств программы Windows Commander, в котором очень много компонентов **CheckBox**, и если не подведет печать, то вы сможете увидеть, что все они перечеркнуты полосой.

Если у вас Windows 7, то тут установка новой темы усложняется. Вы можете редактировать aero.msstyles, но не можете его обновить, потому что ОС заблокировала и защищает файл от нежелательных посягательств. Но это можно обойти.

После редактирования файла сохраните его в какой-нибудь отдельной папке, не изменяя имя. Файл должен все еще называться aero.msstyles. Для реализации задуманного вам понадобится любой файловый менеджер. Стандартным Проводником копирование будет невозможно. Я использую для этих целей Total Commander.

Теперь переходим к оригинальному файлу темы c:\Windows\Resources\Themes\Aero\aero.msstyles и заходим в его свойства (щелчок правой кнопкой мыши по файлу — и выбираем пункт свойств). Перейдите на вкладку **Безопасность** (Security) и

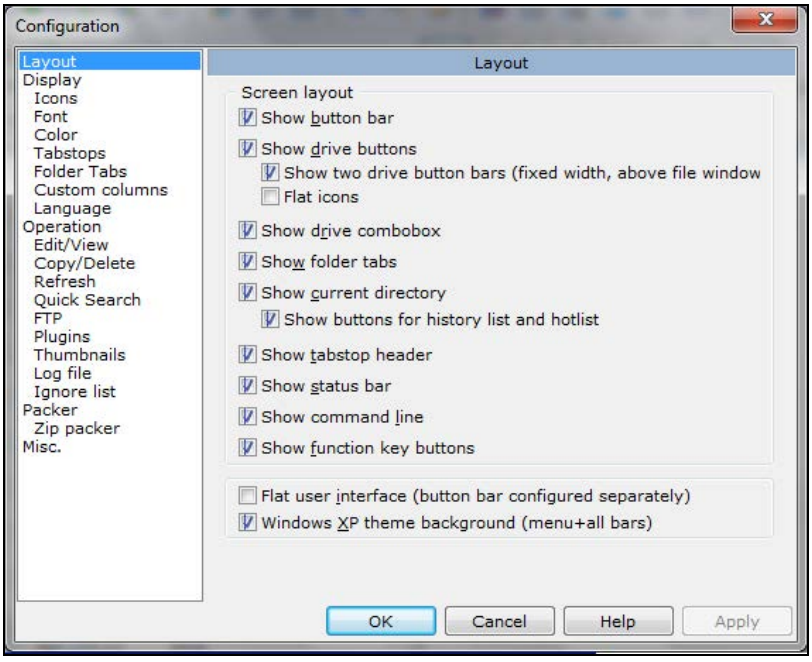


Рис. 2.8. Окно свойств Windows Commander с перечеркнутым компонентом **CheckBox**

просмотрите права доступа файла. У меня получилось так, что только TrustedInstaller имеет полные права, а все остальные могут только читать (рис. 2.9). Это значит, что когда ОС загружается и выполняется от имени вашего пользователя, она без проблем может прочитать файл темы и использовать его ресурсы, но не может изменить.

Интересно, что даже администраторы не могут менять права, потому что они не являются владельцами файла. Но это легко исправить, и это, скорее всего, просчет Microsoft в безопасности. Щелкаем на кнопке **Дополнительно** (Advanced) прямо под списком прав доступа, и перед нами появляется окно расширенных свойств. Здесь переходим на вкладку **Владелец** (Owner). Владельцем файла так же будет являться TrustedInstaller. Но вы же администратор и можете без проблем перехватить файл себе. Просто меняйте имя владельца на свое (рис. 2.10). Обладая правами администратора, вы эту операцию должны выполнить без проблем.

> ***Внимание!***
>
> Перехватив файл на себя, вы становитесь владельцем, и ОС уже не сможет защищать файл от изменений. Как вернуть владение файлом обратно пользователю TrustedInstaller, я, к сожалению, не знаю. Я пробовал это сделать, но ничего не вышло.

Теперь вы владелец файла. Измените права доступа на полный контроль (Full Control) для своей учетной записи.

Теперь вы имеете право изменять aero.msstyles, но все еще не можете этого сделать, потому что он, скорее всего, заблокирован системой, ведь если у вас в данный момент используется тема Aero, то ОС использует файл. Для начала переключите

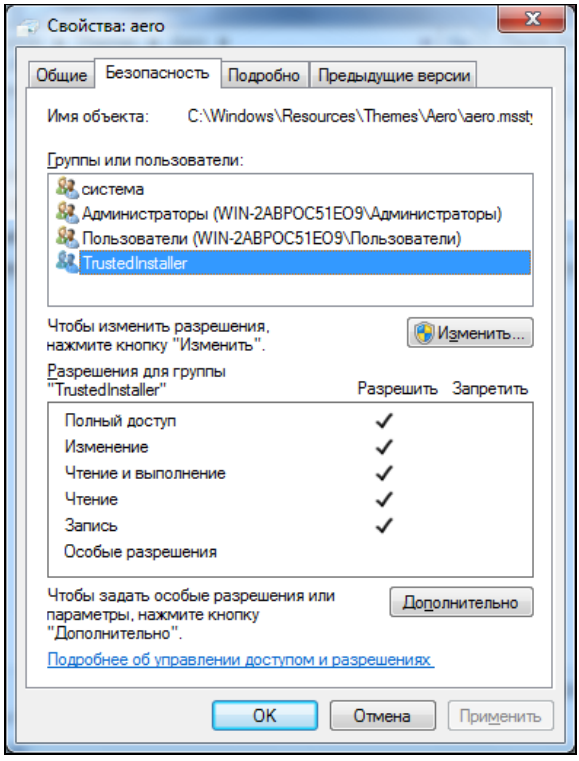


Рис. 2.9. Только TrustedInstaller имеет полные права на файл темы

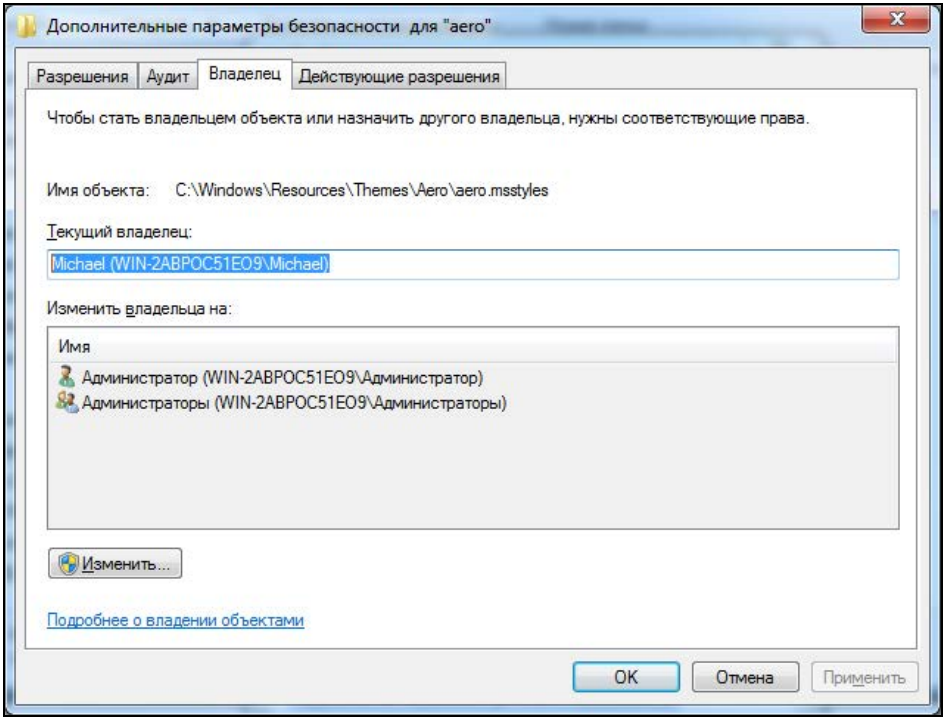


Рис. 2.10. Изменение владельца файла

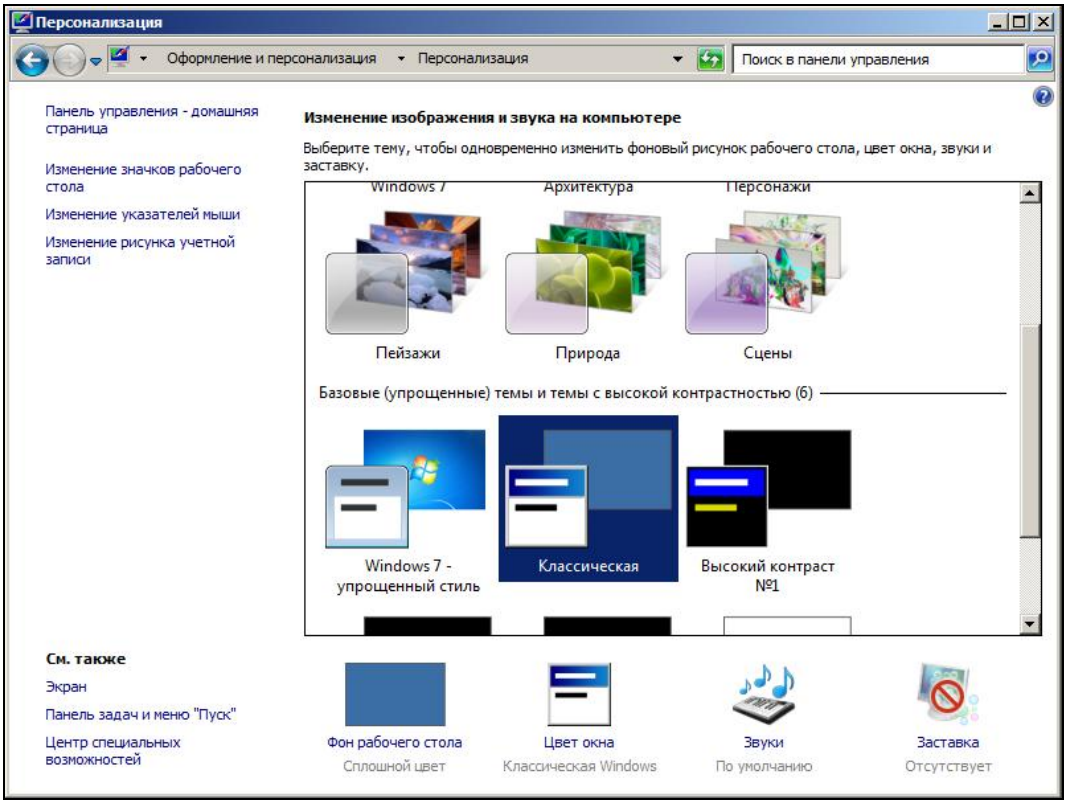


Рис. 2.11. Окно выбора тем

текущую тему на стандартную. Для этого щелкаем правой кнопкой мыши по рабочему столу и выбираем команду **Персонализация** (Personalize). Перед вами откроется окно выбора тем Windows, как на рис. 2.11.

Нужно выбрать классическую тему **Классическая** (Windows Classic), чтобы ОС не использовала свою графическую систему Aqua. Но и в этом случае вы не сможете изменить aero.msstyles, потому что он все еще используется рабочим столом. Нажмите комбинацию клавиш <Ctrl>+<Alt>+<Esc>, и перед вами должно открыться окно Диспетчера задач сразу на вкладке процессов. Найдите в нем explorer.exe и "убейте" его, только сначала не забудьте запустить Total Commander или любой другой файловый менеджер, иначе убийство рабочего стола будет бессмысленным, хотя и беспощадным.

Процесс explorer.exe отвечает за рабочий стол, поэтому с него уйдут такие удобные функции как панель задач, и не будет работать **Компьютер**. Так что копирование файлов окажется проблематичным. Именно поэтому я рекомендовал вам иметь под рукой какой-нибудь файловый менеджер.

Вот теперь изменение aero.msstyles становится возможным, и вы можете его заменить своей версией. Как только вы произвели подмену, снова запустите Диспетчер задач (Task Manager) и выберите в нем меню **Файл | Новая задача (Выполнить)**

(File | New task (Run)). Перед вами появится окно запуска новой задачи (рис. 2.12), которое похоже на то, что мы видели при выполнении команды **Пуск | Выполнить** в Windows XP. В этом окне введите explorer.exe и запустите его. Рабочий стол снова "запустится", и вы можете вернуть ему тему Aqua.

Таким образом, мы можем создать свою тему на основе стандартной, и она без проблем будет устанавливаться в систему. Хотя без сложностей можно обойтись в случае Windows XP. Как видите, в Windows 7 проблемы появились и очень серьезные. Наверное, поэтому в Интернете не так уж и много хороших тем для системы, и все, что мы видим, — это банальная смена фона рабочего стола и изменения цветовой гаммы. Что-то большее даже сама Microsoft не предоставляет. А зря. ОС Windows всегда славилась открытостью к пользователю (хотя и не бесплатностью), и из нее можно было лепить что угодно. Это была реальная платформа для построения чего-то собственного и индивидуального.

Создание новой темы с помощью редактора ресурсов — достаточно сложная, не очень удобная и кропотливая процедура. Нужно сохранять каждый рисунок в отдельности, редактировать его в графическом редакторе, а потом снова загружать в файл ресурсов.

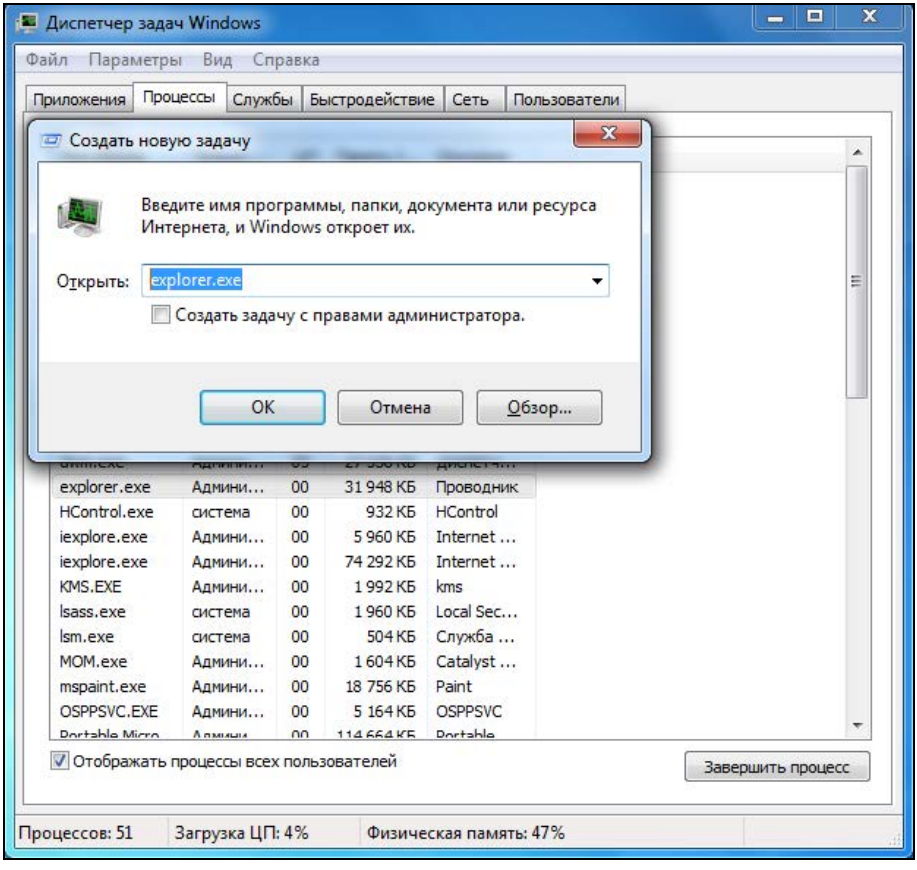


Рис. 2.12. Окно выбора тем

2.4. Оболочка

Следующий файл, который мы будем редактировать, — shell32.dll. Это файл оболочки. В нем еще больше интересных ресурсов, которые пользователь видит каждый день. Файл shell32.dll находится в папке \Windows\System32. Откройте этот файл в программе Restorator, и вы сразу же увидите множество разделов. Рассмотрим каждый из них в отдельности и взглянем, что там есть интересного.

2.4.1. AVI

В этом разделе находятся видеоклипы в формате AVI. Анимацию из них можно увидеть во время поиска файлов и компьютеров в сетевом окружении в момент удаления или копирования файлов. AVI-файлы легко редактируются, но при наличии графических программ, которые стоят дорого, поэтому я использую CyD WEB Animation Studio или GIF Studio Pro (**http://www.cydsoft.com/**). Эти программы вы найдете в электронном архиве к книге, в каталоге \Soft. Оба пакета предназначены для работы с GIF-файлами, но умеют читать и сохранять и AVI. Это значит, что вы можете превратить в AVI любую GIF-анимацию, найденную в Интернете.

Единственный недостаток этой программы — не сохраняется цвет прозрачности. Но нежелательный фон легко изменить и сделать более привлекательным, тогда он впишется в любое окно. Например, можно нарисовать каждому фрейму красивую рамочку.

Если для редактирования видеофайлов вы будете использовать другую программу, то при сохранении ни в коем случае не используйте режим сжатия, потому что система не работает с такими файлами и при воспроизведении не использует кодеки. В крайнем случае можно попробовать установить алгоритм сжатия Microsoft RLE.

2.4.2. Картинки

В разделе **Bitmap** снова множество картинок. Тут и изображения кнопок для панели задач и обозревателя (ресурсы 204—228), и анимационная картинка логотипа в обозревателе (ресурсы 240—247), помимо этого масса фоновых рисунков для различных окон Windows. Советую обратить внимание на рисунок 14351 — фон окна, которое вы видите при закрытии ОС Windows.

Не каждая версия Windows использует все картинки. Например, в Windows 2000 нет ресурса 14351, потому что для выхода из системы используется простое окно (без рисунка).

2.4.3. Меню

В разделе **Menu** можно увидеть различные меню. Например, под номером 197 находится всплывающее меню, которое появляется после перетаскивания файла правой кнопкой мыши.

В нем четыре пункта, которые можно подменить:

- **Copy here** (Копировать) — "Клонировать";
- **Move here** (Переместить) — "Бегом сюда";
- **Create Shortcut Here** (Создать ярлык) — "Запомнить ссылочку";
- **Cancel** (Отмена) — "Я передумал" или "Да ну его...".

Таким образом, можно откорректировать все основные меню, которые пользователь видит при работе в Проводнике.

2.4.4. Dialog

В этом разделе находятся все диалоговые окна, которые видны при работе с Windows. Например, под номером 1003 находится окно, которое появляется при нажатии кнопки **Start** (Пуск) и вводе команды в строке поиска. Диалоговых окон просто громадное количество, и редактировать есть что.

Очень часто в качестве текста в различных элементах управления используются специальные символы. Они начинаются со знака `%`, после которого идет буква (чаще всего `s`). Такие символы в реальной жизни будут подменяться чем-то другим. Например, в текстовом заголовке "`&Current user (%s)`" комбинация `%s` как раз указывает место, в которое будет подставляться имя пользователя в окне.

2.4.5. String

В разделе **String**, как всегда, множество строк, и снова я покажу, в какую сторону двигаться, чтобы улучшить их. Откроем ресурс под номером 5. Здесь есть сообщение под номером 65, которое выглядит следующим образом: "Are you sure you want to delete it?" (Вы действительно хотите удалить это?). Звучит как-то по-детски. Не лучше ли заменить это уведомление чем-то вроде "Стиратель готов к работе, начать рециркуляцию?"

Все сообщения, которые вы найдете в этом разделе, можно увидеть, работая в Проводнике, при выполнении операций копирования/удаления файлов и др. Если вы не установили файловый менеджер (типа Windows Commander), а пользуетесь средствами Windows, то с этими сообщениями вы встречаетесь каждый день, и стоит сделать их выразительнее.

2.4.6. Icon

Уже понятно, что здесь находятся значки. Их вы можете увидеть у ярлычков в Проводнике (Windows Explorer), Панели управления (Control Panel) или окне **Компьютер** (Computer). В Windows XP они достаточно красивы и вписываются в тему, но если вы установили Style XP и тему в манере Mac или Linux, то вполне логичным будет поменять все значки и сделать их в таком же стиле. Тогда система будет полностью гармоничной.

Лично мне больше по душе стиль, используемый в компьютерах Apple, и Windows я тоже превратил в подобие Mac OS X. Я знаю людей, которые чаще работают в Linux и делают все, чтобы не забывать о своей любви, даже когда работают в Windows.

Как видите, полный тюнинг системы возможен только при ручном редактировании ресурсов основных системных файлов.

2.5. Памятка

С помощью редакторов ресурсов можно не только украшать программы. Некоторые хакеры, используя их, занимаются локализацией программ на различные языки и, по слухам, неплохо зарабатывают. Хотя с чего тут зарабатывать, когда этот софт становится пиратским. От такой работы только удобство для пользователя, а для фирмы-производителя — убытки.

Лично я редактирую ресурсы только для собственного использования и не распространяю свои работы в Интернете (и не собираюсь этого делать!).

Помните, что когда вы вмешиваетесь в ресурсы, то модифицируете запускаемый файл. Иногда даже незначительные изменения могут нарушить работу всей программы и повлиять на ее стабильность. Именно поэтому всегда нужно делать резервную копию исполняемого файла. Программа Restorator, которую мы рассматривали в этой главе, делает это автоматически. Но не стоит надеяться на компьютер, и перед каждым редактированием нужно делать собственную копию.

Я также напоминаю, что изменение запускаемого файла может привести к нарушению лицензионного соглашения, а это грозит тем, что фирма не будет производить поддержку измененного продукта. В некоторых странах невыполнение условий такого договора может приводить к более печальным последствиям (к каким именно, зависит от степени нарушения).

Но надо учитывать тот факт, что производитель не может учесть потребности всех, поэтому эти нужды усредняются. Мы же можем для себя решить некоторые проблемы юзабилити с помощью редактирования ресурсов любимой программы.

ГЛАВА 3

Шутки над друзьями

Шуточки являются одним из способов самовыражения. Лично я очень люблю хорошие компьютерные шутки, с радостью могу позабавиться над друзьями и с удовольствием смеюсь, когда шутят надо мной.

Сразу хочу предупредить, что в моем понимании ради шутки можно затормаживать работу компьютера, временно запрещать запуск, организовать циклическую его перезагрузку и т. д. Нельзя только уничтожать информацию, ломать железо или окончательно выводить его из строя без возможности восстановления. Это уже не только не смешно, но и подло, глупо, если не сказать большего, и я бы сказал, но редактор все равно вырежет все, что я думаю о подлости, потому что такое нельзя печатать :).

Лучшие шутки — это те, которые вызывают улыбки и смех, но и их нужно пробовать на опытных специалистах. Шутить над неуверенными и мало знающими пользователями не этично, хотя иногда уж очень забавно.

Мало понимающие в компьютерах (как их принято называть, ламеры) как маленькие дети, потому что, сами не подозревая, иногда говорят или делают что-то очень смешное, что специально придумать очень сложно.

Некоторые эксперименты достаточно опасны с точки зрения стабильности работы железа, и эта информация дается только в познавательных целях. Не применяйте приведенные способы на практике, если не имеете достаточного опыта и не уверены в своих силах, дабы не превратиться из шутника в подлеца.

> ***Внимание!***
>
> Если будет описываться нечто, требующее вскрытия системного блока, то не забудьте выключить компьютер. Компоненты компьютера находятся под напряжением, и это может быть опасно для вашей жизни.

Ну вот, я хоть и не Минздрав, но вроде бы всех предупредил, и можно переходить непосредственно к информационной части этой главы.

3.1. Шутки с мышью

Самая классическая шутка 90-х годов с мышью — мышка без шарика. Просто вытащите его из мыши, и она перестанет работать. Когда пользователь начнет ее дергать, то не сразу догадается, что она пустая. Профессионалы тотчас замечают, что мышь стала слишком легкой (вес шарика составляет почти половину веса всей мыши), и раскроют эту шутку.

Вы не знаете, где у мыши может быть шарик? Вам повезло, потому что вы уже не застали это чудо компьютерной техники. Это сейчас все хвостатые оптические, а раньше они были шариковые, как ручки, и постоянно засорялись.

Еще одна классическая и одна из самых популярных шуток — подмена проводов. Спрячьте куда-нибудь подсоединенную к компьютеру мышь (не отсоединяя ее). Если используется компьютерный стол, то можно закинуть за него и спрятать провод. Теперь на это место кладем другую (бутафорию), а провод тоже забрасываем за стол, чтобы создать впечатление, что устройство включено в компьютер. Главное, чтобы мыши были похожи. Когда жертва сядет за компьютер, то схватится за бутафорскую мышь, и будет думать, что она не работает. Разгадать проблему очень сложно, потому что компьютер не ругается (мышь-то подключена), и если взглянуть на корпус сзади, то в разъеме будет торчать штекер.

Точно также можно поступить и с клавиатурой, только ее спрятать труднее. Если положить ее за компьютер, то подмена быстро раскроется. Но тут можно поступить немного иначе — выдернуть штекер клавиатуры и спрятать его, а в разъем от клавиатуры воткнуть мышь.

Современные мыши и клавиатуры в основном подключаются по USB и поэтому подменять не так уж и сложно. Ведь главное, чтобы из USB торчали провода. Хуже, когда мышь или клавиатура (или обе сразу) беспроводные. Тут уже сложнее произвести подмену.

Когда я писал первое издание, самыми популярными мышками были шариковые, и я предупреждал, что нужно торопиться с шариковыми шутками, потому что эти мыши выходят из моды. Так вот, мыши с проводами так же выходят из моды и продажи, так что скоро шутка с USB-проводами устареет. А жаль, лично я если и использую мышь, то только проводную, потому что у беспроводных постоянно в неудачный момент садятся батарейки. Я же использую только ноутбуки, поэтому уже давно привык к тачпаду.

Но оптика тоже имеет свои недостатки. Переверните оптическую мышку, и вы увидите посередине углубление с линзой. Простейший способ — заклеить линзу чем-то тонким и непрозрачным (например, цветным скотчем). Мышь перестает работать, а, по моим наблюдениям, на линзу обращают внимание в последнюю очередь. Дно мышки продолжает светиться, потому что у большинства оно прозрачное, но вот сама сердцевина не прозрачна. Эффект получается как с вытаскиванием шарика из старых мышек, только там было значительное изменение веса, а тут нет.

Если у вас есть двухсторонний скотч, то можно приклеить мышь к столу или коврику. Конечно, такая шутка раскроется быстро, но эффект от нее не меньше.

Ваши коллеги или друзья с хорошим чувством юмора должны оценить это по достоинству.

Вот еще один вариант. В настройках системы установите мышь для левши. Для этого запустите установку ее свойств, вызвав команды **Пуск | Панель управления | Все элементы панели управления | Мышь** (или **Пуск | Панель управления | Оформление и персонализация | Персонализация | Мышь**). Перед вами откроется окно конфигурирования параметров мыши (рис. 3.1). Установите флажок **Обменять назначение кнопок**. Теперь левая кнопка будет выполнять функции правой, и наоборот. Это весьма простая шутка, которая сработает только над начинающими.

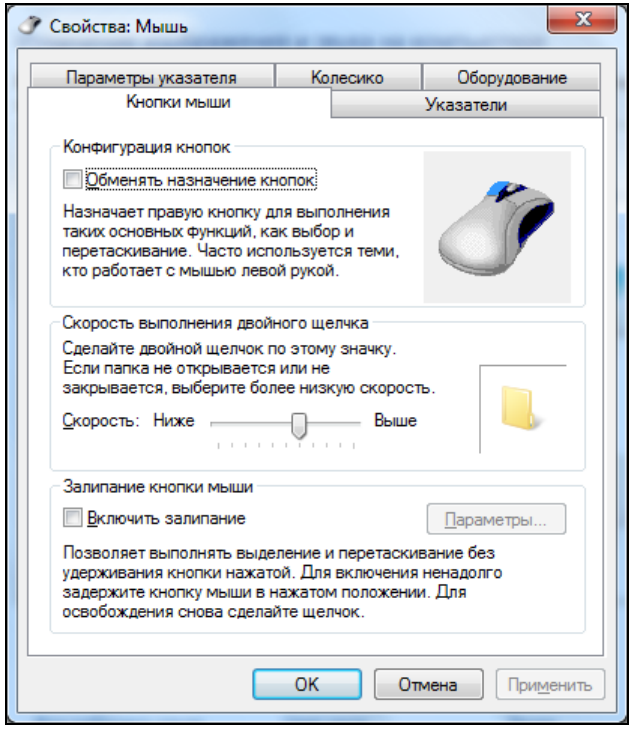


Рис. 3.1. Настройки параметров мыши

В настройках мыши можно еще установить параметр **Скорость выполнения двойного щелчка** в максимально возможное положение **Выше**. Это потребует от пользователя хорошей сноровки. Когда я передвинул в это положение ползунок на своем компьютере, то, как бы быстро я не нажимал, мне не удавалось сделать двойной щелчок.

Почему-то шутки с клавиатурами и мышами очень популярны на 1-е апреля. Мне приходилось видеть подобные шутки как в России, так и в Канаде. Несмотря на то, что все уже давно знают, на последнее 1-е апреля у нас на работе тестер прошелся с утра и отключил всем, кто пришел позже него, мыши.

3.2. Железные шутки

Следующие "шалости" требуют вмешательства в железо компьютера. Именно поэтому для реализации описанных здесь приемов понадобится свободный доступ к компьютеру и возможность вскрытия корпуса системного блока, поэтому удобнее дождаться, чтобы друзья вышли в другую комнату, или прийти на работу раньше всех. Конечно же, вам еще понадобятся знания компьютера.

3.2.1. Смерть видео

Для затравки раскрутите корпус компьютера. Теперь чуть-чуть открутите винтик от видеокарты, немного приподнимите ее из разъема и закройте корпус. Вытаскивать нужно совсем чуть-чуть. Я последний раз делал это лет десять назад на видеокарте NVIDIA и материнской плате ASUS. Достаточно, чтобы карта хотя бы с одной стороны выглядывала на миллиметр или два. На первый взгляд все на месте, а компьютер загрузиться не сможет. При старте будут раздаваться только звуковые сигналы и никаких движений.

Если вы не знаете, где находится видеокарта, то эту плату легко определить: достаточно посмотреть, к чему подключен монитор, но я надеюсь, вы обладаете немного большим опытом.

Самое главное в этой шутке, что неисправность сможет определить только человек, очень хорошо знающий значения сигналов установленной материнской платы. Остальные будут искать проблему очень долго, потому что все на месте, а такой маленький перекос определить сразу сложно.

Чтобы пощекотать нервишки даже профессионалу, можно отключить PC-Speaker, через который идет звук. Это маленький динамик, расположенный внутри компьютера. Очень часто он прикреплен к днищу системного блока или находится внизу передней панели. Лично я всегда в своем компьютере выдергиваю из этого динамика провода, чтобы он не доставал своими неприятными звуками. Для нормального озвучивания существует звуковая карта и человеческие колонки, правда об ошибках загрузки, например о неполадках с видеокартой, вызванных описанной только что шуткой, через звуковую карту не сообщается.

3.2.2. ATX — не защита

Давным-давно, в тридевятом царстве, в тридесятом государстве, т. е. в России, я работал в одной компании, где у меня был начальник с хорошим чувством юмора. Однажды заместитель начальника надел на ушки для навесного замка винтик, закрутил гайкой и сбил резьбу (ну не было под рукой замка). Он сделал это для того, чтобы защитить корпус своего компьютера от посягательств с моей стороны, ведь я постоянно делал что-то с внутренностями его компьютера.

Но он забыл, что бывают модели корпусов (тогда это были ATX, сейчас уже не знаю, есть ли названия у того зоопарка корпусов, которые представлены на рынке),

у которых без проблем снимается верхняя крышка и передняя панель, и их блокировать просто не имеет смысла.

Я снял кожух, одну боковую стенку (вторая закрыта на винт) и переднюю панель. В его компьютере три пятидюймовых отсека. В верхнем стоит CD-ROM, а через остальные два видно все внутренности. Я залез туда рукой и на ощупь отключил питание с флоппи-диска. Вскоре после этого я вытащил из мусорного ящика целую пачку дискет, потому что он думал, что они испорчены, а реально не работал дисковод. Помимо этого, я получил благодарность от соратников по работе за сообразительность и лишился премии за наглость :).

3.2.3. Чуть отключим

Можно вытащить из материнской платы батарейку. Компьютер-то работать будет, а вот все настройки и время будут сбрасываться после каждого выключения. Первые два дня пользователь будет вспоминать "добрыми словами" всех своих родственников и Билла Гейтса (ну любят пользователи Windows вспоминать его), пока не поменяет заветную батарейку в системном блоке.

Переходим к следующему приколу. Совсем чуть-чуть выдвигаем разъем из монитора. Компьютер работоспособен, но откликаться ни на что не хочет.

Вообще, существует много мест, где можно приложить свои шаловливые ручки методом "отключить совсем чуть-чуть". Очень удобно вытаскивать вилку питания из принтера. Гнездо там глубокое, поэтому после извлечения нужно просто приставить его к розетке. Вроде все нормально, но не работает.

Однако не советую слишком увлекаться экспериментами с проводами питания. Если между контактами проскочит искра, то может выгореть компьютер и устройство, которое вы отключили, но не убрали кабель (например, тот же монитор). Особенно горит китайское безымянное "Made in Гараж".

Если у вас появился полный доступ к внутренностям компьютера жертвы, то тут шутки приобретают совершенно иной размах. Вы можете поменять местами на материнской плате колодки кнопок Reset и включение питания. Таким образом, даже сообразительный человек не с первого нажатия сможет догадаться, в чем проблема, и почему компьютер не запускается по кнопке Power On.

Отключить можно все, начиная от дисководов и приводов CD-ROM и заканчивая вентилятором на процессоре. Мне больше всего нравится последнее, потому что если на материнской плате стоит процессор Intel, то он через некоторое время после запуска просто останавливается при перегреве процессора. В этот момент происходит эффект зависания или компьютер вообще выключается.

Если вы не уверены в железе жертвы, то не советую играть с охлаждением, потому что можно что-то спалить (некоторые модели процессоров AMD не отключались и сгорали). В этом случае за неудачную шутку у вас под глазами могут проявиться синие кружочки, а также возможен побочный эффект в виде сотрясения мозга :). Так что особо злостным шутникам следует заниматься спортом из серии боевых искусств.

3.2.4. Монитор

У некоторых мониторов яркость убирается полностью, и остается черный экран. Если убрать яркость, то монитор по всем признакам работает, но информация не отображается. Это единственная шутка, на которую я попался, и долгое время не смог понять, в чем дело. Я прыгал вокруг компьютера, колдовал, проверял кабели, но все работало, а изображения не было. Воспроизводилось только меню монитора, но мне даже в голову не пришло проверить яркость и контрастность :(.

Наконец мой обидчик не выдержал и с диким смехом показал на кнопки управления параметрами монитора. После этого я несколько дней подряд жестоко мстил за себя, потому что так меня еще никто не мог провести.

Мониторы FLATRON 795FT (который был у меня в тот момент) уже встретить сложно, а во всех современных экранах, которые я проверял, невозможно убрать яркость до такого уровня, чтобы экран был абсолютно черным.

Могу еще посоветовать положить магнит позади монитора, чтобы его не было видно. В этом случае он будет давать страшные наводки, и глаза моментально будут уставать. Жертва будет ругаться и плеваться на производителя, но никто из моих подопытных кроликов не догадался о причинах происходящего. Но помни, что не каждый магнит оказывает такое воздействие и не каждый монитор на них реагирует. Я не электронщик, и объяснить это не могу.

Если магнит не будет найден, то вытащите его сами, иначе человек может испортить зрение, а это уже не смешно. Со здоровьем шутить нельзя, поэтому данную процедуру нужно проводить кратковременно, да и эффект от этого будет больше.

Бояться этого метода тоже не стоит. Для того чтобы магнит испортил зрение, он должен пролежать очень долго, а пользователь должен по 8 часов проводить за компьютером, не отходя на перекуры и обеды. Например, у меня на работе при включении большого кондиционера (более 2 метров длиной, мощность не знаю) на монитор идут наводки, и он постоянно дергается, как от магнита. И так я работаю все лето уже в течение двух лет. Без кондиционера нельзя, потому что жара в моих широтах достаточно сильная (летом в среднем по 40 °C), но и с ним тяжело из-за наводок.

И все же со здоровьем лучше не шутить. Если жертва не заметит мерцания, то продолжать шутку смысла нет. Лучше вытащить магнит и честно признаться. Даже если мерцание будет заметно и жертва начнет волноваться и веселить народ поисками неисправности, то затягивать шутку тоже нежелательно.

3.2.5. Турбовентилятор

Как же многих раздражает громкий вентилятор! Видимо эти люди не встречались со мной. Сейчас шутки с вентилятором — мои самые любимые. Недавно мне подкинули свежую идею, в которую я влюбился до кончиков ногтей :).

Найдите где-нибудь пластмассовую линейку и отломите от нее несколько маленьких кусочков. Потом забросьте их в вентилятор блока питания и ждите, когда

жертва включит компьютер. Грохот будет стоять такой, что глаза от страха могут вылезти на лоб :). Но если гула не будет, то срочно выключайте компьютер. Возможно, что вентилятор просто заклинило, и тогда блок питания может сгореть, а нам этого допускать нельзя. Мы шутники, а не злодеи какие-то. Именно поэтому старайтесь не переборщить с запчастями, которые подкидываете в вентилятор.

Когда я протестировал эту затею на своем приятеле, то он сначала испугался, потом долго смеялся, а вслед за тем так возбудился, что повесил на решетку от вентилятора полоски туалетной бумаги и тонкой фольги от шоколада. Теперь вентилятор дует на всю эту гирлянду, и за системным блоком стоит сумасшедший гул, а он наслаждается этими звуками. Вроде, как мелодии какие-то слышит :). Вот сижу и думаю, может записать его завтра на прием к психиатру, а то Интернет совсем с ума сведет хорошего человека.

В принципе, бумагу и фольгу можно использовать и ради шутки. Когда человек не знает, что к сетке, за которой прячется пропеллер, прикручена фольга, и услышит шум, может получить и саечку за испуг.

3.2.6. Суперскотч

На старой работе, перед самым увольнением я написал программу, которая печатала на этикеточном принтере баркоды, PDF-коды и информацию о продукции. Принтер должен был распечатывать все эти данные на самоклеющихся этикетках, которые операторы потом прикрепляли на коробки с продукцией.

К чему это я? А к тому, что такая этикетка-самоклейка прилипает к чему угодно, да так, что отодрать ее проблематично. Сначала мы склеивали ящики в столах, чтобы они не открывались. Потом занялись розетками и, в конце концов, компьютерами. Тут первой досталось кнопке старта компьютера, ее заклеивали двойным и тройным слоем. Следом — все дисководы, приводы CD-ROM и разъемы системного блока (USB, LPT и т. д.).

Если нет самоклеющейся этикетки, то можно воспользоваться скотчем. Так я одному парнишке уже на новой работе весь системный блок обмотал скотчем. Пришлось употребить весь рулон. Как он маялся, когда разматывал все это :). Мои же мучения стоили того, чтобы увидеть, как освобождают системный блок от рулона скотча. Но самое интересное случается, если под рукой нет ножниц, и ленту не выходит срезать.

Но больше всего мне понравилось заклеивать дисководы. Это нужно делать аккуратно, чтобы вашу работу не было видно. Если скотч прозрачный, то он незаметен, и дисковод кажется пустым, но при этом вставить туда дискету проблематично.

3.2.7. Мультикнопочник

У меня на компьютере три кнопки "пуск" и четыре кнопки Reset :). Зачем столько и откуда они взялись? Все очень просто. Только одна из них рабочая, а все остальные — это просто рисунок, распечатанный на бумаге и аккуратно наклеенный на

системный блок. Я-то знаю, какая кнопка настоящая, а все остальные, кто пытается включить компьютер, впадают в панику или начинают нажимать на все подряд.

При реализации данной шутки главное, чтобы изображение было хорошего качества. Рисунок может не соответствовать подлинному образцу, и кнопка может иметь другую конфигурацию. Можно обклеить корпус картинками кнопок различных форм.

Чуть позже я пошел еще дальше. На работе у меня кнопка пустая, потому что сам выключатель я снял и вывел на проводах сбоку компьютера. Тот, кто не знает, начинает тыкать в кнопку "пуск", а компьютер не запускается. Таким образом, я не только прикалываюсь над другими, но и защищаюсь, потому что чужой человек не сможет включить без меня компьютер. И нечего им лазать по моим файлам, это моя приватность.

3.3. Сетевые шутки

Опять же возвращаемся на 10 лет назад в тридесятое государство. Мы с заместителем начальника отдела находились на большом расстоянии друг от друга (в разных зданиях), и он постоянно звонил мне, чтобы загрузить своей очередной проблемой, связанной с программированием на Visual C++. Телефон стоит не на моем столе, и чтобы постоянно не вставать, я показал ему, как пользоваться командой `net send` (отправлять сообщения по сети). Если вы не слышали об этой команде, то для отправки сообщения нужно написать в командной строке так:

```
Net send Адрес Текст_сообщения
```

Выполняете эту директиву в любой командной строке, и у адресата появляется окно с текстом вашего сообщения. Это работает только в NT-системах (Windows NT/2000/XP/2003), но сейчас в большинстве сетей это не проблема (начиная с Windows Vista, эта команда не поддерживается). Если же у вас используется Windows 9*x*, то можно только посочувствовать и поплакать над этим горем. (Правда, представить, что у кого-то еще жив этот раритет, довольно трудно.)

Итак, не проходит и недели, как меня замначальника забросал таким количеством сообщений, что нервы не выдержали. Вы не представляете, как меня бесит, когда во время войны с очередным монстром появляется окно с вопросом, а игра сворачивается. Недолго думая, я написал небольшую программу на Delphi. На форме у меня была только одна кнопка, по нажатию которой выполнялся следующий код:

```
var
 i:Integer;
begin
 for i:=0 to 10 do
  begin
   WinExec('NET SEND 10.1.1.15 Ты будешь страдать каждый день', SW_SHOW);
   sleep(1000);
  end;
end;
```

Этот же код на C++ выглядит следующим образом:

```
for (int i=0; i<10; i++)
{
    WinExec("NET SEND 192.168.1.121 You will be cry by me", SW_SHOW);
    Sleep(1000);
}
```

Здесь запускается цикл из 10 шагов, в котором с перерывом в 1000 миллисекунд отправляется сообщение на адрес 192.168.1.121. Если убрать строку с задержкой, то экран бедной жертвы засыплет сообщениями так, что та не сможет работать. Хотя и без этого достаточно. А можно написать код еще злее — сделать цикл бесконечным, тогда прервать программу можно будет, только сняв задачу.

Вы можете написать что-то подобное на любом языке программирования, на это много времени не потребуется. В принципе, можно создать даже командный файл. Тут все уже зависит от ваших знаний и умений.

Если в вашей сети к компьютерам подключены принтеры, а администраторы полные "чайники", то можно поиграть и с этими устройствами. По умолчанию любой в Windows локальный принтер становится доступным по сети вплоть до Windows XP, и это делает его хорошей мишенью для шутки. Да и сейчас принтеры очень часто открывают для общего доступа в локальных сетях, потому что на первый взгляд это очень безобидное устройство.

Зайдите через сетевое окружение на компьютер жертвы и дважды щелкните по его принтеру. Он установится в вашу систему, и вы сможете без проблем пользоваться им. Только не надо отправлять на него картинки или текст, потому что этим вы сразу же выдадите сетевое происхождение напечатанного документа. Пользователь может зайти в Диспетчер печати (Print Manager) и успеть увидеть источник задания. Уж лучше каждые пятнадцать минут направляйте на печать пустую страницу, которая обработается достаточно быстро и незаметно. Вот этим вы заставите пользователя задуматься о неисправности принтера или драйвера. Повторяйте эту операцию, пока пострадавший не догадается, или вам не надоест смеяться. Можно отправлять на печать тестовую страницу, меньше шансов выдать себя.

Как видите, очевидные варианты — не всегда самые прикольные. Иногда лучше немного подумать и сделать что-то действительно оригинальное, и при этом не выдать себя, иначе можно начать войну. Вам тоже могут отомстить и подшучивать над вашим компьютером.

Классической шуткой в сети является отправка сообщений от другого лица, например, через уже знакомую команду `NET SEND` (в данном случае мы будем использовать эту команду не для флуда, а для обмана зрения). Допустим, что вы работаете в небольшом офисе и хотите послать своему коллеге информацию от имени начальника. В этом случае необходимо, чтобы его компьютер был выключен (или хотя бы не находился в сети). Для этого есть три варианта:

- временно выдернуть сетевой шнур из компьютера босса. Но если в этот момент шефу что-нибудь понадобится, и он узнает, кто нарушил связь, то у вас могут возникнуть проблемы с получением очередной премии;

- проследить, когда босс будет перезагружать или выключит на время компьютер. Для этого можно воспользоваться программой CyD Careful Observer (ее можно скачать с **http://www.cydsoft.com/**), которая может наблюдать за компьютерами в сети, и при потере связи выдавать сообщения или запустить бесконечный ping;
- самый опасный метод — сменить IP-адрес вашего компьютера на такой же, как у начальника. Это вызовет конфликт, и оба компьютера могут быть выведены из сети. Подождите некоторое время. Шеф, скорее всего, начнет перезагрузку, чтобы разрешить ситуацию. Как только это произойдет, немедля еще раз поменяйте свой адрес на его.

Если вы добились временного выхода начальства из сети, нужно подменить имя своего компьютера. Для этого щелкните правой кнопкой мыши по строке **Компьютер** (Computer) в главном меню Windows, выберите пункт **Свойства** (Properties) и в появившемся окне слева выберите ссылку **Дополнительные параметры системы** (Advanced system settings). Перейдите на вкладку **Имя компьютера** (Computer Name) и щелкните по кнопке **Изменить** (Change). Здесь замените имя компьютера и нажмите кнопку **OK**.

Теперь, пока начальник перезагружается и отсутствует в сети, вы можете от его имени отправлять сообщения. Можно послать что-то типа "Зайди ко мне" или "Ты уволен". Получатель будет думать, что это руководитель шлет сообщения, и как минимум испугается.

Помните, что у вас в распоряжении не так уж много времени. Перезагрузка Windows идет примерно 3 минуты (или чуть больше/меньше, в зависимости от версии и замусоренности). Как только вы отправили сообщение, сразу верните на место имя компьютера и IP-адрес, т. к. компьютер начальства после перезагрузки снова может выдать ошибку из-за конфликта адресов или имен, и тогда администраторы сети начнут искать конфликт и выйдут на вас.

Если в сети используется электронная почта, то задача упрощается. В *разд. 5.5* мы будем рассматривать, как отправлять анонимные сообщения или письма от чужого имени, и я уверен, что коллеги поверят. Текст сообщения зависит от конкретной ситуации.

Когда подшучиваете с помощью сообщений, то выбирайте в качестве жертв людей с хорошим чувством юмора. Это поможет вам избежать лишних проблем и ссадин :).

3.4. Софт-шутки

В этом разделе мы рассмотрим способы подшутить над ОС Windows. Они наиболее просты в реализации, а эффект дают не менее интересный, чем те, что мы рассматривали ранее.

3.4.1. Искусственное зависание

Давайте сделаем копию рабочего стола вместе со значками и панелью, но без запущенных программ (клавиша <Print Screen>). Потом в любом графическом редакто-

ре выполните вставку из буфера обмена и сохраните копию экрана в файл в формате BMP. Теперь уберите с рабочего стола все значки и спрячьте панель с кнопкой **Пуск** (Start), чтобы ничего не осталось. Далее нужно установить в качестве фона сохраненную вами копию экрана. Даже профессионалы клевали на эту бутафорию. Интересно наблюдать, когда жертва пытается щелкнуть по значку или кнопке **Пуск** (Start), а ничего не происходит, потому что он тыкает в обои, а реальные ярлыки и панель спрятаны за пределами экрана.

3.4.2. Ярлыки

Я очень люблю приписывать ярлыкам совершенно другие программы. Для этого щелкните правой кнопкой мыши по ярлыку и в появившемся меню выберите пункт **Свойства** (Properties). Перейдите на вкладку **Ярлык** (Shortcut) и измените содержимое поля **Объект** (Target), указав здесь путь к другой программе (рис. 3.2). Лучше всего поменять местами значения этого свойства в двух разных ярлыках.

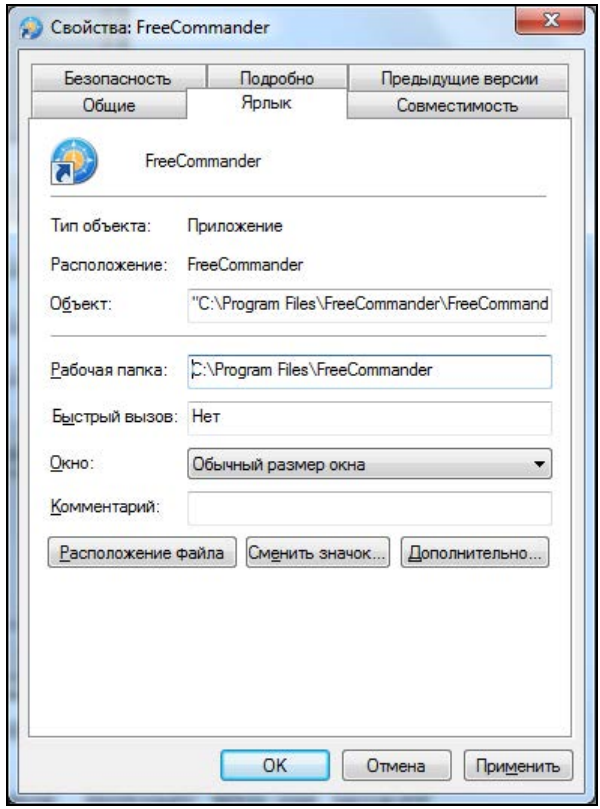


Рис. 3.2. Окно свойств ярлыка, открытое на вкладке **Ярлык**

Тут главное быть внимательным и не поменять значок, потому что он может автоматически измениться на тот, что используется в указанной вами программе. Если это произошло, то вернитесь к свойствам ярлыка и нажмите кнопку **Сменить зна-**

чок (Change Icon). Появится окно открытия файла. Найдите запускаемый файл программы, которая была до вашего вмешательства. ОС возьмет из нее значок.

Таким простым способом можно по выбору значка Microsoft Word запускать, например, Калькулятор (Calculator) или Блокнот (Notepad). Чаще всего пользователями овладевает недоумение, и только после нескольких перезапусков они догадываются, что их обманули.

3.4.3. Мусор на рабочем столе

Мой начальник постоянно держит все ссылки на документы, файлы и программы на рабочем столе. Когда там уже нет места и негде бросить очередной файл, скачанный из Интернета, он переустанавливает Windows. Получается, что загромождение рабочего стола является для него индикатором времени для переустановки ОС. Хороший показатель, не правда ли? Я бы до такого не догадался никогда.

Но это не единственный его недостаток. Он всегда и везде ставит простейший пароль — 11. Видимо, боится забыть. Недавно он усложнил нам задачу и начал устанавливать другой пароль — 1111. Его интеллектуальный уровень вырос, и он смог запомнить, что цифра повторяется четыре раза :).

Благодаря знанию пароля администратора легко пробраться на компьютер и сделать с ним (с компьютером) все, что угодно. Еще во времена Windows 98 он часто оставлял открытым диск C:, и тогда мы веселились через сеть по полной программе. Если у вас есть пароль администратора на чужой компьютер, но при этом в сетевом окружении не видно диска C:, то это дело поправимо.

Наберите в строке адреса окна сетевого окружения следующий путь:

```
\\Компьютер\c$
```

Здесь вместо `Компьютер` нужно указать имя или IP-адрес компьютера жертвы. Если пока нет прав доступа к диску, то перед вами может появиться окно для ввода имени пользователя и пароля. Укажите данные администратора, и весь диск окажется для вас полностью доступным.

Итак, получив доступ к диску, мы копировали по сети на его рабочий стол (C:\Documents and Settings\All Users\Desktop для Windows 7) кучу маленьких файлов, ссылок и документов. Попробуйте и вы проделать это с кем-нибудь. Интересно наблюдать за человеком, у которого прямо на глазах на рабочем столе появляется разный мусор.

Если нет доступа к компьютеру по сети, но вы можете воспользоваться его клавиатурой (в перерыв или пока хозяин куда-то вышел), то можно, заранее подготовившись, пойти другим путем.

Создайте на рабочем столе файл с каким-либо заманчивым названием и расширением bat. В этот файл необходимо поместить следующий код:

```
md hi
md format
```

```
md c
md delete
...
```

Потом в свойствах ярлыка укажите какой-нибудь заманчивый значок и прячьтесь в ожидании жертвы.

Если вы сделали все очень привлекательно, то он запустит файл, и на рабочем столе появится множество бесполезных папок. А главное, что названия у них будут format, c, delete. Шок — это по-нашему!!!

3.4.4. Смерть Windows 9*x*

В 2005-м году я поменял работу и род деятельности и стал системным администратором. Просто надоело вкалывать программистом, и нужна была работа со свободным графиком, где можно было бы писать программы для себя и сочинять новые статьи и книги. Моей основной обязанностью было администрировать сеть из сорока компьютеров и двух серверов. Мой предшественник уехал в Москву и оставил все в совершенно запущенном состоянии. Только на двух компьютерах стоял Windows XP и на одном — Windows 2000 Professional. Все остальные машины управлялись из-под Windows 98. А конфигурация некоторых компьютеров — Pentium III с 32 Мбайт памяти. И это во времена, когда 512 Мбайт стоит копейки. Хочется посмотреть в глаза тому человеку, что выписывал счет на такую своеобразную комплектацию. Я бы ему "настучал по процессору" и "прочистил оперативку".

Я был в шоке, но переустанавливать систему никто не хотел, чтобы не останавливать работу.

Но мне подбросили одну великолепную идею, которая позволяет спокойно блокировать Windows 9*x*. Достаточно в корне диска C: создать пустой файл с именем win.com, и ОС больше сама не будет стартовать. Можно только насильственно указывать полный путь C:\Windows\win.com или удалять пустой бутафорский файл.

Вот так я последовательно кидал файл на все компьютеры, дамочки-пользователи кричали, что компьютеры сломались, а я забирал их на восстановление и устанавливал Windows 2000 или XP в зависимости от мощности процессора и количества памяти. Жаль, что меня уволили за то, что при мне компьютеры стали ломаться чаще, а ведь я это делал с добрыми намерениями и повысил надежность и безопасность сети. Шучу, меня не уволили, компания обанкротилась, но я был не причем.

Для большей достоверности желательно сделать свой файл win.com невидимым, чтобы какой-нибудь умник его не обнаружил и не уничтожил. Хотя на предприятиях дамочки не особо разбираются в файлах.

Сейчас уже Windows 9*x* встретить нереально, но если включить воображение, таким методом можно подменить многое. Можно сделать любую программу в Windows нерабочей.

3.4.5. Бутафория

В электронном архиве к книге в каталоге \Chapter3 вы можете найти программу IE.exe. Попробуйте запустить ее. Выглядит она как настоящий Internet Explorer, а реально эта программа написана мною за пять секунд. Ничего тут работать не будет, потому что все содержимое окна — это рисунок. Подсуньте этот файл жертве и измените в настройках значка Internet Explorer строку запуска так, чтобы исполнялся наш файл, а не стандартный IE из состава Windows.

Как только пострадавший попытается запустить программу, так слово "ишак" в отношении IE будет самым ласковым и нежным :).

Если вы дружите с программированием, то эту шутку сможете воспроизвести и сами с любой другой программой в такой последовательности:

1. Выберите программу, которой жертва пользуется чаще всего.
2. Снимите скриншот окна этой программы.
3. Создайте обычное приложение в Borland Delphi или любой другой среде программирования. На форме уберите область заголовка окна и элементы управления в ней, а в качестве фона (`background`) укажите скриншот. В случае с Delphi установите свойство `BorderStyle` в `bsNone`, поместите на форму компонент `TImage` и загрузите в него скриншот программы.

Бутафория готова, и ее можно подбрасывать своим друзьям.

> ***Примечание***
>
> Исходный код примера-шутки с Internet Explorer, написанный на C#, вы можете найти в каталоге \Chapter3\SharpIE.

3.4.6. Запланируй это

В Windows есть такая удобная оснастка, как Планировщик заданий (Scheduled Tasks). Ее вы можете найти в меню **Пуск | Все программы | Стандартные | Служебные | Назначение задания** (Start | All Programs | Accessories | System tools | Scheduled Tasks) или **Пуск | Панель управления | Администрирование | Планировщик заданий** (Start | Control Panel | Administrative tools).

Запустите эту оснастку, и вы увидите окно, похожее на отображенное на рис. 3.3.

В дереве заданий (слева) щелкните правой кнопкой мыши по строке **Библиотека планировщика заданий** (Task Scheduler Library) и выберите в контекстном меню пункт **Создать задачу** (Create Task). Первая вкладка информативная, где нужно указать имя задания. Постарайтесь выбрать что-то, не вызывающее подозрения. На второй вкладке (**Триггеры** (Triggers)) можно указать время, когда должна выполняться программа. Внизу окна нажмите кнопку **Создать** (New), и появится окно задания времени и периодичности выполнения задачи.

Ну а на вкладке **Действия** (Action) можно выбрать действия, которые будут выполняться в указанное время. Снова внизу окна есть кнопка **Создать** (New), которая

позволит задать программы или сценарии для выполнения. Можно задать сразу несколько программ. Нажмите кнопку **Создать** (New) и в появившемся окне задайте два параметра: **Действие** (Action) (по умолчанию установлено в запуск программ) и **Программа или сценарий** (Program/Script) — непосредственно файл для выполнения. Есть еще необязательные опции, которые в большинстве случаев просто не нужны.

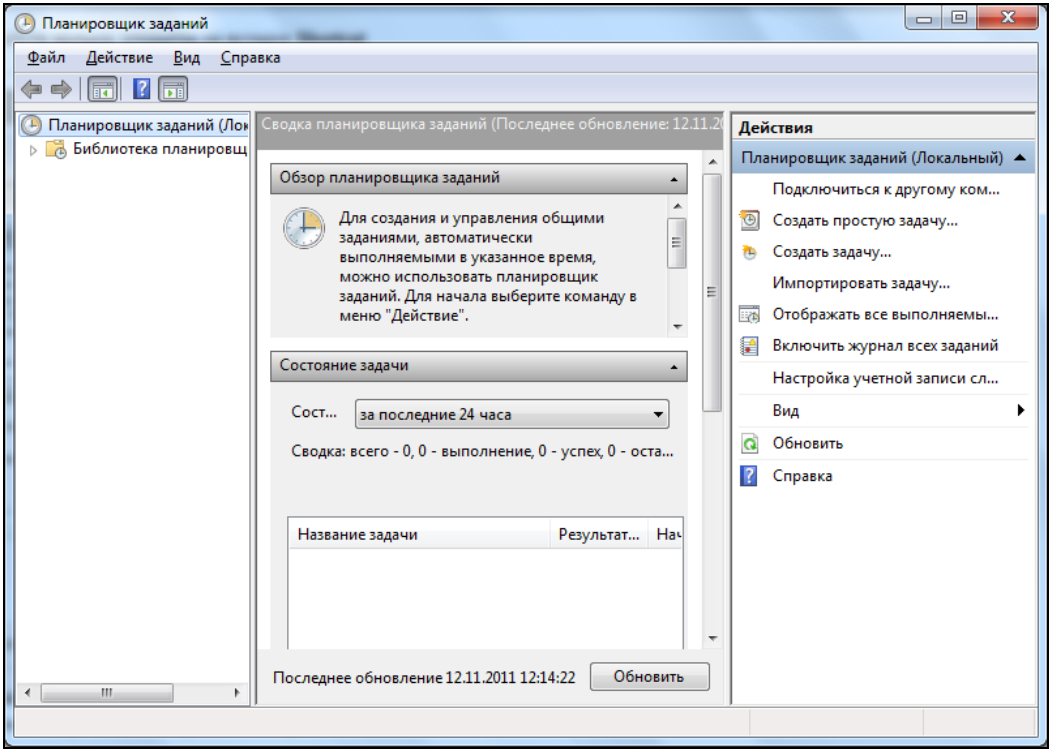


Рис. 3.3. Окно настройки запланированных задач

Завершите работу мастера. Теперь в заданное время будет запускаться указанная программа. Когда это будет происходить, пользователь станет теряться от неожиданности. И снова замелькают мысли о вирусах или барабашках в системном блоке :).

3.5. Шутейские ресурсы

Мы много времени потратили на изучение ресурсов *(см. главу 2)*, и эти знания пригодятся не только для изменения настроек системы, но и шутки ради. Забавляться таким способом хорошо над начинающими или просто ламерами. Они всегда читают надписи, которые видят, и доверяют им. Опытные пользователи знают наизусть программы, с которыми они работают, и им незачем лишний раз применять пункты меню, когда есть панели инструментов с кнопками и клавиши "горячего" вызова.

Другая категория — продвинутые пользователи. Они не первый день за компьютером, большинство надписей знают наизусть, но если они замечают что-то неладное, то это может их ввести в ступор. Я не раз встречал довольно знающих людей, которые на какую-то нестандартную мелочь начинают выдумывать сумасшедшие теории. Когда зависает машина, то некоторые умники начинают выводить теории багов, списывают на жучков в микросхемах, глючность материнки, а ведь проблема заключается всего лишь в ошибке программы.

3.5.1. Windows Total Commander

Самый распространенный файловый менеджер по умолчанию использует английский язык. Если я не ошибаюсь, то он реализован на Delphi (хотя это не имеет особого значения), и в коде прописан именно английский. Чтобы отображать другие языки, используются текстовые файлы, в которых все надписи даны в открытом и легко читаемом (а значит, и редактируемом) виде. Если вы используете английский язык, то вам нужно будет работать с файлами WCMD_ENG и редактировать именно их.

Точнее сказать, файлов для каждого национального языка (например, для России с именем WCMD_RUS) целых два: один с расширением mnu, а другой — lng.

В mnu-файле находятся заголовки для пунктов меню. Они выглядят примерно так:

```
POPUP "&Файл"
  MENUITEM "Изменить &атрибуты...", cm_SetAttrib
  MENUITEM "&Упаковать...\tALT+F5", cm_PackFiles
  MENUITEM "&Распаковать...\tALT+F9", cm_UnpackFiles
  ...
  ...
END_POPUP
```

Как видите, это полная копия текстового описания меню из ресурсов. Вы можете как минимум сделать более интересными названия пунктов меню, но это будет простым украшением. Наша задача — подшутить над пользователем, поэтому лучше измените клавиши быстрого вызова. На работу программы это не повлияет, но спутает все карты. Пользователь будет видеть в меню одни клавиши, а реально для вызова соответствующей команды нужно использовать другие.

Для полного счастья перетасуйте аккуратненько названия всех пунктов меню. Даже большинство опытных ребят знают наизусть не все "горячие" клавиши, и далеко не для всех пунктов меню есть кнопки на панели. Редко используемые команды никто запоминать не будет, поэтому хоть иногда приходится лезть в меню, а здесь названия перепутаны, и будут вызываться не те команды, которые ожидаются. Ну а если вашу программу запустит чайник, то он получит по полной программе. Слава Биллу, если этот лам не удалит все файлы со своего винчестера, что достаточно сложно. Постарайтесь оформить меню как можно интересней и перемешать все, что только попадет под мышь.

Результат — первое действие спектакля вызывает замешательство, а потом начинаются поиски вирусов и троянского коня.

Теперь поближе познакомимся с файлом WCMD_RUS.LNG. Это тоже текстовый файл, в каждой строчке которого находятся отдельные текстовые сообщения, которые можно увидеть во время работы с Windows Total Commander.

Тут тоже есть, где развернуться: поменять местами сообщения или просто изменить их, чтобы запутать бедную жертву. Вот несколько примеров:

- "Нельзя копировать файл сам в себя!" — можно заменить на "Копирование прошло удачно";
- "Копировать %i файл(а,ов) в:" — новый вариант "Переименовать/переместить %i файл(а,ов) в:";
- упаковку превратите в распаковку, перемещение в копирование и т. д.

Постарайтесь хорошенечко и отредактируйте все, что только мыслимо.

После того как закончите свой тяжелый труд, осмотритесь еще раз. Может, вам придет в голову еще более безрассудная идея. Хоть я и шутник со стажем, но глаз мог уже замылиться.

3.5.2. Темы Windows

В *главе 2* мы рассматривали, как редактировать темы Windows. Надеюсь, что вы прочитали эту главу полностью. Если что-то упустили, то неплохо было бы перечитать.

Итак, в прошлой главе вы увидели, что все элементы управления — это всего лишь картинки. Так кто нам мешает поменять эти картинки местами и из флажка (**CheckBox**) сделать переключатель (**RadioButton**) или еще что-нибудь подобное Как это будет выглядеть в Windows 7, показано на рис. 3.4. Я недавно проверил подобную шутку над заместителем начальника своего отдела и такое услышал про Билла Гейтса, что у всех в отделе долго потом уши болели. А когда он узнал, что над ним прикололись, то я уже хотел идти покупать себе костыли :). Замначальника у меня достаточно продвинутый, но просто не ожидал, что может так попасться.

Через пару дней я закрасил в ресурсах тем все компоненты цветом фона диалоговых окон. Таким образом, они стали сливаться с диалоговыми окнами, т. е. оказались невидимы. Посмотрите на рис. 3.5, где показано все то же окно настроек Windows Total Commander, в котором остались только надписи, а элементы управления просто исчезли. И вот так во всех окнах Windows.

В ресурсах тем Windows очень много интересного, попробуйте поковыряться самостоятельно. Я дал вам пищу для размышления, а как вы этим воспользуетесь, зависит от вас. Главное — включить свое воображение и использовать его в правильном направлении.

Может быть, поэтому Microsoft защищает свои файлы тем? Хотя я что-то не припоминаю никаких вирусов или троянских коней, которые бы портили темы. Но если быть честным, то я и с вирусами не особо знаком.

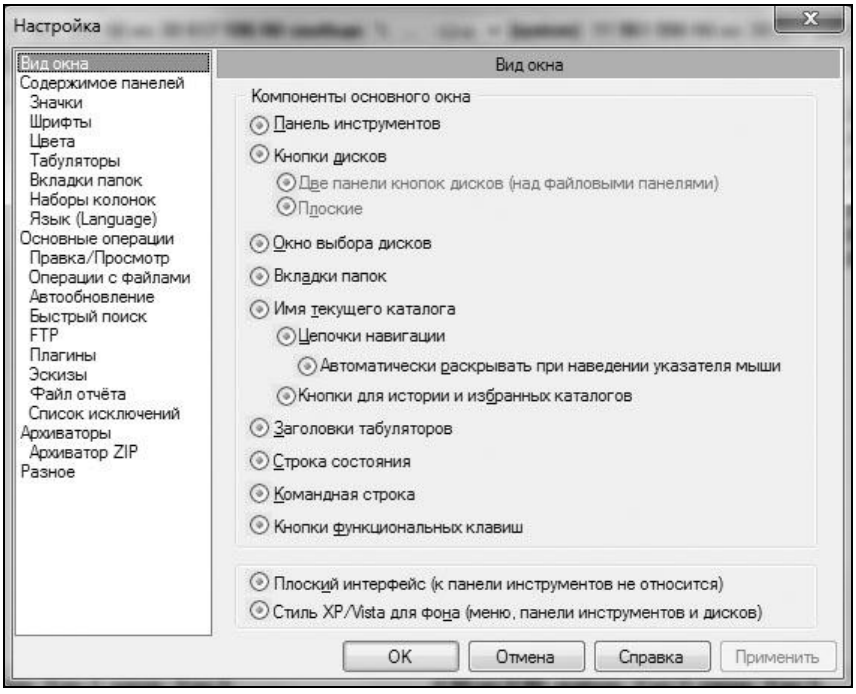


Рис. 3.4. Все элементы **CheckBox** превратились в **RadioButton**

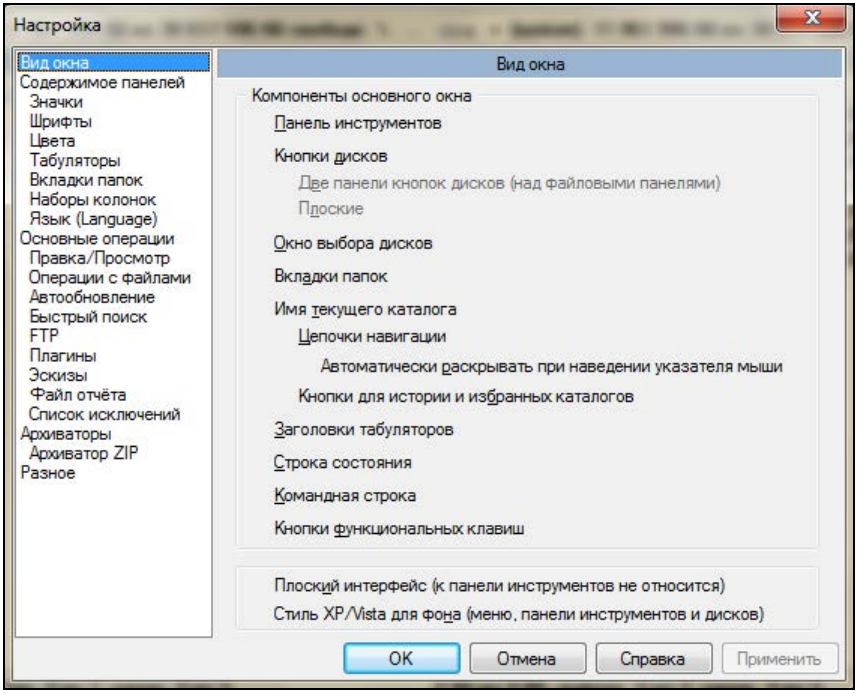


Рис. 3.5. Исчезнувшие элементы управления

Диалоговые окна

Если вы нашли в ресурсах какое-то окно, то можно перетасовать все элементы и поменять местами надписи для кнопок **OK** и **Отмена** (Cancel). Пользователь станет до посинения давить кнопку **OK**, а ничего происходить не будет.

Если попалось модальное окно (которое блокирует работу программы, пока его не закроют), то я бы убрал заголовок, чтобы не было видно кнопок **Свернуть** (Minimize), **Развернуть** (Maximize) и **Закрыть** (Close), а также сделал невидимыми кнопки **OK** и **Отмена** (Cancel). В этом случае программа будет ожидать от пользователя подтверждения или отмены действия, а кнопок нет, и ему некуда будет нажимать. Так что придется воспользоваться Диспетчером задач (Task Manager) для ее снятия.

Удалять кнопки не советую, потому что без них файл может не запуститься, а вот изменить свойство `Visible` на `false` у всего, что только можно, будет очень хорошим решением. Можете даже спрятать абсолютно все окна, тогда пользователю вообще нечего будет выбирать.

Запускайте свой Restorator или любой другой редактор ресурсов, который вам больше нравится, и начинайте править все подряд. Большинство программ, написанных на Visual C++, в своих ресурсах содержит много интересного, и все это легко поддается редактированию. Тут я больше ничего добавить не могу, потому что это процесс творческий, и в каждом случае требует своего подхода.

Только не забывайте перед редактированием сохранять копию рабочего файла, потому что некоторые изменения могут сделать программу неработоспособной, а это уже не остроумно. Если вы хотите добиться именно этого, то просто удалите файл и не истязайте больше ресурсы.

Итог

Редактирование надписей, удаление, замена или перемещение текста очень хорошо срабатывает для любого типа пользователей. Даже опытные люди порой приходят в исступление, когда видят нарушение заведенного на экране порядка, а чайник вообще может впасть в коматозное состояние примерно на час :). Ваша задача при создании шуток с ресурсами — подготовить нужные файлы на своем компьютере, а потом только подкинуть их на компьютер жертвы.

Напоследок хочется поблагодарить Билла Гейтса за предоставленную всем народам ОС, в которой так легко насмехаться над ближним. Уж где-где, а в этой операционной системе настоящему шутнику есть, где разгуляться.

3.6. Полное управление

Допустим, что вы знаете имя и пароль администратора на другом компьютере или домене сети. В этом случае шутки могут быть еще более изящными и эффективными. Для начала нужно создать в своей системе учетную запись с идентичными параметрами.

Для этого выполните следующие действия:

1. Щелкните правой кнопкой мыши по строке **Компьютер** (Computer) в главном меню и в появившемся меню выберите пункт **Управление** (Manage). Перед вами откроется окно управления компьютером (рис. 3.6). Слева расположено дерево элементов компьютера, каждому из которых соответствует служебная программа.

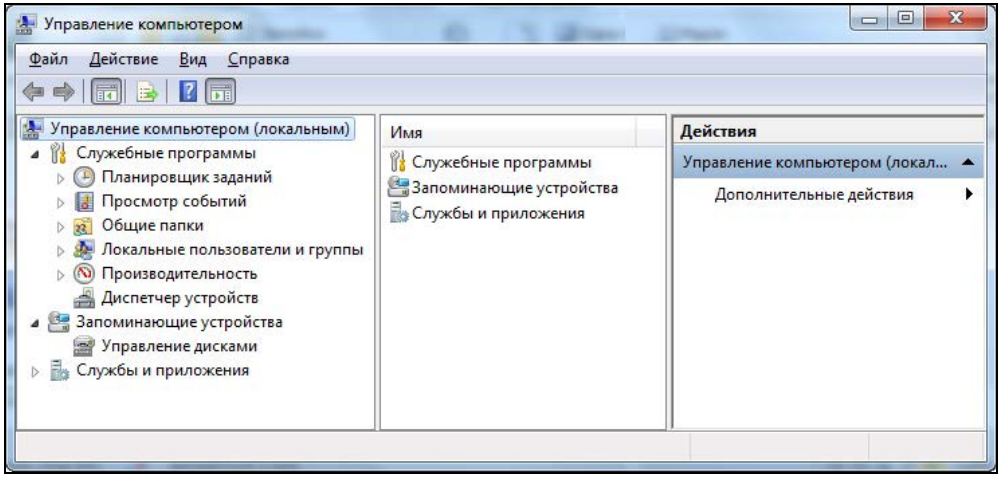


Рис. 3.6. Окно управления компьютером

2. В этом дереве откройте ветку **Управление компьютером | Служебные программы | Локальные пользователи и группы | Пользователи** (Computer Management | System Tools | Local Users and Groups | Users). В правой части окна должен появиться список всех пользователей компьютера. Для редакции Home Edition версии этот список может отсутствовать.
3. Щелкните правой кнопкой мыши по **Локальные пользователи и группы** (Local Users and Groups) и в появившемся меню выберите пункт **Новый пользователь** (New User). Перед вами появится окно, в котором нужно указать имя пользователя и пароль. Введите данные, как на компьютере, которым вы хотите управлять. Помимо этого сбросьте флажок **Потребовать смену пароля при следующем входе в систему** (User must change password at next logon).
4. Сохраните учетную запись, нажав кнопку **Создать** (Create). Перезагрузите компьютер и войдите в систему под этим именем и паролем.
5. Снова щелкните правой кнопкой мыши по строке **Компьютер** (Computer) в главном меню Windows и выберите пункт **Управление** (Manage). Той же кнопкой активизируйте самую верхнюю строку **Управление компьютером** (Computer Management) и в контекстном меню найдите пункт **Подключиться к другому компьютеру** (Connect to another computer). Вы увидите окно для ввода имени компьютера. Укажите компьютер, которым хотите управлять, и нажмите кнопку **OK**.

В принципе, окно программы управления компьютером не должно сильно измениться. В нем будут практически те же пункты, но теперь вы имеете возможность просматривать содержимое чужого компьютера и управлять им. Тут шутки уже могут быть посолиднее.

Очень красиво смотрится, когда у ничего не подозревающего пользователя вдруг выезжает лоток CD-ROM.

Для этого нужно выбрать раздел **Управление компьютером | Запоминающие устройства | Управление дисками** (Computer Management | Storage | Disk Management). Справа от структуры компьютера появится список всех доступных физических/логических дисков и съемных дисков (рис. 3.7). Щелкните по любому из дисков CD-ROM правой кнопкой мыши и выберите в появившемся меню пункт **Извлечь** (Inject). Крышка CD-ROM откроется.

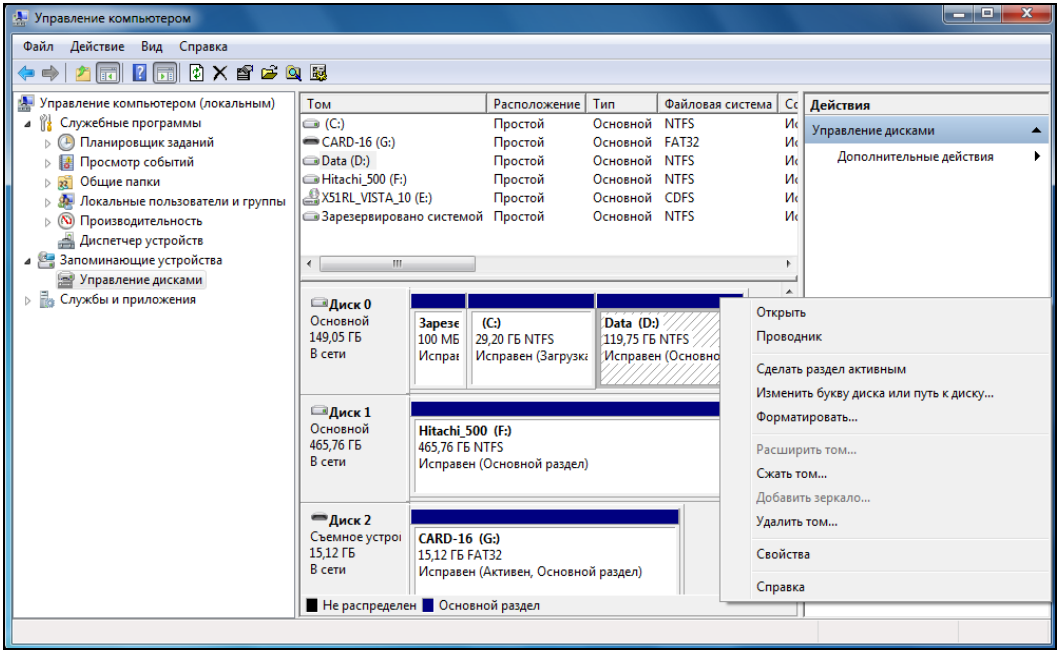


Рис. 3.7. Управление дисками

Можно еще запустить на удаленном компьютере дефрагментацию диска. Это заставит винчестер работать в усиленном режиме, оптимизируя содержимое. Компьютер будет работать медленнее, но с помощью этой операции мы можем сделать жертве доброе дело. За счет оптимизации файлов скорость работы компьютера после дефрагментации может увеличиться, и потом пользователь, над которым мы подшутили, даже скажет нам спасибо.

3.7. Программные шутки

Программно можно реализовать самые эффективные шутки. Я программирую уже давно и иногда люблю сотворить что-нибудь шуточное. Если вы хотите самостоятельно научиться создавать такие программы, то советую прочитать книгу "Программирование на C++ глазами хакера" [1] (Hackish C++ Pranks&Tricks) или "Программирование на Delphi глазами хакера" [2]. Если нет тяги к этому занятию, то можно просто воспользоваться готовыми решениями. Благо в Интернете их предостаточно.

Одной из самых известных фирм по разработке такого программного обеспечения является RJL Software (**http://www.rjlsoftware.com/**). На ее сайте вы найдете множество веселых утилит, с помощью которых можно заставить улыбнуться кого угодно. Они расположены на странице **http://www.rjlpranks.com/pranks/**. Любую из этих маленьких программ нужно скачать и просто запустить файл. Обращаю ваше внимание, что программы невидимы, и просто так их закрыть нельзя. Чтобы закончить их работу, нужно нажать комбинацию клавиш <Ctrl>+<Alt>+<Del>. Если вы работаете в Windows после 2000-го года, то перед вами появится окно безопасности Windows с кнопками для выбора нужного действия. Нажмите кнопку **Диспетчер задач** (Task Manager), чтобы запустить Диспетчер задач Windows (Windows Task Manager). В этом окне перейдите на вкладку **Процессы** (Process) и найдите в списке имя файла запущенной программы. Выделите его и нажмите кнопку **Завершить процесс** (End Process).

Есть и более простой способ завершения работы шуток от RJL Software. Отведите курсор в левый верхний угол экрана, и вы увидите сообщение, после которого программа сама закроется.

Вот, как мне кажется, наиболее интересные шутки от RJL Software:

- Avoid — запустив ее, вы больше никогда не щелкнете мышью по кнопке **Start** (Пуск). При каждой попытке навести курсор кнопка будет убегать вдоль панели задач;
- ClickStart — каждые 45 секунд имитируется нажатие кнопки **Start** (Пуск);
- Cursor Fun — эта программа заставит курсор беспорядочно двигаться по экрану, пугая пользователя и сбивая с толку;
- Clippy — через определенное время на экране будет выскакивать скрепка в стиле помощника MS Office и давать глупые советы;
- Fake format — программа создает видимость форматирования какого-либо диска. Появляется вполне реалистичное окно форматирования, и любой пользователь может не на шутку испугаться потери данных;
- Fake delete — утилита имитирует удаление какой-либо папки. Если вы уже испытали на ком-нибудь Fake format, то попробуйте еще и Fake delete. Это будет как контрольный выстрел, чтобы окончательно добить бедного пользователя (предварительно поинтересуйтесь состоянием сердечно-сосудистой системы коллеги);

- Fake Start Menu 95 — программа заменяет стандартную панель задач Windows, но при этом не реагирует ни на какие события (действия пользователя);
- HeadAche — экран начинает мигать черно-белым цветом. Для того чтобы остановить это, нажмите комбинацию клавиш <Alt>+<F4>;
- Rotate — программа переворачивает рабочий стол вверх ногами. Конечно же, реального изменения нет, потому что делается копия рабочего стола, а разворачивается рисунок и отображается на весь экран. Чтобы завершить работу, нажмите комбинацию клавиш <Alt>+<F4>;
- Show — Hide Desktop — программа прячет и отображает иконки на рабочем столе;
- Time Traveler — каждые 30 секунд время на вашем компьютере будет изменяться на случайное значение.

Но классикой жанра я считаю программу Floppy Madness, которая была популярна в 90-е годы, когда широко были распространены съемные гибкие диски — дискеты. Сейчас информацией обмениваются с помощью флешек, а для них ничего оригинального я не встречал. На первый взгляд, примитивная затея, потому что программа постоянно опрашивает дисковод, пока пользователь не вставит дискету. Когда это произойдет, появляется сообщение об ошибке с надписью вроде "Чтение с дискеты невозможно". Вроде просто, но есть возможность изменить текст сообщения, если запустить программу с параметром `setup` (набрав в командной строке в каталоге, где расположена программа, `FLOPPY.EXE setup`). Можно указать один из следующих вариантов:

- "Ну, наконец-то. Я-то думал, что ты уже забыл про меня";
- "Спасибо за бутерброд";
- "Опочки, сейчас отформатирую!!!";
- "Дискета пуста, или мне кажется?";
- "Читай сам эту дискету, я уже устал".

Одно из преимуществ утилит от RJL Software — их маленький размер, что позволяет легко подбросить файл своему другу. Можно отправить программу по почте, а можно подбросить на рабочий стол, чтобы пользователь сам ее запустил.

Но не только RJL Software умеет шутить. Есть еще Dewa Soft и ее программа Key Panic. Вы должны указать программе какое-нибудь слово, и она сгенерирует исполняемый файл размером около 70 Кбайт. После его запуска клавиатура окажется фактически блокированной (в том смысле, что на экране будет только слово, введенное вами). Например, если указать слово "бублик", то что бы ни набирала жертва, в результате будут только бублики. Программу можно скачать с сайта **http://dewasoft.com/Software/KeyPanic/KeyPanic.html**. У нее есть недостатки — она платная (12 долларов) и разработана под старые версии ОС Windows (95/98/ME/2000/XP). И если не заплатить, то пользователя будут предупреждать о том, что в системе находится программа-шутка. Если все оплачено, то невидимость гарантируется.

К моменту выхода второй версии книги данная программа стала восприниматься некоторыми антивирусами, как троян. Например, вот возмущения в базе данных Symantec:

http://symantec.uz/en/in/enterprise/security_response/writeup.jsp?docid=2001-010412-0842-99&tabid=2

На сайте разработчика написано оправдание, что он и не думал, что кто-то будет использовать его программу во зло.

В Интернете можно найти очень много разных шуточных программ, но создать что-то самому намного приятнее. И тем, кто уже умеет программировать, и тем, кто еще только пробует создавать шуточные программы, я еще раз рекомендую прочитать книги [1] или [2]. Тут вы найдете множество готовых решений и на их основе сможете создать что-то свое, даже не имея образования программиста.

3.8. Шутки читателей

После выхода первого издания книги я получал много интересных шуток от читателей по почте. Я их куда-то складывал в надежде использовать при переиздании, но сейчас что-то не могу найти. Прямо, как моя жена. Она постоянно все убирает так, чтобы не потерять, но и сама потом найти не может.

Вот одна из шуток, которую я все же отыскал в одном из текстовых файлов на жестком диске:[1]

"Здравствуйте!!! Вот прочитал вашу книгу: “Компьютер глазами хакера”, для себя открыл много интересного, в частности понравилась статья "шутки над друзьями". Вот как я люблю пошутить: создаю текстовый файл, в нем прописываю следующее: `shutdown -r`, сохраняю, потом меняю расширение с txt на bat. Сей файл нужно кинуть другу на винт, а ярлык от файла в автозагрузку. После включения компа появится надпись о завершении работы виндовз, и через 30 сек комп перезагрузится, потом опять то же самое. Вместо перезагрузки можно сделать немного по-другому: прописать `shutdown -l` — завершение сеанса, `shutdown -s` — выключение, результат на лицо — друг мой всячески проклинает виндовз и микрософт".

3.9. Мораль

Нет предела совершенству, главное — иметь хорошее воображение. Если вы тоже любите подшутить над ближним, то пишите мне. У меня почтовые ящики регулярно меняются, поэтому лучше писать мне через обратную связь на сайте **www.flenov.info**, тогда письмо точно дойдет до меня.

Я собираю хорошие компьютерные шутки и обязательно испытаю ваш прикол на своем заместителе начальника и передам вам от него привет :).

---

[1] Стиль автора письма сохранен, грамматические ошибки исправлены.

Только помните, что хорошая шутка должна быть безвредной. Можно временно выводить из строя, вешать ОС, но ничего уничтожать и ломать нельзя. Это уже неэтично, и легче просто стукнуть по монитору молотком. Прежде чем начать подшучивать, обязательно убедитесь, что ваш избранник имеет чувство юмора и правильно поймет вас. Некоторые люди могут слишком эмоционально воспринять ваши попытки развеселить себя, их и окружающих.

Не забывайте присылать мне свои идеи. Если вы придумали что-то оригинальное, то народ должен с этим познакомиться.

Подшути над ближним своим, ибо он пошутит над тобой и возрадуется :).

ГЛАВА 4

Советы хакера

В данной главе мы рассмотрим некоторые секреты при работе за компьютером. Это позволит вам правильно использовать свой компьютер и повысить его производительность. Будем рассматривать не только работу с ним и ОС Windows, но и с Интернетом.

Когда я еще не был женат, то постоянно находился в режиме online и выходил из этого состояния только для того, чтобы покушать или поспать. Сейчас у меня уже двое детей, и отрываться от компьютера приходится немного чаще, но все равно я провожу в Сети очень много времени. Поэтому для меня весьма важным является использование компьютера и Сети с максимальной отдачей. За многие годы работы набралось уже немало приемов и методов повышения эффективности, и сейчас я собираюсь поделиться с вами этим опытом.

В данной главе мы узнаем, как оптимизировать или форсировать работу компьютера. Для этого будут описаны различные методы разгона процессора.

4.1. Как не заразиться вирусами

Это самая больная тема для пользователей Интернета. Многие считают, что, установив хороший антивирусный пакет, они обезопасили свой компьютер от вторжения зловредных программ. Это верно, но такая защита эффективна не более, чем на 10%. Почему? Все очень просто! Когда появляется новый вирус, то большинство антивирусных программ даже при использовании эвристического анализа далеко не всегда могут его определить.

Новые вирусы распространяются с максимальной скоростью и инфицируют все, что попадается на их пути. Вероятность подхватить заразу при неумелых действиях возрастает до 90%. По прошествии какого-то времени пользователи Интернета обновляют свои антивирусные базы и лечат компьютеры. После этого заразиться намного сложнее, потому что зловредный код уже изолирован и его действия и эффект уменьшаются.

Итак, антивирусы предназначены для лечения, а нам необходимо средство для предотвращения заражения компьютера. Хотя современные анализаторы антивирусов и обладают невероятным интеллектом, который позволяет выявлять даже неизвестные вирусы, они все равно не без недостатков. Вирус может оказаться злым и успеет уничтожить информацию, например, отформатирует диск или просто все сотрет. Такой компьютер лечить уже будет поздно.

Первая стадия, когда появляется злой вирус, и на него еще нет противоядия, является наиболее опасной, и тут все могут оказаться под угрозой, как обладатели защитных средств, так и те, кто ими не пользуется.

За все время моей работы с компьютером на моем компьютере вирусы никогда еще не запускались. Они попадают на мой компьютер через почту или веб, но сразу изолируются, в большинстве случаев без участия антивирусных программ. У меня уже около 20 лет опыта работы за компьютером, и за первые 15 лет антивирус был только один год (я только однажды покупал годовую лицензию). Но даже в то время антивирус регулярно обновлялся, но не находился в запущенном состоянии, дабы экономить ресурсы компьютера и не отнимать лишнюю память. Каждодневные проверки только уменьшают вероятность заражения, но никак не исключают ее.

Последние несколько лет у меня стоит бесплатный антивирус от Microsoft — Microsoft Security Essentials, потому что он "кушает" не так уж и много ресурсов, бесплатен и не надоедает рекламой. И только в последний год он стал о себе иногда напоминать, когда я стал посещать по работе множество сайтов, которые не желательно посещать, и раньше я подобные не посещал. Просто по работе нужно искать много картинок, и Google иногда в своей поисковой выдаче показывает далеко небезопасные сайты, а об этом узнаешь, уже когда щелкаешь по картинке.

На сайте одного из крупнейших производителей антивирусных продуктов — Лаборатории Касперского (**http://www.kaspersky.com/**, **http://www.kaspersky.ru/**) — раньше можно было увидеть текущую активность вирусов. Низкой активности присваивается зеленый код. Его можно было наблюдать, когда по Сети прогуливаются старые вирусы, от которых давно есть вакцина, или новые, но абсолютно неоригинальные по своей природе.

Сегодня заглянул на сайт, и этого индикатора не нашел. Зато я нашел этот индикатор в правом нижнем углу на сайте другого производителя популярного антивируса — McAfee (рис. 4.1).

Во время появления новоиспеченного и оригинального вируса, который начинает заражать системы, код активности повышается, но нам от этого не легче. Увидев такое предупреждение, остается только выключить компьютер, чтобы не заразиться, и ожидать, пока производитель вашего антивирусного продукта не подготовит вакцину, которую можно будет скачать из Интернета, и спокойно жить дальше.

Прежде чем защищаться, давайте немного познакомимся с нашим врагом, узнаем, как он устроен и какие методы использует. Только так можно будет найти эффективное решение проблемы.

Большая часть повествования поможет вам предохраниться не только от вирусов, но и от троянов, и даже, в какой-то степени, от спама. Вы должны уметь не только

защищаться от вторжения, но и научиться изолировать вирусы или обезвредить троянскую утилиту. Если вы являетесь администратором сети и получили зловредный код, самостоятельно написанный каким-либо хакером специально с расчетом на вас, чтобы выкрасть определенную информацию, то антивирус такую утилиту может и не обнаружить и не сможет обезвредить. Тут уже безопасность зависит от ваших умений и навыков выявления и борьбы с хакерскими приемами.

Рис. 4.1. Сайт McAfee

Меня часто спрашивают: "А какой антивирус лучше всех?" Лучший — это тот, который сидит перед монитором, а не тот, который запущен на компьютере. У каждого антивируса есть свои сильные и слабые стороны, но заразится ли ваш компьютер вирусом, больше зависит от вас.

Но помимо антивируса, важную роль в безопасности играет и сама ОС. Такие ОС как Windows 95/98 и ME были совершенно незащищенными, и пользователи работали от имени администраторов в системе. Естественно, любые программы запускались в их системах от тех же прав и могли делать с системой все, что угодно.

С появлением Windows XP компания Microsoft пыталась уговорить всех заводить учетные записи простых пользователей, работать под ними и переключаться в режим администратора только по мере необходимости установить новую программу

или изменить что-то в системе. Это правильная политика, которую большинство проигнорировало. А все потому, что большинство программ под Windows XP были написаны так, что они использовали систему, сохраняли информацию в такие папки как Program Files или Windows\System32, хотя это совершенно не нужно было. Эти папки содержат системные файлы и должны быть защищены от изменения.

В Windows Vista компания Microsoft пошла на опрометчивый шаг — заставила всех работать от имени простого непривилегированного пользователя, а User Account Control (UAC, контроль учетных записей пользователя) контролировал доступ к запретным областям и требовал подтверждения пользователя в случае, если программа пытается получить доступ к важной для стабильной работы системы области. Это вызвало недовольство пользователей, потому что все плохо написанные программы переставали работать или надоедали подтверждениями.

Лично я перешел на Windows Vista с большим удовольствием и отказался от всех программ, которые не стали работать на этой системе. Раз не работают, значит, они не безопасные, а я не хочу подвергать свой компьютер риску. В Windows 7 управление учетной записью было улучшено, и система стала работать быстрее и интеллектуальнее, но вероятность заражения вирусами в Windows все же остается, потому что это самая популярная ОС и наиболее интересна для хакеров.

Если так боитесь вирусов, то следует перейти на компьютеры с MAC OS X или Linux. Эти системы пока не сильно популярны и не интересны хакерам, поэтому вирусов для них очень и очень мало. Лично я недавно приобрел себе Apple Air и в нем экономлю на антивирусах.

4.1.1. Как работают вирусы

Когда мы рассматривали структуру программы, то говорили о заголовке исполняемого файла *(см. разд. 2.1)*. В этом заголовке есть точка входа — адрес внутри программы, с которого начинается выполнение. Если вирус должен присоединиться к программе, то он дописывается в ее конец и изменяет точку входа на себя, а программа со старого адреса вызывается после выполнения тела вируса. Таким образом, после старта запускаемого файла сначала активизируется вирус, а потом управление передается основной программе.

Особо ленивые писатели вирусов не любят разбираться с заголовками. Они, наоборот, добавляют запускаемый файл другой программы к своему, т. е. тело вируса оказывается в начале файла.

Так работает большинство вирусов, которые прикрепляются к программам, и таких до 2000 г. было очень много, особенно в операционной системе MS-DOS. Если вы хотите защититься от вредоносного кода, то минимальным требованием должно быть слежение за заголовками исполняемых файлов. Как только заголовок изменился, нужно бить тревогу, потому что это может быть вирус или червь. Конечно же, вручную это делать тяжело, но необходимо следить хотя бы за размером основных программ, ведь когда к исполняемому файлу прикрепляется вирус, изменяется его размер.

Но существует вариант, когда тело вируса добавляется к запускаемому файлу, а заголовок не изменяется, т. к. в этом случае тело вируса вызывается из другой программы. Получается эффект, как в динамической библиотеке — программа загружает в память дополнительный файл, выполняя в нем тело вируса.

Как я уже говорил, такие вирусы властвовали до 2000 г. Тогда Интернет был развит еще не так сильно, как сейчас, и основным средством распространения инфекции были дискеты или файлы, скачанные с BBS (Bulletin Board System, электронная доска объявлений), с помощью которых люди обменивались информацией. Некоторые вирусы записывались не в программу, а в загрузочную область дисков, и выполнялись при первом же обращении. В этом случае после запуска файла с дискеты вирус загружался в память и распространялся по файловой системе, заражая все, что попадалось на пути.

Зачем производился поиск и заражение всех исполняемых файлов? Все очень просто. В MS-DOS была только одна возможность загрузить программу автоматически при старте компьютера — autoexec.bat. В этом файле прописываются программы, которые должны запускаться при загрузке ОС. Если бы все вирусы записывались в этот файл, то антивирусам легко было бы обезвредить внедренный код. Именно поэтому заражались все файлы. После этого при загрузке любой зараженной программы запускался и вирус.

Есть вирусы, которые просто копируют себя в систему и помещаются в раздел автозапуска. С распространением Windows именно такие вирусы стали наиболее популярны, потому что здесь уже больше способов их спрятать. В данном случае уже нет смысла сканировать весь диск в поисках исполняемых файлов и заражения их, достаточно записаться в автозагрузку, и дело в шляпе. При каждом старте системы ОС сама запустит вредоносный код. Но теперь такие вирусы не столь признаны, потому что с ними уже научились бороться.

В Windows, помимо большого количества способов автоматической загрузки, появилось очень много файлов, которые обязательно загружаются при старте ОС, например системные динамически подключаемые библиотеки (DLL, Dynamic-Link Library). Это тоже упрощает жизнь вирусам. Если раньше нужно было заражать все, потому что заранее неизвестно, с какими программами работает пользователь, то теперь достаточно инфицировать одну из библиотек или важный исполняемый файл, и нет необходимости в сканировании.

Плюс ко всему, появилось множество мест, откуда программа может запуститься при старте системы, а значит, вирусу проще спрятаться.

Выходит, если раньше проблема пряталась только в exe- и com-файлах, то теперь источник зла нужно искать и в динамических библиотеках, у которых есть большой недостаток — возможность выполнять код при старте DLL. И если вирус записать в автозапуск важной библиотеки, то он сможет загружаться автоматически. Таким образом, количество потенциальных лазеек в системе резко увеличилось.

Ну а если код вируса загрузится раньше кода антивируса, то злостный код может блокировать работу антивируса, и ему проще будет скрыться в системе. Уже были

подобные случаи, когда вирусы побеждали за счет блокировки защитных средств. Но были и смешные случаи, когда один злой код при заражении компьютера искал своего конкурента (другой злой код) и уничтожал его.

Но динамические библиотеки — не единственное зло. Корпорация Microsoft для упрощения жизни пользователей во многие свои продукты включила элементы языка программирования Visual Basic. Такая поддержка есть почти во всех компонентах пакета MS Office. Это очень удобно, когда с помощью несложного языка можно упростить свою жизнь и расширить возможности используемой программы. Но хакеры увидели в этом очередную лазейку.

Большинство пользователей Интернета привыкло, что опасность от вирусов кроется в исполняемых файлах, и никто не мог себе представить, что угроза придет из текстовых документов или электронных таблиц MS Office. Именно поэтому первые вирусы, встроенные в документы Microsoft Word или исполняемые в почтовой программе Microsoft Outlook, заразили громадное количество компьютеров за минимальное время. К таким обстоятельствам не были готовы ни пользователи, ни лучшие антивирусные продукты.

Жертвой может оказаться любая программа, которая содержит какой-то скриптовый язык и выполняет какой-то код, и это не обязательно должен быть байт-код классического исполняемого файла. Так, например, в свое время очень опасными были слишком большие возможности JavaScript. Это такой сценарный язык, который встроили в браузеры для придания страницам интерактивности. Интерактивность — это хорошо, но безопасность лучше. Если в сценарном языке есть команда, которая позволяет получить доступ к компьютеру, и хакер будет использовать эту команду для своих злых целей, то браузер может оказаться потенциальной угрозой.

Лично я никогда не приветствовал вирусописательство и считал это самым глупым занятием. Это ребячество, присущее только маленьким детям, которые при покупке новой игрушки стараются ее поломать, а не использовать по назначению. Именно так ведут себя хакеры, которые не работают (или играют) за компьютером, а пытаются поломать его.

Лично я сам в 1998 г. как-то написал один вирус, который просто плодился по файловой системе в MS-DOS, но не делал ничего другого. Этот вирус я испытал в своем компьютере и никогда не выпускал в свет. Я даже удалил исполняемый файл и долго хранил только исходный код. Возможно, он даже где-то сохранится на компакт-дисках в архивах.

В настоящий момент вирусы распространяются через Интернет и практически не используют в качестве носителя файлы или дискеты (есть ли еще они у кого-нибудь?). Основным переносчиком стала электронная почта, веб-страницы и массовые рассылки. Вы получаете письмо, к которому прикреплены вирус и заманчивый текст, убеждающий открыть программу-вложение. Если такой файл запустить, то вирус заражает компьютер и рассылает себя по всем адресам, внесенным в вашу адресную книгу.

4.1.2. Эвристический анализ

Эвристический анализатор может спасти от самых примитивных вирусов, которые не способны вызвать эпидемию. И это вполне логично, раз антивирусы умеют распознавать новый вирус, то он не сможет распространяться. Но профессиональный вирусописатель сможет обойти автоматический анализ.

Антивирус — это программа. А как программа может узнать, что перед нами злой код, а точнее вирус? Все очень просто, это можно определить по функциям и последовательности действий, которые выполняет программа. Например, если программа читает из Сети данные и тут же пытается выполнить в локальной системе команду, передав ей в качестве параметра полученные из Сети данные, то велика вероятность, что перед нами троянская программа.

Но такие же действия может выполнять и вполне честная и добрая программка, а значит, анализатор может привести к проблеме. Именно так и произошло один раз со мной: антивирус Касперского и McAfee по ошибке одну из моих программ воспринимали как вирус (точнее, это был инсталлятор к моей программе).

Давайте рассмотрим, почему антивирусы ошиблись в отношении моей программы. Инсталлятор был выполнен в виде единственного файла, который являлся на самом деле простым самораспаковывающимся архивом. Такие архивы состоят из двух частей:

- исполняемая часть, в которой находится код распаковки архива;
- область данных, где находятся заархивированные данные, которые нужно будет разархивировать.

Антивирусные программы, видимо, решили, что нельзя разархивировать и тут же запускать распакованный файл. Что тут такого страшного, когда все инсталляторы делают так же, я не знаю, но то, что автомат может ошибаться, для меня очевидно на собственном кошельке. Да, именно на кошельке, потому что из-за ошибок в антивирусах некоторые пользователи не установили себе эту программу и с недоверием стали относиться к другим моим программам. Сейчас уже доверие возвращается, но слишком много было потрачено на это ресурсов.

С другой стороны, мы уже сказали, что обмануть автоматический анализатор очень просто, и об этом можно почитать в Интернете. Если вы программист и заинтересовались данной темой, то советую заглянуть на сайт **http://www.wasm.ru/**, где можно найти информацию на русском языке по обману. На этом сайте присутствует множество профессионалов, которые регулярно выкладывают интересные исследования. Можно так же поглядывать на сайт журнала "Хакер" и не помешало бы его читать. На словах могу сказать, что очень часто обмануть можно простой заменой последовательности выполняемых действий или заменой функций (очень часто одно и то же действие можно выполнить несколькими методами).

4.1.3. Как же предохраняться?

С вирусами никогда не знаешь, откуда придет очередная угроза, но защититься от вирусов не так уж и сложно и в наше время достаточно даже держать бесплатного

антивируса от Microsoft. Я не знаю, насколько он хорош и лучше платных аналогов, но его может быть вполне достаточно.

Во времена MS-DOS я сканировал жесткий диск только раз в год (и то для очистки совести: вирусы ни разу не обнаружились). Как мы уже знаем, в ту пору основным источником заражения были BBS и дискеты. Первое я не использовал, и с этой стороны угрозы для моего компьютера не было. А все дискеты, прежде чем открыть в файловом менеджере, я обязательно проверял антивирусной программой, даже если дискету дал хороший знакомый. Друзья могут не знать о существовании на их компьютере вирусов и, не желая того, принести вам зараженный файл. Подтверждения этому я встречал очень часто, когда находил вирусы в загрузочных секторах дискет ничего не подозревающих друзей.

В настоящее время я не пользуюсь дискетами и не обмениваюсь исполняемыми файлами с друзьями таким образом. Сейчас все пересылается через Интернет. Все и всегда надо брать из первоисточников, т. е. с официальных сайтов в Интернете. Именно официальные источники могут на 99% гарантировать отсутствие вирусов. Конечно же, были случаи, когда хорошо зарекомендовавшие себя фирмы по неосторожности распространяли вместе со своими продуктами вирусы, но это бывает крайне редко, и такие ошибки интернет-сообществом определяются очень быстро и исправляются моментально.

Ну а с друзьями мы обмениваемся документами и фотографиями, которые не умеют выполнять никаких сценариев или кода, поэтому не принесут никакого вреда.

Используйте нераспространенные программы

Как я уже говорил, сейчас основным источником вирусов стал Интернет, а точнее электронная почта. В качестве почтовой программы я раньше использовал The Bat! (**http://www.ritlabs.com/**), которая не поддерживает сценариев и не имеет встроенного языка VB (язык Visual Basic может позволить автозапуск прикрепленного к письму файла) или VBScript. Хотя в большинстве почтовых клиентов уже есть защита от автозапуска через сценарии VB, но иногда в них отыскивают уязвимые места, и вирусы получают черный ход для проникновения в систему. Конечно же, и в The Bat! есть ошибки, которые иногда находят, но эта программа не очень широко известна, поэтому вирусы практически не используют ее слабые места.

Программа The Bat! не бесплатна, поэтому я отказался от нее, не хочу использовать крэки (потому что сам программист), а платить — нет денег. Но на данном рынке полно других программ для работы с электронной почтой, и вы легко сможете найти для себя что-то подходящее. Дабы не делать никому рекламы (а мне за нее не платят), я не буду рекомендовать ничего конкретного.

Я всем рекомендую использовать что-нибудь не очень распространенное, потому что вирусописатели делают ставку на самое популярное. То, что для ОС Linux или Mac OS X не пишут вирусов, еще не говорит о невозможности их создания. Просто эти ОС мало распространены, и масштабы заражения будут небольшими. Любой крэкер или вирусописатель ищет известности и как хакер хочет получить уважение большинства, поэтому и использует ОС Windows, как самую востребованную среди домашних пользователей.

Если поставить под угрозу 1% пользователей всех компьютеров, то об этом могут написать в Интернете и даже в каком-то offline-издании. Но стоит поставить под угрозу более 90% всех пользователей, т. е. всех пользователей Windows, то об этом будут трубить в Интернете, во всех СМИ, в том числе и по телевидению.

Но даже если вы работаете с самой незаметной программой, все равно нельзя быть уверенным в своей безопасности. В разных программах встречаются одинаковые ошибки, и тогда ваш компьютер тоже будет подвержен атакам. Допустим, что вы используете для доступа к веб-сайтам самый простой браузер, который ничего не поддерживает, кроме отображения текста, и не может быть атакован. Но для получения данных от сервера используется протокол HTTP, а тот в свою очередь работает поверх TCP/IP. Если в одном из этих протоколов будет найдена ошибка, используя которую злоумышленник получит доступ к локальному диску вашего компьютера, то тут уже никого не будет волновать, какая у вас программа или ОС. В этом случае можно будет без особых проблем произвести взлом.

Конечно, фраза "ошибка в HTTP или TCP/IP" звучит нелепо, потому что эти протоколы мало несут угрозы. Более удачным примером может быть шифрование. Если в каком-то алгоритме шифрования будет изъян, то под угрозой окажутся все.

Непопулярные программы — это благо, которое с другой стороны может обернуться источником больших проблем. Предположим, что ваш продукт разработчик перестал поддерживать, и найдена критическая ошибка. Обновить программу будет невозможно, а переход на другую отнимет много времени и средств. Чтобы не столкнуться с такой ситуацией, лучше выбирать программные средства, в будущем которых можно не сомневаться. Такими бывают продукты фирм, которые считаются вторыми или третьими по популярности, но никак не последними. Первыми умирают самые незаметные и неизвестные. Единственное, что может спасти ситуацию, — если разработчик откроет исходные коды или проект изначально был с открытым кодом, и его начнут поддерживать другие программисты.

Но как показывает практика, даже наличие исходного кода не всегда спасает проект и его далеко не всегда подхватывает сообщество программистов. Программисты, которые работают над проектами с открытым кодом, очень часто, как и хакеры, хотят признания. Если сказать, что я работаю над ОС Linux, то мне будет легче добиться признания, чем если сказать, что я работаю над очередным почтовым клиентом, коих сейчас на рынке уже очень много. Так что если уж создатель не захотел поддерживать свой исходный код, не факт, что кто-то еще захочет.

Все как-то выглядит страшно? Работать с популярными программами тоже можно, и я использую их без проблем. Они интересны хакерам, но чтобы спать спокойно, достаточно хотя бы вовремя обновлять программы. Популярные проекты, особенно платные, очень хорошо поддерживаются разработчиками, и ошибки вовремя латаются, чтобы не допустить эпидемий.

Регулярно обновляйте программы

Если вам необходимы возможности распространенных программ, то регулярно проверяйте наличие обновлений. В этом отношении лучше всех работает Microsoft.

Как бы ни ругали эту компанию, она очень большое внимание уделяет поддержке пользователей и регулярно предоставляет обновления, позволяющие исправить погрешности в своих разработках. Ошибки есть везде, но ищут в основном в самом популярном. Корпорация Microsoft делает все возможное для уменьшения негативного эффекта от собственных ляпсусов.

Своевременное обновление ОС и основных программ тоже позволяет обезопаситься от вторжения вирусов. Всевозможные аналитические компании всегда показывают разные данные, но все они сводятся к тому, что большинство пользователей Интернета не обновляет свои продукты: одни из-за лени, другие из-за слабого канала связи, а некоторые из-за использования нелицензионного программного обеспечения. Вирусописатели пользуются этим. При нахождении новой уязвимости, позволяющей проникнуть в систему, очень часто появляются вирусы, использующие этот изъян. Если вы узнали, что появилась какая-то брешь, то обязательно обновите систему.

Я рекомендую пользоваться лицензионным программным обеспечениям для возможности получать полноценную поддержку и обновления. В своем блоге **www.flenov.info** я часто общаюсь с читателями, и мы не раз обсуждали легальность программного обеспечения. Очень часто мне говорили о том, что если платить за весь необходимый софт, то компьютер обойдется слишком дорого, и только программное обеспечение может обойтись в тысячу или даже тысячи долларов. Но ведь если посмотреть реальности в глаза, то на большинстве компьютеров нужно не более 200 долларов на программное обеспечение. Нужна сама ОС, которая в OEM-варианте стоит около 50 долларов, и нужен офис, который стоит примерно столько же (я имею ввиду Microsoft Office Home and Students, которого для дома более, чем достаточно).

Возможно, вам понадобятся еще программы, но просто нужно ставить то, что реально нужно. Для редактирования фотографий очень часто достаточно Paint.NET и если и нужен Photoshop, то в домашних условиях большинству будет достаточно и Photoshop Elements. Лично я использую лицензионную версию Elements, которая, начиная с 9-й версии, стала вполне подходящей для большинства домашних задач.

Обновлений для программ очень много, и сложно разобраться, какие из них устанавливать. Корпорация Microsoft должна своевременно доводить до сведения всех пользователей о найденных ошибках, а о наиболее критичных нужно сообщать во всеуслышание. В большинстве случаев компания старается промолчать, чтобы лишний раз не говорить о своих оплошностях, но это не правильно. Хакеры следят за такими лазейками и знают о них больше, чем рядовые пользователи.

В последней версии Windows обновление вышло на достаточно высокий уровень, но еще не идеально. Буквально неделю назад жена сообщила мне, что на детском компьютере обновление постоянно сообщает о том, что оно не может установиться. Так как сообщение показывалось желтым цветом, то жена не особо обращала внимание и сказала мне только потому, что стала играть в игру на детском компьютере, и ей надоело видеть это сообщение.

Когда я посмотрел, что компьютер не может установить, оказалось, что это был Windows 7 SP1, который вышел, кажется, в феврале. Получается, что компьютер

находился без обновлений пять месяцев и всего лишь выдавал предупреждение. Каждый день компьютер пытался установить обновление, но не мог. Мне кажется, уже пора было выбрасывать красный флаг.

Доверяй, но проверяй

При работе с электронной почтой никогда не доверяйте получаемым сообщениям и никогда не запускайте прикрепленные файлы!!! Даже если вы получили письмо, в поле отправителя которого указан адрес вашего друга, вложение не может считаться надежным. Если компьютер отправителя заражен, то вирус будет от его имени рассылать всем копии писем, и вы можете попасть на эту удочку.

Писатели вирусов используют психологию и социальную инженерию и большое внимание уделяют тексту рассылаемого письма. Я очень часто получаю письма от своих знакомых, партнеров и даже друзей с текстом "Посмотри этот файл", но это точно вирусы.

Если я не ожидаю файла от друга, то я его не открою. Особенно если там исполняемый файл.

Вложения

Если вы получили по почте исполняемый файл с предложением открыть его, то прежде чем это делать, не поленитесь обратиться к отправителю с просьбой удостоверить посылку. Вирусы могут только рассылать письма, а следить за запросами подтверждения не могут.

Как определить, какие файлы во вложении могут содержать вирусы, а какие нет? Вирусов точно не может быть в текстовых файлах TXT, в картинках JPG, GIF, BMP, в аудио- и видеофайлах WAV, MP3, AVI и некоторых других. Но нельзя быть совершенно уверенным, что в будущем эти форматы не смогут быть заражены. В определенных ситуациях и при использовании отдельных программ вирусы смогут распространяться через что угодно. Пока хакеров сдерживает слишком большое количество условий. После кражи исходных кодов Windows появился вирус Agent, который заражал компьютер при безобидном просмотре специально сконструированных BMP-файлов.

Когда смотрите вложение к письму, вы должны быть убеждены, что оно имеет правильное расширение. В Windows по умолчанию не отображаются расширения для зарегистрированных типов файлов. Это значит, что если вложение имеет расширение exe, то перед вами предстанет только его имя. Хакеры пользуются этим и дают файлам двойные расширения. Например, если файл назвать update.jpg.exe, то расширение exe система спрячет, а вы увидите только update.jpg. Создается ложное представление, что перед вами картинка, а на деле при двойном щелчке файл будет запущен, что грозит заражением компьютера.

Чтобы не было проблем с псевдорасширениями, я рекомендую отказаться от их сокрытия для зарегистрированных типов файлов. Для этого нужно перейти в Панель управления, вызвав меню **Пуск | Панель управления** (Start | Control Panel) и

запустить компонент **Свойства папки** (Folder Options) либо выполнив команду **Пуск | Панель управления | Оформление и персонализация | Свойства папки**. Здесь необходимо перейти на вкладку **Вид** (View). Перед вами откроется окно, как на рис. 4.2. Уберите флажок с пункта **Скрывать расширения для зарегистрированных типов файлов** (Hide extensions for known file types).

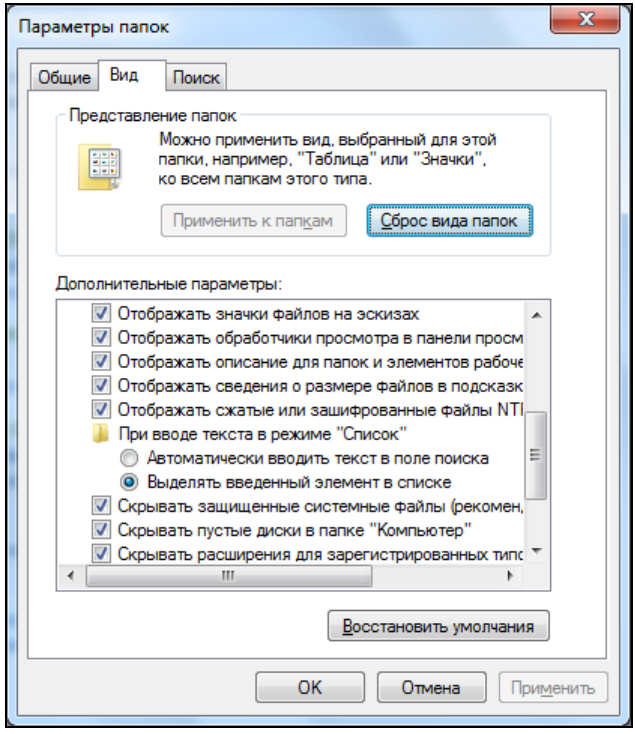


Рис. 4.2. Окно настроек свойств отображения файлов

Сомнительные сайты

Помимо электронной почты, источником инфекции можно считать и веб-сайты. Так как в интернет-браузерах (а главное, в самом распространенном из них Internet Explorer) регулярно находят ошибки, позволяющие получить доступ к диску пользователя, то этот способ заражения нельзя исключать. Я использую Интернет по назначению и путешествую только по официальным сайтам. Там не задействуют бреши в браузерах для заражения пользователей, ибо это очень сильно подорвет авторитет компании.

Большинство персональных страничек тоже не используется для нанесения вреда, но иногда среди них можно найти тестовый полигон хакера. Но если вы любите путешествовать по сайтам сомнительного характера, то тут уж вероятность получить неприятности увеличивается в несколько раз. В этом случае обновлять нужно все и регулярно, а антивирус должен быть всегда включенным. И даже при выпол-

нении всех этих условий система заполняется различным мусором с невероятной скоростью.

Недавно любопытство заставило меня щелкнуть по одной ссылке, и в корне диска C: тут же появились два файла: xxx.exe и yyy.exe. Когда пишешь подобные книги, то приходится тестировать много сомнительного софта или интернет-сайтов и заражать свой компьютер. Благо, что файлы только появились, а не запустились, и моментальное удаление избавило мой компьютер от случайной возможности заражения.

Однажды мне пришлось писать статью по интим-сайтам для одного из журналов. Для этого пришлось попутешествовать по Сети, после чего неделю вычищал диск от посторонних программ. Это были еще Windows 98 и Internet Explorer 6.0, которые позволяли все, что угодно. Многие из них, конечно же, не работали, потому что требовали ручного запуска, но само их присутствие меня не радовало.

Если вы являетесь любителем клубнички и других сладких, но вредных фруктов, то приготовьтесь к тому, что ваш компьютер будет регулярно получать порцию недоброкачественных файлов, и надо только молиться, чтобы это зло не начало работать и не нанесло вред.

Взломанные сайты

Но даже если посещать только проверенные сайты, заражение вирусом не исключается. Каждый подросток хочет создать собственный сайт, и большинство старается использовать современные и неизвестные технологии. Программирование — это не такое уж и простое занятие. Чтобы создать хороший и безопасный сайт, требуется опыт и глубокие знания, а одна ошибка может привести к печальным последствиям.

Благодаря Интернету и доступности литературы количество хакеров увеличивается. Доступность программ для автоматического поиска и использование уязвимостей в некоторых случаях позволят взломать сайт даже ребенку. Взломав сайт, хакер может внедрить в код веб-страницы ссылку для загрузки вирусов, и легким движением руки безопасный ресурс превращается в очень опасный.

Я для собственных нужд написал небольшую программу (относительно небольшую) CyD Network Utilities (можно найти на **www.cydsoft.com**), в которой реализован достаточно интеллектуальный модуль поиска уязвимостей на сайтах. Программа неплохо ищет даже SQL Injection.

Проблему усугубляют российские хостинговые компании, на серверах которых работают сайты. На одном сервере могут работать тысячи сайтов, и если есть ошибки в конфигурации, то все эти сайты могут оказаться уязвимыми. Где-то в середине 90-х все сайты на одном из серверов крупного хостера — Valuehost были заражены трояном, а точнее сказать, в главную страницу была внедрена ссылка на троян. Среди жертв оказалась и моя страница, и когда я посетил свою страницу, то вирус начал качаться мне на диск. Кто бы мог подумать, что я чуть ли не заражусь от собственного сайта. Кому еще можно так доверять, как не самому себе.

Я не хочу делать рекламу или антирекламу российскому хостингу, но после этого я решил перенести все свои сайты на хостинг в США. После этого вроде бы с подобными проблемами не сталкивался. Вроде бы российские ИТ-шники славятся своими знаниями, но когда дело доходит до реальности, взломы в Рунете происходят очень и очень часто.

Подобные случаи заражения целых серверов хостинговых компаний являются не единичными. Я слышал о нескольких компаниях, клиенты которых пострадали от взломщиков.

Если вы собираетесь писать собственный сайт и при этом не обладаете достаточным опытом или знаниями, одумайтесь. Не портите себе репутацию и не подставляйте других. Если же желание экспериментов и славы преобладает, то со всей строгостью подойдите к выбору хостинговой компании.

Мой e-mail — моя крепость

У меня всегда было 4 почтовых ящика: рабочий, для общения с друзьями, публичный и мусорный. Сейчас количество мусорных ящиков увеличилось до трех. Рабочий знают только коллеги, и он существует уже 6 лет. При этом количество вирусов и спама, попадающего в этот ящик, минимально. Адрес для общения с друзьями более распространен, и на него иногда приходят вирусы и немножечко спама. Остальные два — для широкой публики, их адреса известны многим, поэтому во времена большой вирусной активности я удаляю мегабайты зараженных писем.

Ну а сколько спама я удаляю с публичных (я их называю мусорными) ящиков и посчитать трудно. Стоит указать свой почтовый адрес во время регистрации на не очень качественном сайте, как сразу начинает сыпаться спам. Поэтому при регистрации на любых сайтах (форумы и даже социальные сети) я использую только мусорные ящики, которые не жалко.

Если количество ужаса во входящих превысит все разумные пределы, то я просто забрасываю мусорный ящик и создаю себе новый. А т. к. мне по роду деятельности постоянно приходится тестировать много сайтов и много регистрироваться, то смену приходится делать как минимум раз в два года.

За счет такого вот разграничения я знаю, что на публичных адресах нужно быть особо внимательным, и письма с вложением удаляю сразу, вне зависимости от формата. Даже если файл по своей сути не может содержать вирусов (например, текст в формате TXT), я не увижу его. По ссылкам я тоже никогда не щелкаю, потому что может быть всякое. Так что, если вы собираетесь выслать что-то, то это будет абсолютно бесполезно, ни один вложенный файл на мой компьютер не проходит.

Фальшивый URL-адрес

Так как мои адреса достаточно известны, на них регулярно приходят письма сомнительно характера. Буквально вчера получил письмо, в котором мой банк просил поменять параметры доступа к счету. Вот письмо, которое я увидел:

Письмо с просьбой смены параметров счета банка

Dear SunTrust valued member.

Due to concerns, for the safety and integrity of the Internet Banking community we have issued this warning message.

It has come to our attention that your account information needs to be updated due to inactive accounts, frauds and spoof reports. If you could please take 5-10 minutes out of your online experience and renew your records you will not run into any future problems with the online service. However, failure to update your records will result in account deletation.

Once you have updated your account records your online banking account will not be interrupted and will continue as normal.

Please follow the link below and renew your account information.
https://www2.suntrust.com//cgi_w/cfm/personal/account_access/account_access.cfm

SunTrust Internet Banking

Я услугами этого банка не пользуюсь, поэтому сразу почувствовал неладное. Внизу письма давалась ссылка на веб-страничку, и адрес вроде бы реальный и без ошибок. Но если навести мышь на строку с URL, то выскакивает подсказка с истинным адресом, который будет загружаться, если щелкнуть по ссылке. В ней почему-то адрес **https://www2.suntrust.com** изменился на IP-адрес **http://211.202.3.208**. После проверки выяснилось, что этот сервер расположен совершенно в другом месте, просто оформлен, как сайт банка.

Хакеры допустили большую ошибку, когда так просто спрятали URL. Намного эффективнее было бы зарегистрировать адрес **www2.santrust.com** (заменена одна буква, которая не бросается в глаза) или что-то в этом роде. Тогда подстава была бы незаметна, потому что разница в именах доменов только в одной букве. Когда видишь IP-адрес, то сразу понятно, что это письмо-фальшивка, а схожее по написанию доменное имя, скорее всего, не вызовет подозрений.

Взломы с использованием схожих доменных имен были очень популярны несколько лет назад. Таким образом очень часто вскрывали пароли пользователей для доступа в Интернет, когда он был достаточно дорогим и использовались dial-up-модемы. Например, пользователь получал письмо с просьбой выслать свой пароль на адрес администрации провайдера. Допустим, что реальный адрес был **support@provider.com**. Хакер регистрировал домен, например, **provader.com** (разница только в 5-й букве) и указывал в запросе e-mail **support@provader.com**. Очень многие пользователи верили таким письмам, потому что не замечали подставного адреса.

Такие атаки легко проходили, потому что до 1995 г. регистрация домена была бесплатной и бесконтрольной, а для многих это было в новинку, поэтому никто не замечал такой простой подстановки. Сейчас регистрация стала платной, да и все имена, схожие с торговыми марками, скуплены, поэтому подобрать что-то похожее стало сложно.

В настоящее время количество таких взломов уменьшилось, но это может быть только затишьем перед бурей. Пользователи стали забывать о таком простом методе, как подмена адресов, и хакеры могут воспользоваться этим спокойствием. Количество новых пользователей Интернета растет с каждым днем, многие из них и не слышали о подобных способах взлома. Введи я на указанном в письме сайте параметры своей учетной записи, то, скорее всего, увидел бы простое сообщение об ошибке, а реально мои данные попали бы в руки хакеров.

Еще пять лет назад таким способом хакеры воровали пароли доступа к Интернету, но с расширением электронной коммерции могут появиться взломы интернет-аккаунтов и другой важной информации.

Сейчас наиболее популярные письма, которые я получаю, построены в стиле: "Я сын какого-то шейха или китайского банкира, и мне нужна помощь в отмывании супер большой суммы денег с 6-ю нулями. Готов поделиться этими нулями". Не знаю, много ли народу попалось на этот развод, но, судя по тому, что такие письма рассылаются уже не первый год, значит, кого-то они ловят.

4.1.4. "И тебя вылечат, и меня..."

Даже самый защищенный компьютер с лучшим антивирусом когда-нибудь может быть заражен. Я это вижу постоянно. Чтобы своевременно избавляться от вирусов, вы должны регулярно выполнять несколько простых действий (помимо описанных в *разд. 4.1.2*), и антивирусник в автозапуске не понадобится, а если понадобится, то простой и не прожорливый к ресурсам компьютера.

Как мы уже знаем, если программа написана специально для вторжения в определенную среду, то она будет иметь уникальный код, и противовирусные системы ее могут пропустить даже мимо интеллектуальных анализаторов. В этом случае безопасность компьютера зависит от умения правильно распознать и нейтрализовать зловредную программу.

Обезвредить большинство заразы не так уж и сложно — просто завершаем работу программы и удаляем все ее файлы. Намного сложнее правильно определить исполняемый файл.

Корень системного диска

Регулярно следите за всем, что появляется у вас в корне системного диска. Вы должны знать, для чего предназначен каждый файл, и отмечать любые изменения. Для наблюдения лучше всего включить отображение скрытых файлов. Для этого нужно перейти в Панель управления и запустить компонент **Свойства папки** (Folder Options). Перед вами откроется окно, как на рис. 4.2. Здесь необходимо перейти на вкладку **Вид** (View) и поставить переключатель **Показывать скрытые файлы и папки** (Show hidden files and folders).

Никаких exe- или pif-файлов в корне диска быть не должно. Единственный com-файл, который может лежать в корне диска C:, — это ntdetect.com. Все остальные

должны иметь расширения sys, bin, ini или bat, и их нельзя запускать на выполнение.

Файл с расширением bat — это командный файл, который может запускать другие программы, поэтому наличие такого зверя тоже должно вызывать подозрение, особенно, если его название отличается от autoexec.bat. Да, в корне должен быть только один (или не одного) файл с расширением bat.

Файлы с расширением bat сами по себе не могут быть вирусами, но это командные файлы, которые могут запускать другие программы и те же вирусы. Именно поэтому за ними тоже надо следить. В корне диска может быть только файл autoexec.bat.

Чтобы вам проще было вести наблюдение, никогда не устанавливайте программы и не копируйте файлы в корень диска. Заведите для этого отдельные папки.

Автозагрузка

Вирусы появляются, где угодно, но чаще всего — в системных каталогах или в корне системного диска. Если за корневым каталогом следить легко (тут не так уж и много файлов), то в системных каталогах (\Windows, \Windows\System, \Windows\System32) искать намного сложнее, потому что здесь исполняемых файлов пруд пруди. В последнее время еще одним любимым местом обитания зловредного кода стал кэш для временных файлов из Интернета. И это логично, ведь сейчас над компьютером властвует браузер.

Вирусы чаще всего стараются попасть в автозагрузку, а это упрощает нам жизнь. В Windows есть утилита msconfig (в некоторых конфигурациях она может отсутствовать), с помощью которой можно легко узнать, что в системе запускается автоматически.

Чтобы воспользоваться утилитой, в меню **Пуск** в строке поиска введите имя программы msconfig.exe. Нажмите клавишу <Enter>, и перед вами откроется главное окно программы, которое состоит из нескольких вкладок. Нас будет интересовать предпоследняя — **Автозагрузка** (Startup). Перейдите на эту вкладку, и вы увидите окно, как на рис. 4.3.

Все имена, которые отобразятся в этом окне, должны быть вам знакомы. В принципе, если даже по незнанию отключить какой-либо флажок, то работу Windows это не нарушит. Может только пропасть какой-то значок в системной области возле часов или исчезнуть некая возможность. Чаще всего первое.

Весь список состоит из пяти колонок, нам понадобятся три:

- **Элемент автозагрузки** (Startup Item) — произвольное имя загружаемой программы. Чаще всего это полное название программы, иногда включает наименование компании;
- **Команда** (Command) — команда, которая выполняется, или путь к файлу;
- **Расположение** (Location) — местоположение загрузки программы.

Наблюдайте за названиями, которые здесь отображаются. Если появилась программа, которую вы не устанавливали, то моментально удалите ее. Следите за все-

ми строками, которые могут вызвать подозрение, например, чужая программа (так маскируются вирусы), странное название или имя запускаемого файла и т. д.

На рис. 4.3 в списке есть одна строка, в которой показан запускаемый файл y.exe с именем "y". Ни один производитель не будет называть так программу, и это должно зародить у вас подозрения. Для проверки можно убрать галочку напротив этой строки и перезагрузить компьютер.

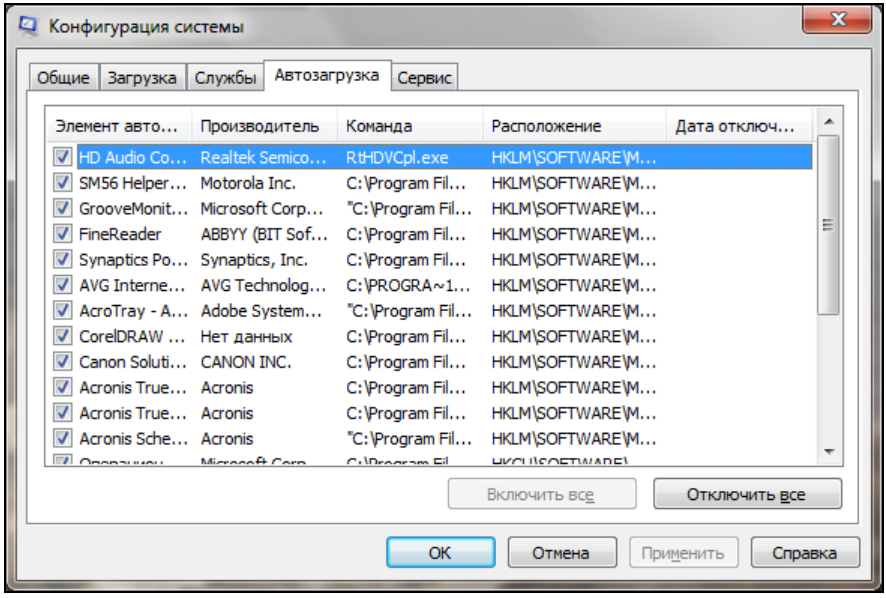


Рис. 4.3. Окно отображения автоматически запускаемых программ в msconfig

В колонке **Расположение** (Location) видно, откуда запускается программа. Здесь могут быть следующие варианты:

- **Основной загрузчик** (Common Startup) — находится в меню **Пуск | Все программы | Автозагрузка** (Start | All Programs | Startup). За этими программами легко наблюдать и без специализированных утилит;
- путь в реестре — если указано значение в таком виде, то вы можете просмотреть соответствующие ключи через программу Редактор реестра (regedit).

Если у вас нет подходящей утилиты, то придется самостоятельно просматривать реестр. Автоматически запускаемые программы можно увидеть в следующих разделах реестра:

- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run;
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce;
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run.

Пример списка автоматически загружаемых программ, полученный при просмотре реестра, приведен на рис. 4.4. Он идентичен перечню, сформированному утилитой msconfig.

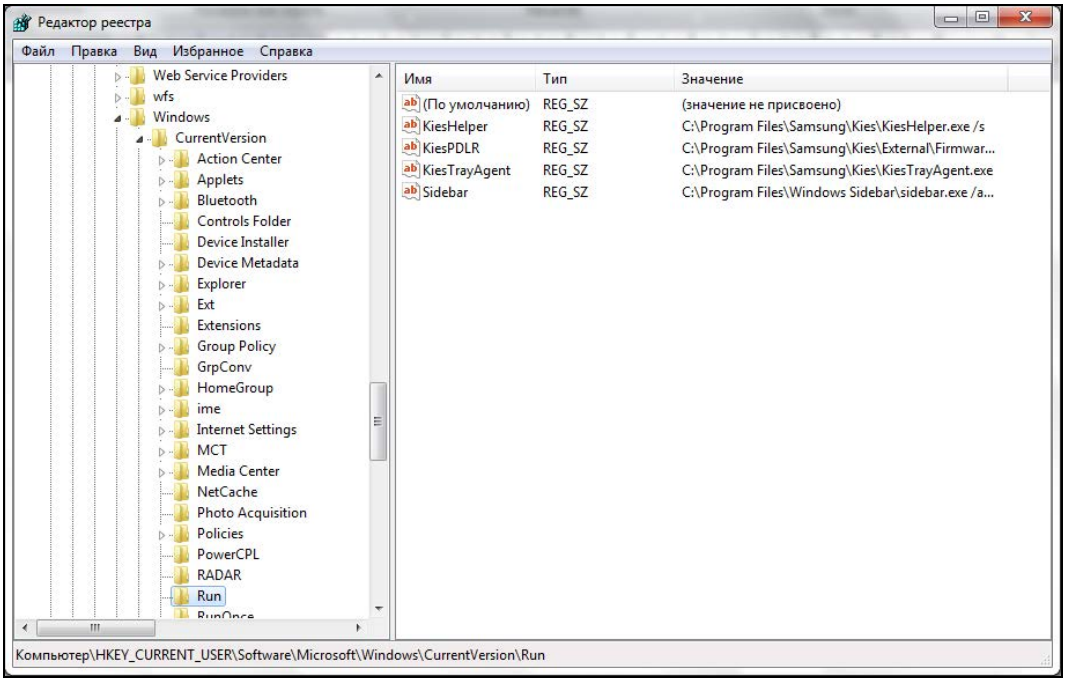


Рис. 4.4. Список автоматически загружаемых программ в реестре

С помощью специальной программы или через реестр мы узнаем имя файла, который выполняется. Не забывайте, что нужно удалить не только ссылку на программу в реестре, но и сам файл. Возможно, что он запускается еще при каких-то условиях, и тогда все может восстановиться в автозапуске, и зловредная программа снова будет стартовать автоматически.

Если файл не удаляется, то, скорее всего, он сейчас выполняется, и нужно завершить работу программы. Для этого совершите следующие действия:

1. Нажмите комбинацию клавиш <Ctrl>+<Alt>+<Del>. Если у вас серверная ОС, то откроется окно с шестью кнопками для выбора выполняемых действий. Нажмите здесь кнопку Диспетчер задач (Task Manager). В клиентской версии ОС сразу появится окно Диспетчер задач (Windows Task Manager).
2. В Диспетчере задач (рис. 4.5) перейдите на вкладку **Процессы** (Processes).
3. Найдите нужный процесс и нажмите кнопку **Завершить процесс** (End Process).

Когда будете отслеживать программы, обязательно обращайте внимание на каждую букву. Хакеры очень искусно умеют маскировать плоды своего творчества. Например, однажды я написал троянского коня, который должен был перезагружать компьютер начальника. Файл я назвал Internat32.exe и поместил в автозапуск через реестр. Целый месяц никто не мог понять, почему компьютер так нестандартно себя ведет. Его тестировали даже профессиональные администраторы, но ничего не нашли. А дело в том, что в системе есть программа Internat.exe, и ее выполнение критично для системы, поэтому ни один администратор не обратил внимание на файл с искаженным названием Internat32, хотя такого не должно быть.

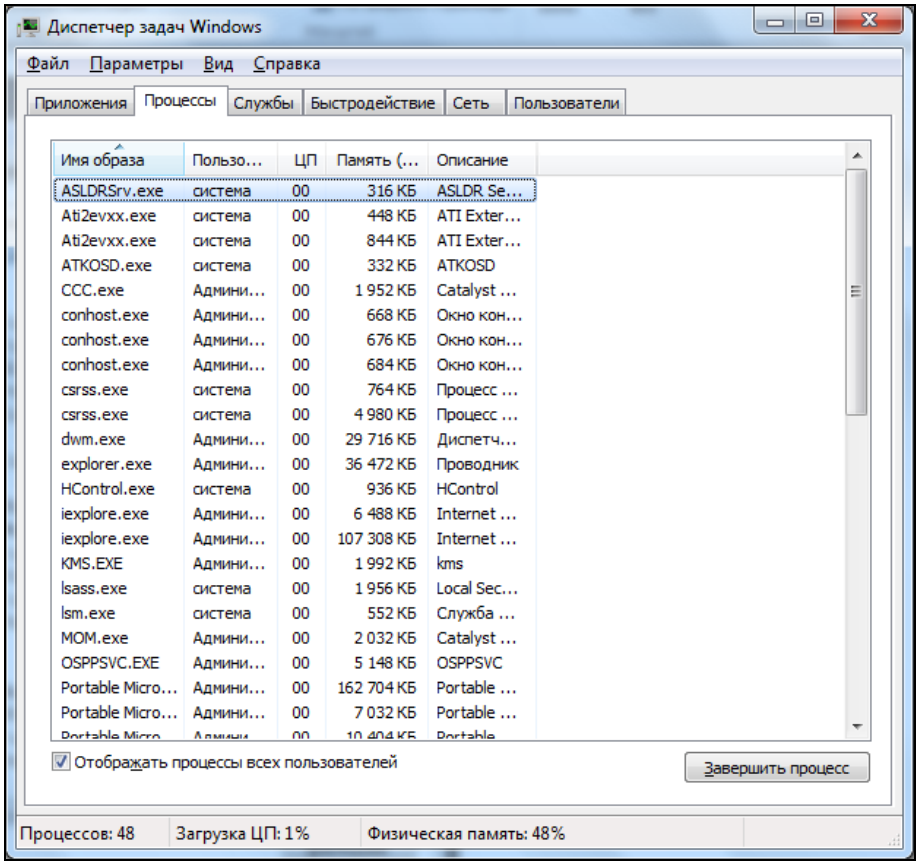


Рис. 4.5. Диспетчер задач — запущенные процессы

Еще один случай произошел через пару лет, когда мне поручили создать программу для слежения за тем, какие программы работают на компьютерах сотрудников нашей фирмы. Тогда троянского коня я назвал scanbisk.exe. И опять все прошло незамеченным. Просто в системах Windows 9*x* была утилита scandisk.exe для сканирования дисков, и никто не заметил, что в названии заменена буква "d" на "b".

Точно так же хакеры производят подмены символов и маскируют программы под другие. Буквы удобно замещать цифрами со схожим начертанием. Например, буква "O" может быть заменена цифрой 0, и это будет уже другой файл, а вот названия будут похожи, и на скорую руку отличие заметить сложно. Затем такой файл кладут в ту же папку, где находится программа, сходства с которой мы добиваемся, и большинство пользователей уже можно считать обманутыми.

Сервисы

В Windows у вирусов и троянов существует способ активизироваться при входе в систему — стать сервисом (службой). Сервисы — это программы, которые выполняются невидимо для пользователя и могут автоматически запускаться при старте системы.

Многие начинающие пользователи боятся управлять службами Windows, потому что некоторые из них могут оказаться критичными для работы. Именно поэтому хакеры в последнее время все больше внимания уделяют написанию зловредного кода в виде сервисов. Лично я подобных вирусов пока еще не видел, но трояны уже попадались. В ближайшее время все может измениться, и появятся вирусы, а может быть, это уже случилось, но я просто с ними не сталкивался.

Если мне не изменяет память, то первыми под службы начали маскировать программы нелегального сбора информации с компьютеров пользователей. Есть еще достаточно много злостных нарушителей нашего спокойствия, и вы должны регулярно следить за своими сервисами, чтобы там не появилось никаких неожиданных программ, которых вы не просили.

Управление службами происходит с помощью оснастки **Службы** (Services). Для ее запуска нужно выполнить **Пуск | Настройка | Панель управления | Администрирование | Службы** (Start | Control Panel | Administrative tools | Services). Перед вами откроется окно, как на рис. 4.6.

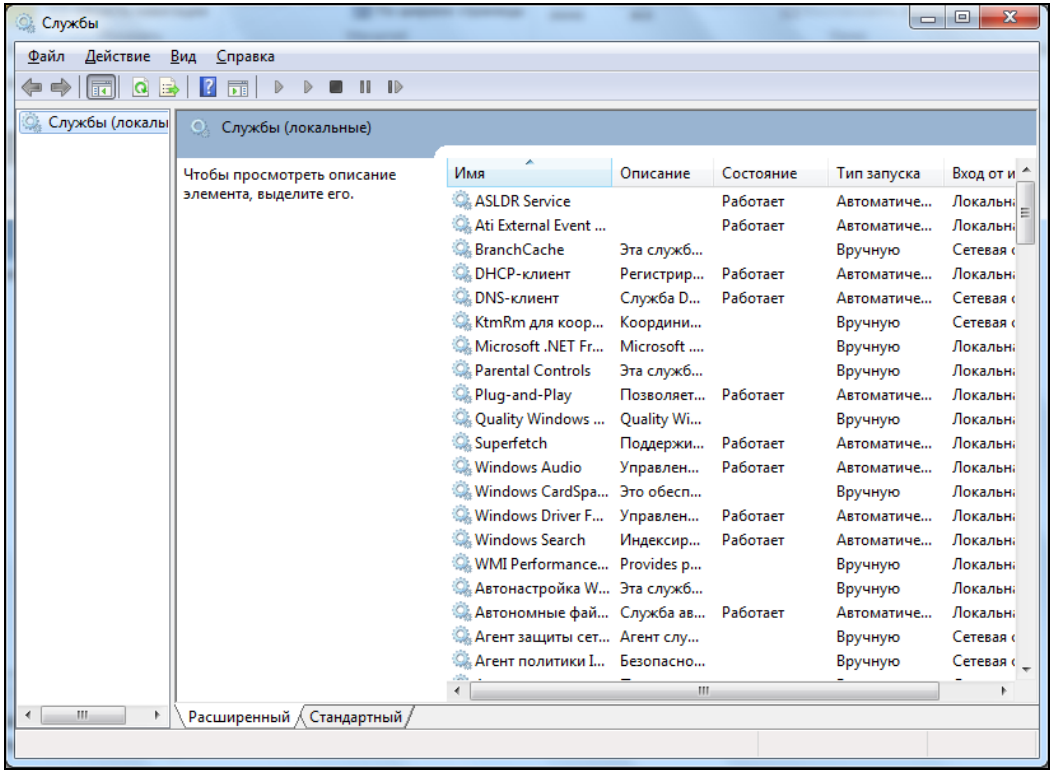


Рис. 4.6. Оснастка **Службы**

Список служб состоит из пяти колонок:

- **Имя** (Name) — короткое название;
- **Описание** (Description) — назначение службы;

- **Состояние** (Status) — текущий статус сервиса, здесь может быть надпись **Работает** (Started), если в данный момент служба функционирует;
- **Тип запуска** (Startup Type) — способ запуска службы. Здесь могут быть такие варианты:
  - **Автоматически** (Automatic) — служба запускается автоматически при старте системы;
  - **Вручную** (Manual) — служба запускается либо вручную, либо при запуске программ, которые ее запускают;
  - **Отключена** (Disabled) — службу запустить нельзя;
- **Вход от имени** (Log On As) — учетная запись, права которой будет иметь служба. Если учетная запись имеет права администратора, то служба будет обладать доступом ко всем ресурсам, а для гостевой учетной записи права ограничены. Чаще всего указывают системную запись, тогда служба будет иметь права пользователя, который вошел в систему.

Не поленитесь и узнайте, какие службы для чего предназначены. Это можно сделать с помощью описания, Интернета или специализированной литературы по ОС Windows. Сейчас в качестве сервисов распространяется много вредоносного кода, и вы должны уметь его обезвредить, не надеясь на антивирус.

Если вы видите название службы, которая вызывает подозрение, дважды щелкните по соответствующей строке, и перед вами откроется окно свойств выбранного сервиса (рис. 4.7).

На вкладке **Общие** (General) вы можете увидеть следующую информацию:

- **Имя службы** (Service Name) — короткое название сервиса;
- **Отображаемое имя** (Display Name) — название, которое вы видите в списке;
- **Описание** (Description) — короткий комментарий. Он очень краток, даже меньше того описания, которое можно увидеть в панели подсказки при расширенном просмотре списка сервисов;
- **Исполняемый файл** (Path to executable) — название файла и его расположение, т. е. командная строка, используемая для старта службы. После имени могут идти параметры, передаваемые сервису.

Вся эта информация предназначена только для просмотра, и редактировать ее нельзя. Но книга называлась бы по-другому, если бы я не показал вам, как можно ее изменить.

Если очень хочется, то подкорректировать можно все, и для этого нет необходимости наматывать мышью километры. Нужно только залезть в реестр и открыть ветку **HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services**. Вот здесь и перечислены все сервисы, и вы можете изменять любые их параметры. Названия разделов не всегда понятны и в большинстве случаев ничего не говорят об их предназначении. Поэтому приходится выделять каждый из них и смотреть в параметрах ключ **DisplayName**, чтобы определить точное имя.

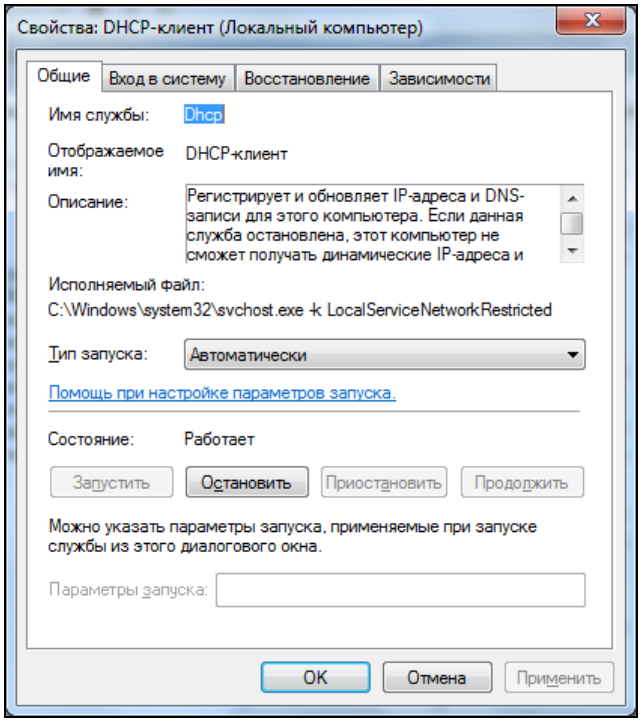


Рис. 4.7. Свойства службы

С помощью реестра вы безболезненно можете редактировать описания. Если хотите изменить параметры запуска, то тут желательно проштудировать документацию по интересующей вас службе. Изучайте хорошенько, потому что при неправильно заданных параметрах служба может запуститься не так, как вы хотите, или вообще не заработать.

Если вы сейчас посмотрите на свой реестр, то заметите, что разделов намного больше, чем вы могли видеть сервисов в оснастке **Службы** (Services) на рис. 4.6. Это связано с тем, что некоторые драйверы в системе запускаются как сервисы и даже работают схожим образом, но оснастка сервисов тут не помощник.

Как всегда, Microsoft предоставила нам возможность ограниченного управления, а большинство вещей осталось скрытыми. Главная проблема состоит в том, что мы не можем штатными средствами точно определить, какие службы сейчас запущенны, потому что видим далеко не все. Некоторые из сервисов достаточно сложны, состоят из нескольких частей и могут иметь по две ветки в реестре.

Я бы за это программистам Microsoft спасибо не сказал, потому что создается обширная поляна для маскировки вредоносного кода, который пока еще не очень прячется в сервисах. Но через год или два, если не появится хорошей возможности мониторинга служб, противный код основательно переберется из процессов в сервисы.

Но вернемся к окну свойств службы. В поле **Исполняемый файл** (Path to executable) окна настройки службы (см. рис. 4.7) можно увидеть путь к запускае-

мому файлу и по нему определить используемую программу. Здесь же есть кнопка **Остановить** (Stop) для остановки службы, после нажатия которой можно удалять все, что относится к сервису. Даже если эта кнопка недоступна, все равно сразу переходите к этой операции. В этом случае уничтожение будет отложенным и произойдет после перезагрузки компьютера.

Для удаления надо перейти в папку, где расположен соответствующий исполняемый файл, и запустить его, указав в качестве параметра ключ `/UNINSTALL`. Этим вы уберете из системы службу, а потом можно будет физически удалять файл с диска, дабы он вас больше никогда не смущал.

Чтобы облегчить себе жизнь и не следить самостоятельно за изменениями в сервисах, можно возложить эту обязанность на одну очень хорошую и полезную программу — Ad-Aware. Ее можно взять с сайта **http://www.lavasoft.com/**. Обязательно скачайте ее и установите, потому что Ad-Aware ищет нарушителей спокойствия среди сервисов и автоматически загружаемых программ.

Даже если вы автоматизируете процесс обнаружения злостного кода, это не значит, что можно сложить ручки и спокойно путешествовать по сомнительным страницам Интернета. Сейчас регулярно появляются новые программы, которые обходят защиту автоматизированных поисковиков, поэтому хоть иногда надо самостоятельно проверять работающие службы.

Еще один вариант контроля запускаемых программ — использование утилиты CyD NET Utils. Ее можно скачать с сайта **http://www.cydsoft.com/**. Здесь есть модуль управления сервисами как локального, так и удаленного компьютера. При этом можно включить отображение не только сервисов, но и драйверов, которые также запускаются из ветки реестра **HKEY_LOCAL_MACHINE\SYSTEM\ ControlSet001\Services**.

Смена параметров

Если ваш компьютер был заражен троянской программой, то после того, как вы вычистили систему, я рекомендую поменять все пароли. Большинство программ этого типа направлено именно на воровство кодов доступа. Первым делом меняйте пароли на Windows, после этого нужно сменить параметры входа в Интернет, и, наконец, не забудьте сменить пароли на все свои почтовые ящики, т. к. именно они чаще всего являются целью троянов.

Если есть время, то лучше сменить пароли на доступ к различным сайтам или форумам, где вы зарегистрированы. Возможно, что программа успела просканировать данные, которые вы вводили в браузере, и переслала их злоумышленнику. Если вы доверяете хранение паролей ОС или браузеру, то не исключено, что эти пароли ушли по сети. Поэтому самые важные из них следует сменить немедленно, например, пароли от доступа к интернет-банку.

Не исключено, что могут пострадать номера кредитных карточек или номера/пароли электронных кошельков. Конечно же, если у вас есть кредитная карточка, то не стоит торопиться ее менять (это может оказаться лишними затратами). Просто контролируйте расходные операции, и если появятся лишние платежи, то в

этом случае нужно сразу же бить тревогу, пока ваш счет не опустошили. Чтобы контролировать собственный счет, я подключил услугу информирования на мой мобильный телефон обо всех совершаемых транзакциях. Как только я оплачиваю что-то, ко мне приходит СМС с информацией о снимаемой сумме, так что ни одна операция не пройдет мимо моего глаза. При этом такая услуга в банке оказалась бесплатной, что очень даже удобно.

4.1.5. Защита ОС

Не отключайте User Account Control (UAC, контроль учетных записей пользователя). Это защита, которая появилась еще в Windows Vista. В Windows 7 в этой системе произошли небольшие изменения в лучшую сторону, и теперь она не так сильно надоедает подтверждениями.

Контроль учетных записей UAC был создан для того, чтобы не допустить изменения наиболее важных компонентов ОС и областей, которые могут повлиять на работу компьютера. Смысл в том, чтобы отделить системные файлы и разделы реестра от пользовательских данных. Пользователь и программы, запущенные пользователем, могут сколько угодно изменять собственные файлы, но если программа хочет поменять что-то в системной области, пользователю дается предупреждение и он должен разрешить подобные изменения.

По задумке разработчиков системными стали папки c:\Program Files, c:\Windows и даже корень системного диска (под c: подразумеваем системный диск, ведь в реальности буква может быть и другой) и некоторые разделы реестра, в том числе и отвечающие за автоматический запуск приложения или сервиса. Если программа хочет сохранить что-то в папке Program Files, она должна получить одобрение от пользователя системы. Это правильное решение, только вот очень много программ до появления Windows Vista сохраняли свои настройки в ini-файлах и хранили их рядом с исполняемым файлом или прямо в каталоге c:\Windows. Если исполняемый файл находится в каталоге Program Files, то при запущенном UAC могут возникнуть проблемы, потому что он будет требовать подтверждения запуска программы в режиме администратора или программа может работать некорректно.

Запускать программы от имени администратора и давать им привилегии, которые им не нужны, только потому, что программист не следует правилам написания кода — ошибка. Уж лучше попробовать найти корректную программу.

Я видел, как UAC отключали потому, что он надоедал на новых компьютерах. Когда мы покупаем новый компьютер, то устанавливаем необходимые программы и программы установки добавляют в систему файлы и изменяют какие-то настройки в системе. Когда компьютер сконфигурирован, то изменений в системных файлах или папках не должно быть и тогда UAC будет молчать. Лично я вижу его подтверждения очень редко, и в основном когда какая-то программа обновляется.

Чтобы запустить управление UAC нажмите кнопку **Пуск** (Start) и наберите в строке поиска программ `учетные записи пользователей` (в английской версии — `UAC`). Для русской версии ОС должна найти программу **Изменение параметров контроля**

учетных записей (UAC), для английской — **Change User Account Control Settings**.

В Windows Vista были только два варианта — включить или выключить контроль. В Windows 7 контроль стал более интеллектуальным. По умолчанию подтверждение будет требоваться в том случае, если какая-то программа пытается получить доступ к запрещенной области. Если же вы сами пытаетесь что-то изменить, то ОС может принять изменения без подтверждений. Тут конечно очень тонкая грань между тем, когда пользователь меняет данные, а когда — программа. Ведь пользователь сам ничего не может поменять, он всегда просит программу сделать это. Но в Windows 7 все же подтверждения не так надоедливы, если сравнивать с Vista.

И даже если вы считаете Windows 7 слишком назойливой, не отключайте UAC, потому что он может спасти компьютеру жизнь. При включенной защите без вашего разрешения ни один вирус не сможет записать себя в автозагрузку, в системную область или в корень диска. Без этого вирус может быть скопирован на компьютер, но запустить его сможете только вы сами.

Если вы запускаете что-то, что не является установочной программой, полученной из официальных источников, а эта программа требует административного доступа и UAC настаивает на подтверждении, то я бы не стал запускать такой файл вовсе. Простые программы типа текстовых редакторов, графических утилит и любые другие программы каждодневного использования не должны требовать привилегированного доступа для своей работы.

4.2. Полный доступ к системе

Компьютерные шутки, рассмотренные в *главе 3*, очень часто требовали доступ к дискам компьютера, и лучше всего по сети. Но многие пользователи открывают доступ только к безобидным папкам. Если вы знаете пароль администратора на компьютере жертвы, над которой хотите подшутить, то логические устройства становятся для вас доступными автоматически. Но если войти в сетевое окружение, то будут представлены только открытые папки.

Как же увидеть какой-нибудь диск, зная пароль администратора? Нужно набрать в Проводнике в строке для ввода адреса следующий путь: ***Компьютер\c$***, где ***Компьютер*** — это имя или IP-адрес компьютера. Затем через обратный слеш (\) пишется имя нужного устройства и знак доллара. Таким способом мы получаем полный доступ к диску, который не виден в сетевом окружении.

Если в вашей сети используется доменная организация, то администраторы домена по умолчанию имеют полные права на каждый компьютер в группе. Для доступа к любому устройству достаточно указать адрес компьютера в виде ***Компьютер\c$*** . Это не есть хорошо.

Тут хочется привести пример из личной жизни. Однажды я пришел в одну фирму и добродушно ввел свой ноутбук в домен. Но через пять минут я заметил некую активность по сети. Об этом говорило необъяснимое моргание значка сетевого под-

ключения, а ведь я в данный момент ничего не передавал. Да и нагрузка на жесткий диск почему-то была достаточно большой.

Просмотр подключений показал, что это недобросовестный администратор местной сети пытается поковыряться в моей личной информации и скачать мои секретные файлы. Благо все пароли на диске спрятаны так, что даже я с трудом могу их найти, особенно после долгих новогодних праздников. Иначе злой администратор украл бы исходные коды моих программ или электронные версии книг, чтобы опубликовать их в Интернете или продавать мои программы под своим именем, и годы плодотворного труда ушли бы в трубу. Я, конечно, не Билл Гейтс, но исходные коды являются результатом кропотливой работы и моей собственностью, которая должна приносить прибыль мне, а не любопытной Варваре.

Как только я удостоверился, что по дискам моего компьютера путешествует посторонний, и точно определил обидчика по его адресу, я тут же выдернул из ноутбука сетевой кабель. Это позволило разорвать связь и не дать злоумышленнику продолжать скачивать данные. Если вы окажетесь в подобной ситуации, то советую поступать так же.

Теперь нужно было найти этого шустрячка и растолковать ему, что он не прав. Поиск тоже не составил труда, потому что женщины в кабинете, где я находился, показали дорогу в комнату администраторов. Через две минуты я разминал мышцы худощавого мальчика, посмевшего забраться на мою территорию :). После этого я вежливо попросил удалить все позаимствованное с моего жесткого диска и проконтролировал этот процесс.

Чтобы у вас не возникло подобных проблем, необходимо отключить доступ к компьютеру сторонним администраторам. Для этого нужно выполнить следующие шаги:

1. Щелкните правой кнопкой мыши по строке **Компьютер** (Computer) в меню **Пуск** (Start) и в появившемся контекстном меню выберите пункт **Управление** (Manage). Перед вами откроется окно управления компьютером (рис. 4.8). Слева расположено дерево его элементов, которыми можно управлять.
2. В этом дереве откройте ветку **Управление компьютером | Служебные программы | Локальные пользователи и группы | Группы** (Computer Management | System Tools | Local Users and Groups | Groups). В правой части окна вы должны увидеть список всех доступных групп. Найдите строку **Администраторы** (Administrators) и дважды щелкните по ней.

   Примечание

   В Home-редакции управления пользователями нет. Тут можно воспользоваться утилитой netplwiz. Нажмите кнопку **Пуск** и в строке поиска наберите название этой утилиты. Перед вами откроется окно, как на рис. 4.9.

3. Если вы работаете в системе под учетной записью администратора, то удалите все остальные. Если у вас своя учетная запись, то оставьте ее и учетную запись **Администратор** (Administrator). Пользователи Home-редакции не могут менять группы. Тут можно только посочувствовать. Но есть сторонние утилиты, кото-

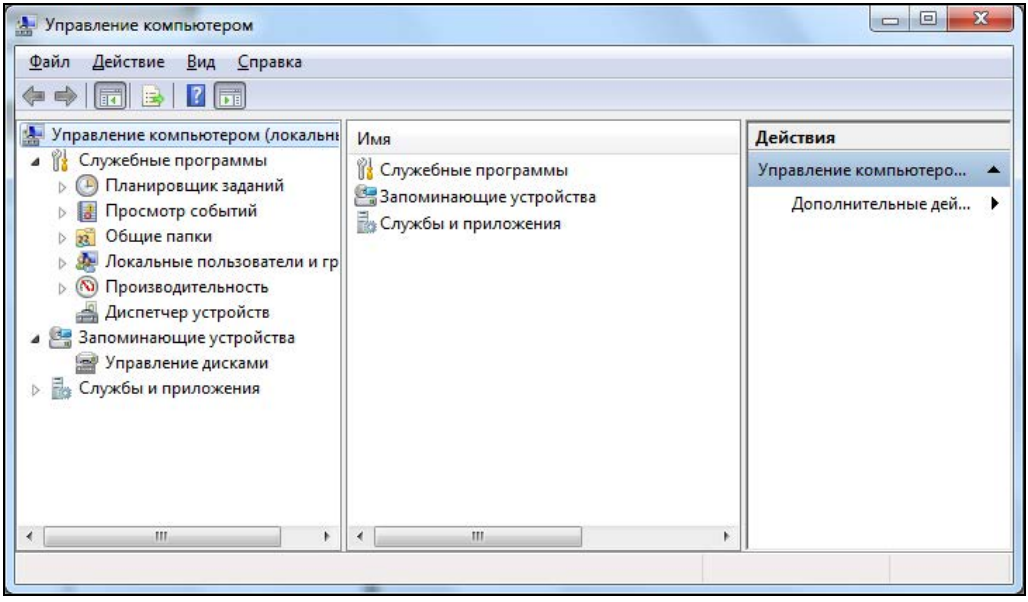


Рис. 4.8. Окно управления компьютером

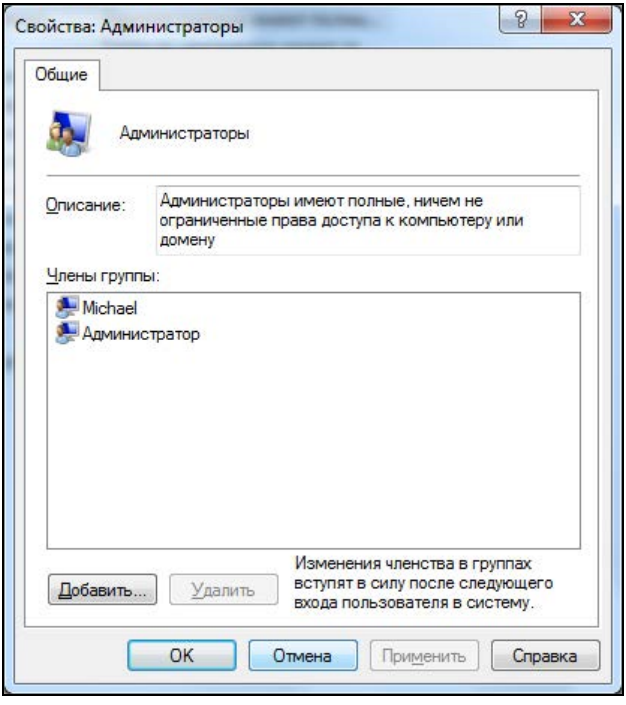


Рис. 4.9. Окно управления пользователями

рые позволяют это делать. Запрещен только интерфейс. Я пробовал получить доступ программно (писал собственную программу на Delphi), и у меня получалось.

Теперь ни один администратор домена не сможет получить доступ к вашим дискам, не зная пароль именно вашего локального администратора системы.

Некоторые считают, что достаточно только запретить доступ к жесткому диску, и сторонний администратор уже не сможет проникнуть в ваши владения. Для этого нужно войти в свойства папки или диска (т. е. объекта, который нужно защитить от постороннего глаза) и на вкладке **Доступ** (Security) удалить всех пользователей, кроме себя любимого. Тем, кого нельзя удалить, нужно запретить все действия.

Теперь в папку сможете попасть только вы, и вроде бы мы добились желаемого результата, без удаления администратора из свойств. Но это только вроде, а на самом деле, если захотеть, то данное ограничение легко обойти. Администратор домена все еще имеет полные права в вашей системе, а значит, может изменять права и на папки. Итак, что должен сделать администратор домена для возвращения себе прав?

1. Войти в оснастку управления компьютером (правой кнопкой мыши щелкаем по строке **Компьютер** (Computer) в главном меню Windows и выбираем команду **Управление** (Manage).
2. Выбрать пункт меню **Действие | Подключиться к удаленному компьютеру** (Action | Connect to another computer), который доступен, если в левой части окна выделен пункт **Управление компьютером (локальным)** (Computer Management (Local)).
3. Найти нужный компьютер и нажать кнопку **OK**.

Теперь вы можете управлять чужим компьютером со своего. Чтобы вернуть доступ, переходим в раздел **Служебные программы | Общие папки | Общие ресурсы** (System Tools | Shared Folders | Shares). Здесь можно открыть доступ к запрещенному ресурсу, причем даже для всех пользователей. Так что удаление всех нежелательных пользователей из группы администраторов является обязательным действием.

4.3. Виагра для BIOS

Большинство из нас, когда не хватает мощности компьютера, бежит его обновлять. А ведь можно увеличить производительность без дополнительных вложений с помощью оптимизации работы компьютерного железа или даже разгона.

Чем отличается оптимизация от разгона? Оптимизация — это настройка параметров устройств с целью максимального использования их ресурсов. При этом мы не нарушаем указанные производителем рекомендации. При разгоне железо заставляют работать на пределе возможностей и с нарушением правил эксплуатации.

Почему надо оптимизировать компьютер? Большинство стационарных компьютеров выпускается с настройками в BIOS (Basic Input/Output System, базовая система

ввода/вывода) по умолчанию. При этом устанавливаются такие значения, при которых любые комплектующие будут работать надежно. Но компоненты различных производителей могут иметь разные технические характеристики и возможности. Если не менять заводские настройки, то железо будет работать с минимальным потенциалом.

В этом отношении очень хорошо покупать ноутбуки и компьютеры крупных производителей, таких как Apple, IBM, Sun. В них тщательно подбирается комбинация компонентов, и BIOS настраивается на оптимальное использование возможностей. В таких компьютерах вообще может не понадобиться сложных настроек. Если вы видели программы конфигурации BIOS для ноутбуков, то должны понимать, о чем я говорю.

Если же компьютер собран в гараже из различных запчастей, то он, скорее всего, будет иметь низкую производительность. Тратить большие деньги на технику и использовать ее по минимуму, по меньшей мере, глупо. Поэтому вы должны уметь выжать из железной коробки все, на что она способна.

4.3.1. Оптимизация системы

Как я уже сказал, оптимизация системы связана с настройкой BIOS. Описывать этот процесс достаточно сложно, потому что существует немало производителей, которые оформляют утилиту настройки по-своему, да еще с учетом многочисленных версий. Однако основные параметры все же называются везде одинаково. Я буду рассматривать настройку на основе самой популярной BIOS от фирмы Award.

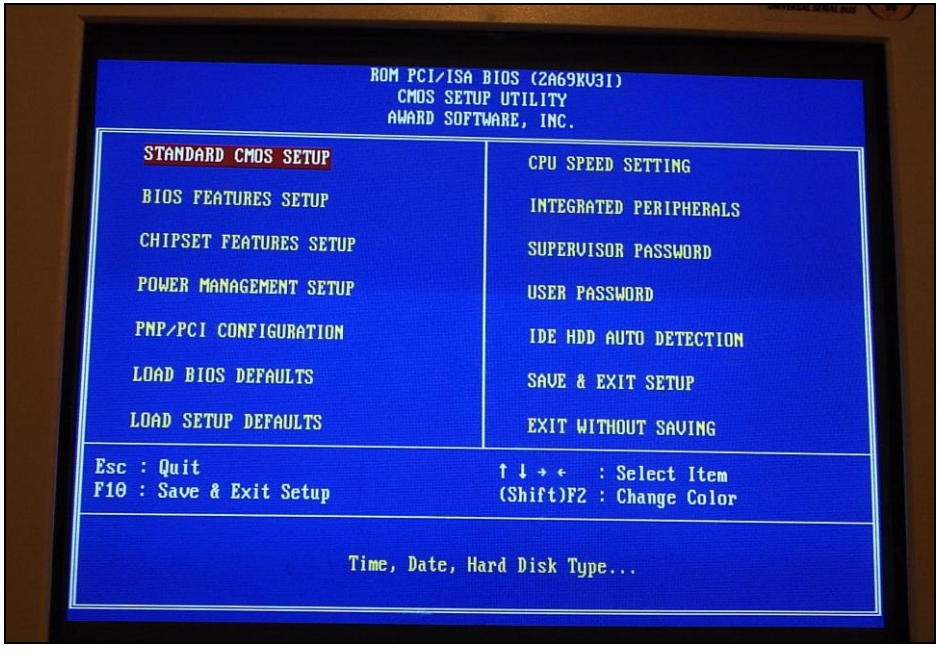


Рис. 4.10. Утилита настройки BIOS от Award Software

Для настройки BIOS нужно перезагрузить компьютер и нажать клавишу входа в утилиту. Какую клавишу нажимать? Во время тестирования памяти и определения IDE-дисков внизу экрана можно увидеть подсказку, которая в переводе с английского значит "Нажмите Del для входа в BIOS". Чаще всего это бывает клавиша <Del>, но иногда встречается <F2> или <F12>.

Современные BIOS имеют возможность не отображать ход тестирования компьютера, а скрывать все за черным экраном или логотипом. В этом случае после начала загрузки нужно многократно нажимать клавишу <Del>, пока не появится главное меню утилиты настройки BIOS. На рис. 4.10 приведен пример такой программы от компании Award Software.

Некоторые из описываемых параметров могут не совпадать для разных компьютеров. И если вы заметили отличия, то я рекомендую ознакомиться с документацией на BIOS к материнской плате вашего компьютера. Книжки-инструкции, которая идет в комплекте с компьютером, будет достаточно. В крайнем случае можно поискать документацию на сайте производителя.

4.3.2. Быстрая загрузка

Самое первое, что надо ускорить в своем компьютере, — это загрузка. Здесь можно оптимизировать тестирование системы. Например, зачем трижды прогонять тест памяти или проверять наличие дисковода, когда это просто не нужно.

Выберите в меню утилиты настройки пункт **Advanced Chipset Features** (Расширенные возможности набора микросхем), в некоторых утилитах это просто **Advanced**. И перед вами откроется список параметров этого раздела (рис. 4.11). В отдельных версиях BIOS в разделе **Advanced** параметры могут быть сгруппированы по подразделам, и ваша задача — найти нужный параметр в одном из них.

Первое, что я рекомендую, — это установить параметр **Quick Boot** в значение **Enabled**. Чаще всего значения изменяются клавишей <Enter> или клавишами <PgUp> и <PgDn>. Теперь, чтобы при старте компьютера не было лишних обращений к дисководу, нужно установить параметр **Seek Floppy** в значение **Disabled**. За окном полным ходом идет XXI век, и если вы все еще используете это старье в виде гибких дисков, то могу только посочувствовать. Тем более что дисковод будет работать даже и с этим значением параметра.

В современных компьютерах такие параметры могут отсутствовать, и, по моим наблюдениям, в таких версиях BIOS память тестируется один раз и не происходит поиска дисковода при старте. Второй параметр отключили, скорее всего, потому, что 3,5-дюймовые дисководы сейчас уже устанавливают все реже.

В большинстве систем по умолчанию компьютер ищет загрузчик сначала на дискете, а потом уже на главном жестком диске. Если вы очень редко загружаетесь с флоппи-диска, CD или флешки, то я рекомендую изменить порядок и поставить жесткий диск в качестве первого устройства. Зачем лишний раз исследовать дисковод на наличие дискеты с загрузчиком или другое устройство, когда это необходимо раз в год.

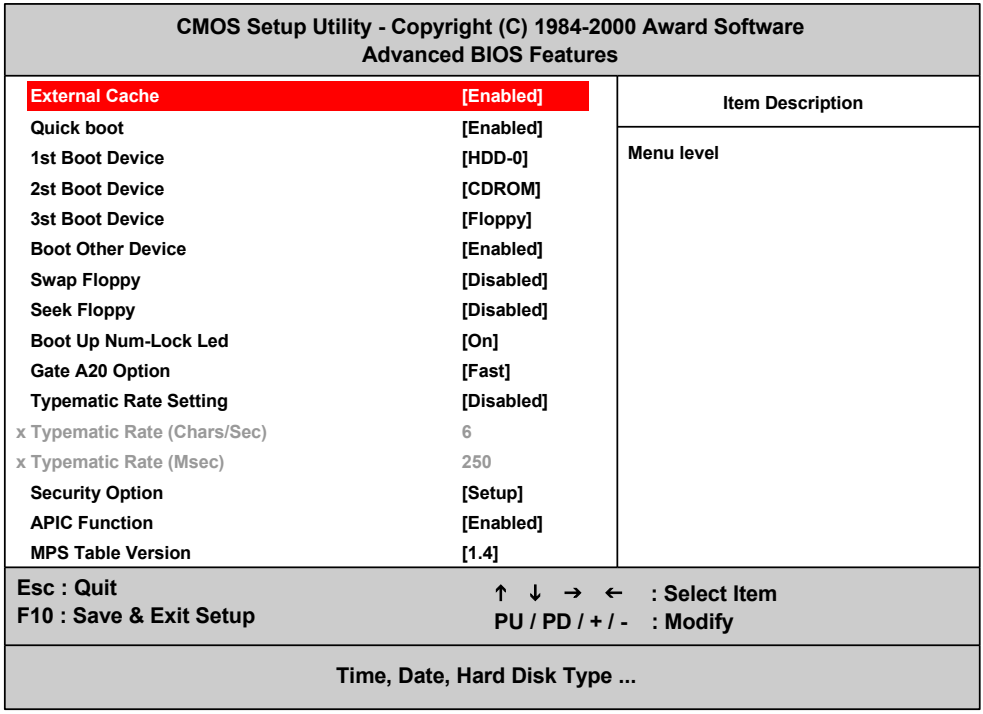


Рис. 4.11. Параметры раздела **Advanced Chipset Features**

Чтобы изменить порядок загрузки, в большинстве BIOS нужно выделить строку **1st boot device** и клавишей <Enter> или <PgUp>/<PgDn> изменить значение на **HDD-0**. Есть утилиты настройки BIOS, в которых порядок загрузки изменяется не в разделе **Device**, а в отдельном разделе **Boot**.

4.3.3. Определение дисков

Очень часто по умолчанию в BIOS установлено автоматическое определение IDE-устройств — жестких дисков и приводов CD-ROM. Но большинство из нас меняет HDD или приводы CD/DVD раз в год, а то и реже. Так зачем же каждый день при загрузке заново их определять?

Настройки определения жестких дисков хранятся в разделе **Standard CMOS Features** (Стандартные возможности CMOS) (рис. 4.12) или в подразделе **IDE Configuration** раздела **Advanced BIOS Features** (Расширенные возможности BIOS). Здесь перечислены четыре устройства IDE (Integrated Device Electronics): два **IDE Primary** (основной встроенный интерфейс дисковых устройств) и два **IDE Secondary** (вторичный IDE). Нигде не должно присутствовать слово **Auto**. Если к одному из шлейфов подключен винчестер или привод CD/DVD, то вы должны это явно указать. Если устройства нет, то установите значение **None** (Нет), чтобы при включении компьютера не проверялся пустой канал.

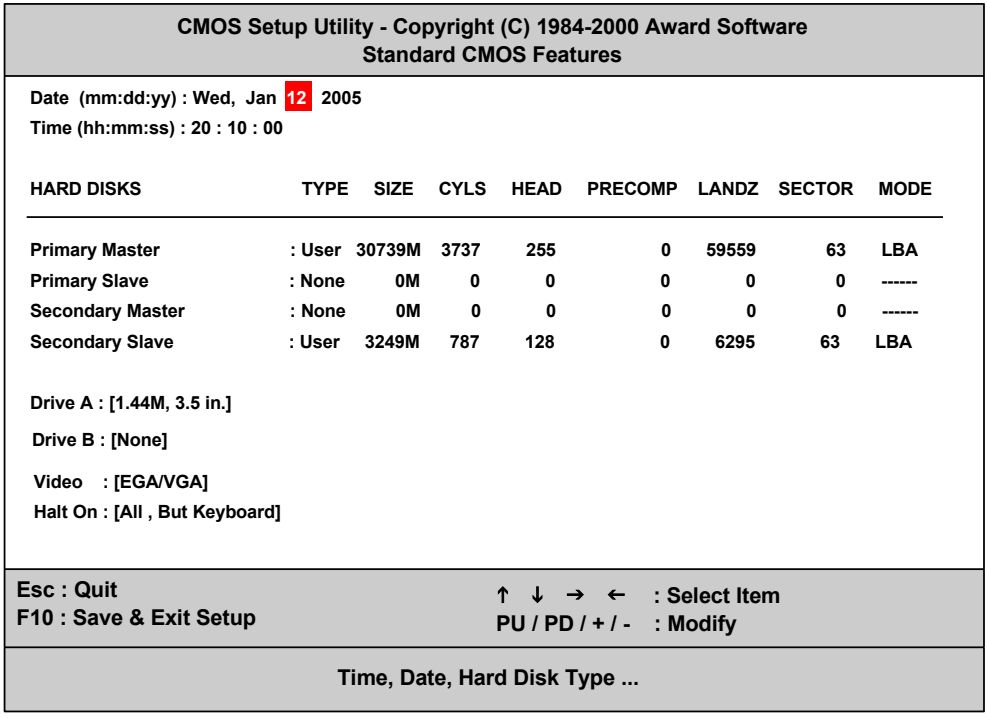


Рис. 4.12. Параметры раздела Standard CMOS Features

Для явного указания подключенного диска нужно выбрать вместо **Auto** значение **User**, и BIOS тут же постарается определить подключенное устройство. Если попытка не удалась, то возможны два варианта:

- к данному каналу ничего не подключено, и нужно указать значение **None**;
- надо использовать отдельный пункт для автоматического определения дисков, расположенный в главном меню утилиты настройки BIOS. Выберите его и выполните поиск устройств.

4.3.4. Быстрая память

В компьютеры может устанавливаться память различных типов, и при настройках по умолчанию BIOS берет самые слабые значения. Скорость памяти характеризуется тремя основными параметрами (перед каждым параметром может содержаться имя типа памяти SDRAM, DRAM и др.):

- **CAS# Latency** — определяет время, необходимое для получения запрашиваемой ячейки с данными (самый важный параметр) Здесь можно указывать значения **2**, **2,5** или **3**. Чем меньше значение, тем меньше задержка и быстрее работа. Современная память хорошо работает при значении **2**, и нет смысла его завышать;
- **RAS# to CAS#** — задержка при чтении памяти, которая может принимать значения от **2** до **4**. Оптимальным считается значение **3**, потому что в этом случае

гарантируется стабильная работа на всех типах памяти и с любыми процессорами. Если вы уверены в качестве памяти, то можно уменьшить значение до **2**. Если будут возникать проблемы, то верните значение **3**;

- **RAS# Precharge** — время до перезаписи блока памяти. Можно указывать значения от **2** до **4**. Стабильность гарантирует число **3**, но при качественной памяти можно понизить значение и до **2**.

Настройки этих параметров можно найти в разделе **Advanced BIOS features** или в подразделе **Chipset Configuration** раздела **Advanced** (зависит от версии BIOS). Чтобы иметь возможность изменить эти параметры, нужно выполнить следующие действия (в зависимости от утилиты конфигурирования BIOS):

- параметр **System performance** установить в состояние **Expert** (рис. 4.13), а **Memory Timings** — в **User**;
- параметру **Extended configuration** присвоить значение **User Defined**, и **SDRAM Timing Control** установить в состояние **Manual-user defined**.

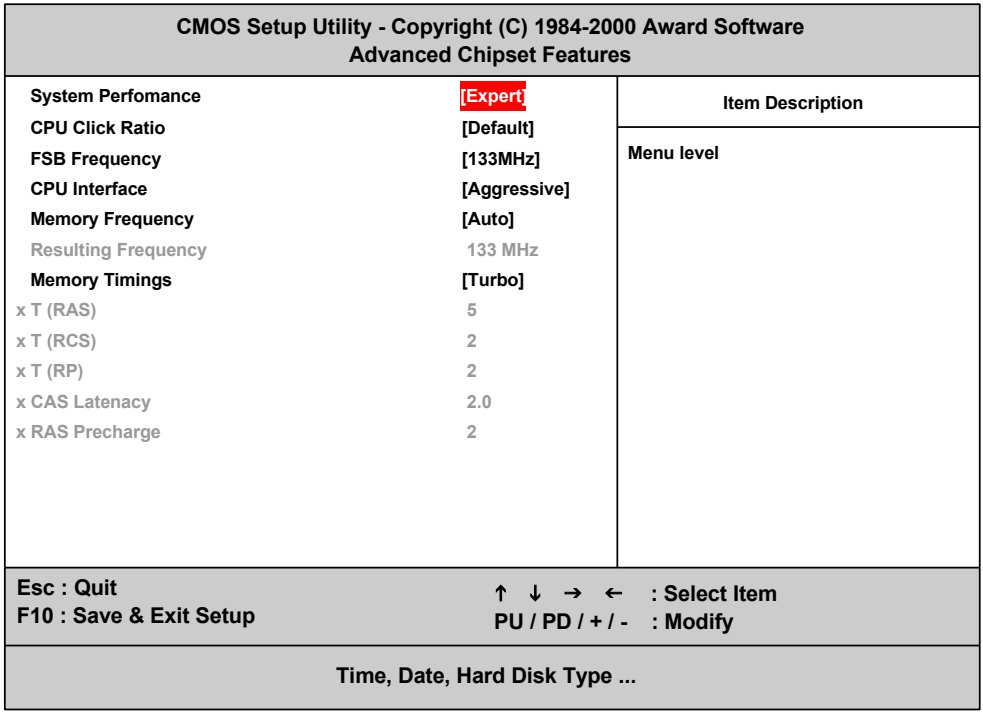


Рис. 4.13. Настройка параметров работы памяти

Смысл обоих действий схож, а разница существует только в названиях, потому что производители именуют параметры, как им вздумается, а иногда просто не могут использовать имена параметров других производителей из-за всяких лицензий и патентных ограничений.

4.3.5. Тотальный разгон BIOS

BIOS — это программа, а в ней могут быть и бывают ошибки, которые влияют на работу системы. Если компьютер работает нестабильно, то это не обязательно происходит из-за Windows. Было немало случаев, когда виновниками сбоев оказывались ошибки в процессоре или BIOS. И Intel, и AMD уже не раз отзывали целые партии процессоров, а производители материнских плат — свою продукцию для перепрошивки.

Чтобы исправить погрешности, нужно обновлять BIOS, при этом исчезают и некоторые ошибки в работе компьютера. Такая процедура может улучшить производительность, если новая прошивка работает быстрее. Это как драйвер: если он работает быстро, то и система бегает, как спринтер, а если тормозит, то весь компьютер будет спать даже при банальных обращениях к периферии.

Описывать прошивку BIOS бесполезно, потому что способ выполнения зависит от материнской платы и ее производителя. В последнее время этот процесс упростился до запуска утилиты, которая перезагружает компьютер и все делает автоматически, главное — взять нужный файл именно с сайта производителя и конкретно для вашей материнской платы. Установка неверной версии BIOS может сделать старт компьютера невозможным, и восстановить работоспособность можно будет только в сервисном центре. Если ошибка обновления произошла по вашей вине, то воскрешение будет платным.

Я рекомендую обновлять BIOS, но только иногда и не сразу после выхода новой версии прошивки, т. к. она тоже зачастую содержит ошибки. Поэтому стоит подождать, пока другие пользователи обожгутся или производитель сам тщательно не протестирует свежую версию.

Обновление BIOS может позволить вашему компьютеру работать с современными устройствами или процессорами, а может исправить критические ошибки. Один мой ноутбук (Fujitsu-Siemens) после покупки не работал от аккумулятора, а другой отказывался воспринимать сетевые карты PCMCIA. В обоих случаях помогло обновление BIOS.

4.4. Разгон железа

В предыдущих изданиях этой книги в этом месте было много информации по разгону компьютера и в основном процессора. В этом издании я перенес всю эту информацию в отдельный документ (см. Doc\Other\Разгон компьютера.docx) в электронный архив, который можно найти по адресу **ftp://85.249.45.166/9785977507905.zip** или на странице этой книги на сайте **www.bhv.ru**. Для этого у меня было всего две причины, и мне двух достаточно в отличие от Николаева.

Первая причина это... Информация безнадежно устарела. Хотя не совсем безнадежно, потому что часть информации еще более-менее актуальна, да и еще вполне реально встретить разгоняемое железо.

Вторая причина, я считаю, в том, что настало время, когда разгон процессора уже не нужен. Лично я при выборе компьютера вообще не обращаю внимания на частоту процессора. Даже самого примитивного будет достаточно для того, чтобы прекрасно работала ОС, шустро обрабатывал мои молниеносные движения пальцев Microsoft Word, и даже бегали игры. Хотя для игр более важным является процессор видеокарты, особенно для локальных игр, а не online.

Тратить время и рисковать перегревом системы ради сомнительной выгоды в вычислительной мощности процессора не вижу смысла. Это пустая трата времени и сил, тем более, что ОС сейчас идут на все, чтобы не использовать процессор по максимуму для экономии энергии. Это касается мобильных систем, которые все больше становятся популярными. И если я не ошибаюсь, то количество продаваемых ноутбуков сейчас превышает количество стационарных компьютеров.

Чтобы реально выиграть в скорости, нужно обратить внимание на слабое звено компьютера. А самым слабым сейчас является жесткий диск. Это, кажется, единственное механическое устройство, которое сохранилось в современных компьютерах, по крайней мере, в большинстве компьютеров. Из него выжали максимум возможного, и дальше уже набирать обороты проблематично.

Чтобы реально выиграть в скорости, можно перейти на более современное устройство — SSD-накопители. Это уже электроника, чтение данных с которой происходит намного быстрее и загрузка компьютера реально увеличивается в несколько раз. Не на 10—15%, которые можно выиграть максимальными разгонами, а намного больше.

Да, сейчас пока SSD обходится очень дорого и 256-гигабайтный диск стоит в несколько раз дороже обычного жесткого диска. Но время летит быстро, и я уверен, что уже через год они станут более доступными. На данный момент очень много используется SSD-накопителей в планшетах и в ультратонких ноутбуках Apple серии Air, но уже к выходу этой книги Intel планирует вывести на рынок множество новых серий ультратонких ноутбуков с различными производителями. Популяризация может привести к значительному падению в цене, а значит, к выгоде для нас с вами, как потребителей.

Вторым слабым звеном, которое еще остается в наших компьютерах, является оперативная память. Мне кажется, что оперативной памяти для современных систем должно быть не менее 3 Гбайт. В принципе, эта проблема решается, и большинство компьютеров уже поставляется в такой конфигурации.

Чем больше оперативной памяти, тем проще ОС работать с программами. Не нужно выгружать на диск неиспользуемые страницы памяти, потому что и так достаточно большой резерв. ОС и ваши прикладные программы могут загрузить все что необходимо в быструю оперативную память и обрабатывать все данные без обращения к медленному жесткому диску.

Так что тут разгонять тоже особо нечего, нужно просто добавить немного оперативной памяти, если ее не хватает.

4.5. Разгон видеокарты

Самый простой и безобидный способ ускорить работу видео — обновление драйверов. Например, когда появляется новая видеокарта от NVIDIA, то ее драйверы зачастую еще "сырые" и используют железо не на всю мощь. Это связано с тем, что программистский отдел всегда запаздывает (не успевает за железячниками). Сначала выпускают чип, а потом уже пишут для него окончательную версию драйверов. В процессе разработки видеочипсета невозможно написать оптимизированный код, поэтому происходит небольшая задержка.

А почему не придержать железо до выхода нормального софта? Тут вступает в силу другой закон. Нет смысла задерживать новую разработку на складе, когда она должна приносить прибыль. Поэтому видеокарты запускают в производство раньше, чем для них готов соответствующий драйвер.

Если судить об NVIDIA и ее продуктах, то эта фирма постоянно выкладывает свежие версии драйверов, которые позволяют улучшить качество картинки и повысить производительность компьютера. Но были случаи, когда новейшая версия софта, наоборот, работала медленнее или вообще отказывалась работать. Однажды был выпущен вариант, в котором некоторые сложные расчеты производились настолько в приближенном виде, что качество картинки пострадало, зато значительно поднялась производительность. Поэтому я рекомендую обновлять драйверы регулярно, но аккуратно, т. к. это не всегда может привести к хорошим результатам. После выхода свежей версии всегда нужно удостовериться в ее работоспособности и качестве на каком-либо тестовом компьютере.

Есть программы, которые с помощью графического интерфейса помогут вам повысить производительность за счет разгона процессора видеокарты или частоты работы памяти. Наиболее популярная из них — это PowerStrip. Программа получила большое распространение благодаря поддержке всех основных видеокарт. Конечно же, разгон будет доступен только в тех случаях, когда это возможно для данной карты.

PowerStrip можно скачать с сайта **http://entechtaiwan.net/util/ps.shtm**. Она позволяет настраивать любые параметры видеокарты, в том числе скорость работы чипа и памяти. Установите программу и перезагрузите компьютер. После перезапуска в системной области возле часов появится новый значок программы PowerStrip. Щелкните по нему, и перед вами откроется меню, в котором надо выбрать **Performance profiles | Configure** (Профили выполнения | Конфигурация). Затем отобразится окно настройки параметров, определяющих производительность видеокарты (рис. 4.14).

В поле **Engine clock** отображается текущая частота работы графического процессора, установленного на видеокарте. В поле **Memory clock** можно увидеть скорость работы видеопамяти. Вдоль левой кромки окна располагаются два бегунка, перемещая которые вверх/вниз можно изменять рабочие частоты: левый отвечает за скорость графического процессора, а правый — за память.

Как и в случае с разгоном процессора, скорость работы видеокарты нужно повышать постепенно, по одному делению и поочередно (процессор, память, процессор,

память и т. д.) и тщательно тестировать после каждого изменения. Как только появилась нестабильность, надо сразу же немного понизить скорость процессора и памяти и на этом остановиться.

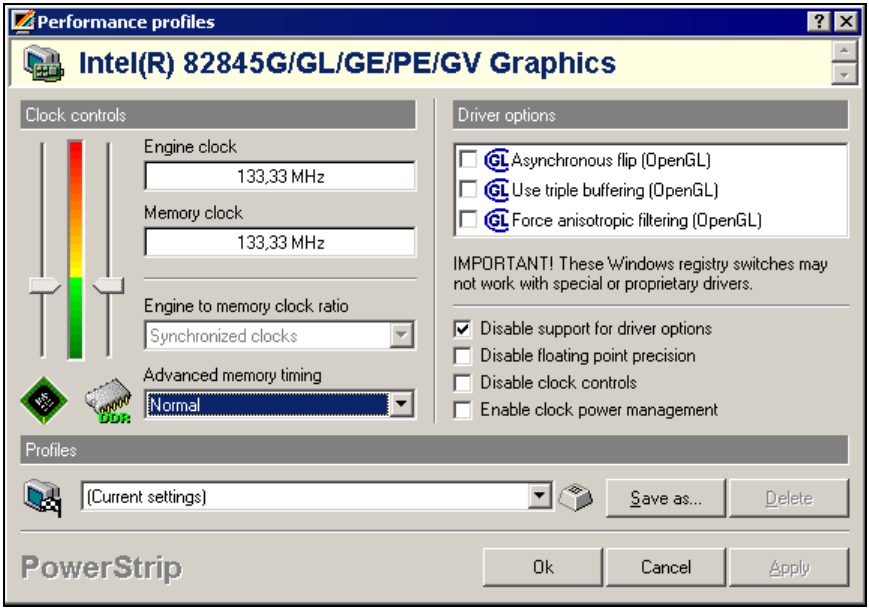


Рис. 4.14. Настройка скорости памяти и чипа

Помимо настройки скорости есть еще множество параметров и свойств, которые можно изменять. Я рекомендую ознакомиться с файлом помощи, чтобы больше узнать о доступных возможностях.

В Интернете есть еще много других программ для изменения производительности видеокарт, но они предназначены для конкретных марок устройств. Например, Radeon Tweaker (**http://radeontweaker.sourceforge.net/**) — программа для настройки видеокарт Radeon от фирмы ATI. Здесь достаточно простой интерфейс в стиле Linux, но небольшое количество настроек.

4.6. Оптимизация Windows

Даже после оптимизации BIOS и разгона железа ресурсов компьютера может не хватить для ОС Windows более новой версии. А ведь может случиться и так, что ресурсов не хватит и для старой, особенно, если ОС перегружена, в автозапуске находится пара десятков программ и сотня лишних сервисов. А у некоторых пользователей просто может возникнуть желание, чтобы компьютер работал еще быстрее. В этом случае стоит оптимизировать работу Windows, чтобы максимально форсировать работу этой ОС.

Большинство из принципов, которые мы будем рассматривать, являются базовыми и не зависят от ОС, т. е. такие же правила будут относиться не только к Windows-

системам. Так уж получилось, что именно окна — самая популярная ОС, и именно их мы рассматриваем в данной книге, но существуют и другие системы, о которых нельзя забывать.

4.6.1. Готовь сани летом

При долгом использовании Windows в ней набирается много мусора и скорость работы постепенно падает. Одним из источников медленной работы является фрагментация файлов. Если у вас винчестер объемом 120 Гбайт, и он не разделен на логические устройства, то ОС, программы и файлы будут находиться на одном диске. Каждый файл система может записать в любое свободное место, причем не обязательно единым куском. Таким образом, разброс может оказаться огромным. Начало файла может быть в самом конце диска, середина — в самом начале, а конец — в середине диска. Чтобы прочитать весь файл, головка диска совершает невероятные, долгие и бессмысленные путешествия.

К чему чаще всего происходит доступ? Конечно же, к системным файлам, и мы должны позаботиться о том, чтобы они компактно размещались на диске. Этого можно добиться регулярной дефрагментацией, но это большая нагрузка на жесткий диск, его пластины, головку, а кроме того, сильный нагрев, который однажды может закончиться фатально. Так что делать дефрагментацию каждую неделю не имеет смысла.

Есть еще один способ — создать диск C: в основном разделе объемом в 25 Гбайт и установить систему на него. Остальное пространство отвести под логический диск D:, и все программы и данные записывать уже туда. Таким образом, системные файлы будут гулять уже в пределах 25 Гбайт, а не по всему диску. Тут и дефрагментация отнимет не так уж много времени, да и надобность в ней будет возникать значительно реже. Хотя нет, 25 Гбайт — это, наверное, мало, для современной Windows нужно 30 Гбайт. А если вы забываете при установке программ менять путь установки, то придется выделить все 40 Гбайт. Но для современных компьютеров это абсолютно не проблема.

Слишком маленький объем тоже является отрицательной чертой. В этом случае удалять старое приходится чаще, чтобы поместить что-то новое, и диск начинает фрагментироваться с большей скоростью. Каждое удаление файла образовывает пустоту на диске (как дырку в сыре), и при записи нового файла система заполняет эту дыру, а если файл не помещается, то дыру заполняет только часть, а остальное улетает в другое место диска.

Если у вас свободного пространства на диске не более 10 Гбайт, то лучше купить жесткий диск большего объема или просто убрать с компьютера все лишнее на внешние носители. Чем больше свободного места на диске, тем больше будут пустоты и больше вероятность того, что данные файлов будут располагаться более компактно.

Диск с данными пускай фрагментируется сколько угодно, но по мере необходимости, чтобы не сильно перегружать диск и он не увидел над головой белых ангелов или красных чертиков :).

Так как ОС находится на отдельном диске, ее можно дефрагментировать один раз, когда вы завершили настройку системы и установили все необходимые программы. После этого система изменяется не так часто, и, значит, не нужно будет думать о системном диске. Максимум, что будет подлежать регулярному изменению — это папка временных файлов, особенно браузера. Но там файлы не такого большого размера, и ее проще иногда чистить, чем дефрагментировать. Лично я раз в полгода удаляю все временные файлы вручную, чтобы очистить кэш браузера и ОС от мусора. Для этого нужно очистить следующие папки:

- c:\Windows\Temp — это папка, где ОС и программы создают временные файлы. Там же часто создают временные файлы и программы установки. Только они не всегда за собой убирают, надеясь, что ОС будет чистить все сама. Она-то, может быть, и чистит, но вот сейчас я заглянул в свою папку, а там 170 Мбайт временных файлов;
- C:\Users*XXXXX*\AppData\Local\Temp\, где *XXXXX* — это ваше имя пользователя. Папка AppData может быть невидимой, но вы можете вручную ввести имя папки в строке Windows Explorer (Проводник). У меня на данный момент в этой папке оказалось аж 11 Гбайт мусора;
- C:\Users*XXXXX*\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ — временные файлы браузера.

Временные папки на данный момент являются, наверное, основным рассадником вирусов. Дело в том, что в эти папки может писать кто угодно и что угодно. Как раз во время перечисления временных папок я заглядывал в свои временные папки, чтобы посмотреть что в них и какой размер. Когда я заглянул в C:\Users*XXXXX*\AppData\Local\Temp\, то в правом нижнем углу выплыло окошко Microsoft Security Essential и сообщило мне, что среди временных файлов есть вирус, который можно удалить.

Давно я не видел этого окошка, и подозреваю, что вирус лежал не активным, иначе антивирусник заметил бы его в памяти уже давно (я надеюсь). Полное сканирование я не делал уже, наверное, год и в эту папку не заглядывал, поэтому исполняемый файл вируса просто лежал и ждал, когда его кто-то запустит. Так как ОС его запускать сама не будет (с чего бы это ей), то у вируса была единственная надежда на меня. Но я тоже не собираюсь этого делать.

Никогда не запускайте никаких исполняемых файлов из временной папки. Даже если имя исполняемого файла вам знакомо и значок выглядит заманчиво, не стоит поддаваться соблазну. Вирусописатель может назвать исполняемый файл как угодно, в том числе и winword.exe, и даже стащить значок у MS Word. Только вот во временной папке нормальным программам делать нечего.

Чтобы проще было чистить компьютер от мусора и не путешествовать по всем возможным папкам, можно просто воспользоваться утилитой очистки, которая входит в ОС. Зайдите в окно **Компьютер** на своем компьютере и щелкните правой кнопкой по значку системного диска (именно там располагается большинство мусора по умолчанию) и выберите пункт меню **Свойства** (Properties). Перед вами откроется окно свойств (рис. 4.15).

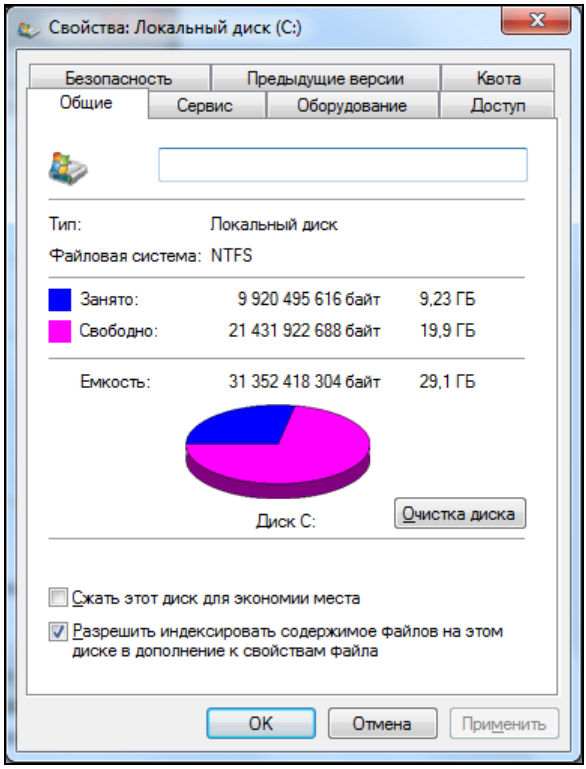


Рис. 4.15. Свойства системного диска

Примерно в центре окна должна быть кнопка **Очистка диска** (Disk Cleanup). Нажмите эту кнопку и не спешите ожидать результат. В зависимости от количества мусора в системе сбор информации о временных файлах может занять несколько минут. Я последний раз чистил полгода назад, и ждать пришлось пару минут как минимум.

Когда сбор данных завершится, перед вами должно появиться окно стандартной программы очистки диска (рис. 4.16). Она простая и для простых действий, как очистка временных папок, вполне пригодна.

Но мусор собирается не только во временных файлах. Он так же собирается и в базе данных реестра, который так же начинает затормаживать. Вот тут хороших утилит для чистки реестра в составе Windows нет.

Системный реестр — это большая база данных, в которой программы могут сохранять свои настройки. Идея (на мой взгляд) отличная и работает вполне хорошо. Только вот программисты далеко не всегда используют ее аккуратно, да и сама компания Microsoft не помогает.

Когда программа устанавливается в систему, то ее очень часто копирует отдельная программа установки, и сейчас очень популярным стал поставляемый с Visual Studio установщик от Microsoft. Он устанавливает все необходимые компоненты, но при удалении программы не удаляет все, а иногда просто не может удалять все.

Особенно это касается разделяемых библиотек, которыми может пользоваться более чем одна программа. Так мусор накапливается в базе данных реестра, и через год или два проще установить ОС заново, чем пытаться вычистить весь мусор.

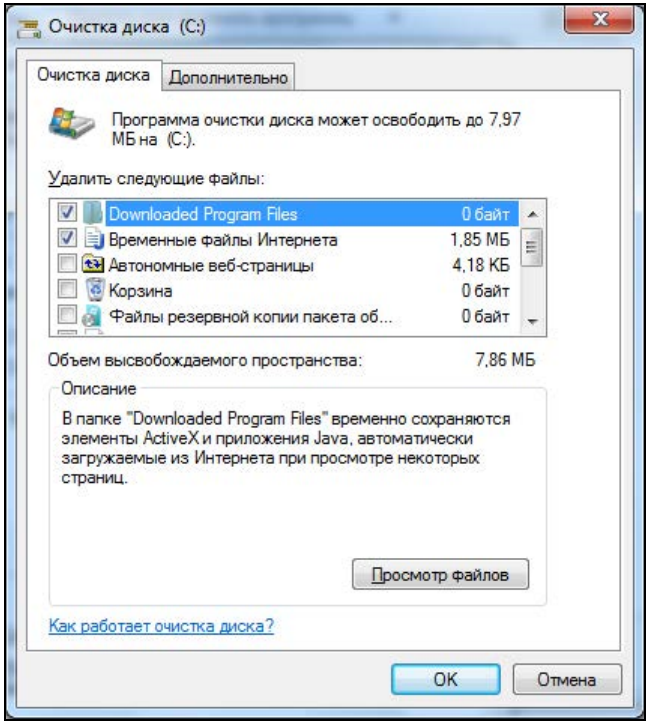


Рис. 4.16. Стандартная программа очистки диска

4.6.2. Службы Windows

Любая современная операционная система включает в себя очень много возможностей. ОС Windows в этом смысле одна из самых лучших, и в ней есть много полезного, но при этом достаточно часто практически ненужного рядовому пользователю. Начиная с Windows 2000, все основные функции реализованы в виде служб, и теперь нам легко управлять ими и выбирать только необходимые.

При оптимизации ОС я рекомендую первым делом обратить внимание на службы, которые запускаются по умолчанию. Мы уже говорили о службах при рассмотрении темы вирусов *(см. разд. 4.1.4)*, а сейчас взглянем на них с другой стороны. Каждый из них отнимает время при загрузке и тратит драгоценную память.

Запустите оснастку служб **Пуск | Настройка | Панель управления | Администрирование | Службы** (Start | Control Panel | Administrative tools | Services). Перед вами откроется окно управления установленными службами (см. рис. 4.6).

В последних версиях Windows это окно стало проще. Внизу вы можете заметить две вкладки: **Расширенный** (Extended) и **Стандартный** (Standard). В первом ре-

жиме откроется панель с описанием выделенной службы. В стандартном режиме выводится только общий.

Выделяя любую службу, вы можете ее запустить, остановить, приостановить или перезапустить с помощью соответствующих кнопок на панели или меню **Действие** (Action). Чтобы настроить какую-либо службу, нужно дважды щелкнуть по ней, и перед вами откроется окно настроек, как на рис. 4.7.

На вкладке **Общие** (General) окна настроек служб вы можете увидеть такие параметры как: **Тип запуска** (Startup type) и **Параметры запуска** (Start parameters). Раскрывающийся список **Тип запуска** (Startup type) может содержать одно из следующих значений.

- **Автоматически** (Automatic) — служба запускается при старте системы. После этого вы можете ее остановить вручную или оставить в запущенном состоянии. Такой статус должны иметь только постоянно необходимые службы.
- **Автоматически, отложенный запуск** (Automatic (Delayed Start)) — этот пункт относительно новый и позволяет запускать службу, когда ОС уже полностью загружена. Пользователь уже может работать с системой, а ОС будет продолжать подгружать нужные сервисы. Очень полезная опция для повышения скорости загрузки компьютера, нужно просто знать, какие службы критичны и должны стартовать сразу, а какие можно отложить на потом. Например, загрузку антивируса лучше не откладывать.
- **Вручную** (Manual) — служба запускается вручную из оснастки или из командной строки. Если вы чем-то пользуетесь очень редко, то лучше выбрать этот режим. Например, вы установили сервер баз данных MS SQL Server для выполнения определенной задачи. После этого удалять сервер жалко (может, еще пригодится), а держать в загруженном состоянии неэффективно, потому что это тормозит систему и отнимает память. В таком случае лучше запускать сервер только по мере необходимости вручную.
- **Отключена** (Disabled) — служба отключена, и ее невозможно запустить никакими методами. Если есть служба, которую вы не используете в целях безопасности, то отключите ее. Это автоматически наложит запрет на запуск всех связанных с ней служб. Например, если отключить базовый сервис сети, то ни одна сетевая служба не заработает.

На вкладке **Зависимости** (Dependencies) вы можете определить взаимосвязи служб. В верхнем списке перечислены компоненты, от которых зависит избранный сервис. Это значит, что при отключении любого из них выбранная служба больше не запустится. Так что для обеспечения надежности работы какой-либо службы нужно запустить все, от чего она зависит.

В нижнем списке вы можете увидеть компоненты, которые зависят от выбранной службы. Если вы решили что-либо отключить, то прежде, чем это делать, семь раз загляните в этот перечень, иначе можете остановить очень полезную службу.

Теперь рассмотрим некоторые службы, установленные на вашем компьютере, которые можно или даже нужно отключить, во-первых, от греха подальше и, во-вторых, для повышения производительности системы:

- **Автоматическое обновление** (Automatic Updates) — при включении этой службы компьютер имеет право автоматически загружать обновления ОС Windows по сети. Если вы жалеете свой трафик и не хотите качать всякую ерунду, то переключите эту службу в ручной режим, чтобы запускать ее по мере необходимости, освобождая тем самым ресурсы. При этом выполните отключение автоматического обновления. Для этого зайдите в Центр обновления Windows. В открывшемся окне щелкните по ссылке **Настройка параметров** слева. В раскрывающемся списке важные обновления выберите вариант **Не проверять наличие обновлений**. Если этого не сделать, то при очередной попытке обновления произойдет ошибка, потому что не запущена служба. Ради скорости можно отключить службу, но ради безопасности не стоит забывать самостоятельно качать критические обновления.
- **Диспетчер очереди печати** (Print Spooler) — обслуживает очередь печати. Даже при наличии принтера при определенных настройках можно работать без этой службы. Ну а если таковой отсутствует, то перевести службу в ручной режим — святое дело. Я, например, очень редко печатаю со своего ноутбука, и держать в загруженном состоянии этот сервис — бессмысленное расходование ресурсов.
- **Планировщик заданий** (Task Scheduler) — запускает определенные задания по расписанию. Лично я никогда не заставлял ОС выполнять свою работу. Некоторые любят, чтобы каждый день в определенное время запускалась дефрагментация диска. Но представьте себе, что вы в это время убиваете очередного монстра в новом 3D Action, а тут вам такие тормоза. Чрезмерно частое использование дефрагментатора — вообще глупое занятие (лишняя нагрузка на винчестер, перегревы и т. д., *см. разд. 4.6.1*), а выполнение по заданию — еще хуже. Достаточно вручную выполнять эту операцию по мере необходимости. Так что забудьте про планировщик и освободите компьютер от лишней службы.
- **Служба серийных номеров переносных устройств мультимедиа** (Portable media serial number) — получает серийные номера всех медиа-устройств, подключенных к системе. А оно вам надо? Тогда переводите запуск службы в ручной режим.
- **DHCP-клиент** (DHCP Client) — служит для динамического получения IP-адреса от DHCP-сервера. Если у вас IP-адрес статический (прописан явно), то в этой службе нет надобности, и стоит сделать ручной запуск. Отключать совсем я не рекомендую.
- **DNS-клиент** (DNS Client) — определяет IP-адреса компьютера по его имени. Если в вашей сети используются домены, то этот клиент необходим, иначе можно перевести в ручной режим запуска. На преобразование имен интернет-сайтов данная служба не влияет.
- **Смарт-карта** (Smart card) — позволяет работать со смарт-картами. Для использования смарт-карты (устройство для хранения ключей, паролей и т. д.) необходим присоединенный к компьютеру специальный считыватель. Если у вас нет устройства чтения смарт-карт, то службу лучше перевести в ручной запуск.

- **Служба терминалов** (Terminal Service) — применяется для того, чтобы другие компьютеры работали по сети с вашим рабочим столом. Для этого необходимы сервер и клиент службы терминалов. Такая возможность часто используется в фирмах, где администраторы удаленно управляют другими машинами, или для работы с "тонкими" клиентами, но в домашних условиях это лишнее. Именно поэтому этот сервис по умолчанию отключен, и если вам не нужен терминальный доступ, то оставьте все, как есть.
- **Удаленный реестр** (Remote Registry) — позволяет изменять параметры реестра по сети. Самое интересное, что она еще и работает по умолчанию. Так что срочно переводите в ручной режим запуска, чтобы реестр вашего компьютера можно было править только локально.
- **Служба FTP-публикаций** (FTP Publishing Service) — необходима в автозапуске только в том случае, если вы хотите использовать свой компьютер в качестве FTP-сервера. Тогда другие пользователи сети смогут с помощью FTP-клиентов подключаться к вашему компьютеру и обмениваться файлами. По умолчанию служба в некоторых версиях ОС Windows не устанавливается (подробней о установке/удалении служб *см. разд. 4.6.3*).
- **Служба IIS Admin** (IIS Admin Service) — используется для управления веб-сервером, входящим в состав некоторых версий Windows. Если вы не планируете использовать свой компьютер для публикаций FTP или веб-страничек, то отключите этот сервис. По умолчанию служба в некоторых версиях ОС Windows не устанавливается (подробнее об установке/удалении служб *см. разд. 4.6.3*).
- **Темы** (Themes) — позволяет управлять темами Windows XP. Если вы предпочитаете классический вид рабочего стола, то сервис зря отнимает память, и его нужно отключить.
- **Telnet** — позволяет удаленному пользователю с помощью командной строки войти на ваш компьютер и запускать программы. Обязательно отключите его. На 99% компьютеров эта служба не используется, и незачем давать возможность злоумышленнику получить доступ к вашей системе. Если когда-нибудь эта возможность понадобится, то запустите Telnet вручную.
- **Служба RunAs** (RunAs) — позволяет запускать приложения от имени другого пользователя. Вероятно, вам это не нужно, так что ее можно отключить.
- **Сервер папки обмена** (ClipBook) — позволяет просматривать страницы папок обмена других компьютеров. Поставьте ручной запуск, потому что такие папки даже в сетях используются редко.
- **Служба факсов** (Fax service) — предназначена для отправки и получения факсов с помощью встроенного факс-модема. Если вы добавили возможность работы с факсом (при инсталляции Windows служба не устанавливается по умолчанию), но пользуетесь им редко, то стоит использовать ручной запуск.
- **Клиент отслеживания изменившихся связей** (Distributed Link Tracking Client/Server) — поддерживает связи NTFS-файлов, перемещаемых в пределах

компьютера или между компьютерами в домене. При локальной работе этот параметр точно должен быть установлен в положение **Вручную** (Manual), но даже если присутствует сеть, я его отключаю.

- **Координатор распределенных транзакций** (Distributed Transaction Coordinator) — позволяет использовать распределенные транзакции для доступа к базам данных, очередям сообщений или файловым системам. Я отключаю эту службу, когда не работаю с базами данных.
- **Диспетчер логических дисков** (Logical disk manager) — осуществляет мониторинг за новыми жесткими дисками. Состояние динамических дисков и информация о конфигурации изменяются не так часто, чтобы их постоянно отслеживать, поэтому переведите службу в ручной режим запуска, но не отключайте совсем.

Как видите, в системе много служб, которые могут понапрасну расходовать ресурсы на вашем компьютере. Если отключить их, то загрузка ОС ускорится и освободится несколько мегабайт свободной памяти.

4.6.3. Удаление ненужного

Один из лучших вариантов оптимизации работы Windows — избавиться от лишних программ. Вспомните об оснастке **Программы и компоненты** (Programs and Features) и удалите неиспользуемые компоненты Windows и сторонние программы. Для этого щелкните по ссылке **Включение или отключение компонентов Windows** (Windows features on or off) и перед вами откроется окно с перечислением всех доступных разделов. Посмотрим назначение каждого из них и определим, что из этого нужно, а что — нет.

- **Internet Information Services (IIS)** — компонент, обеспечивающий поддержку веб- и FTP-серверов на своем компьютере. Чаще всего этим сервисом пользуются программисты для отладки своих веб-приложений и администраторы сети на сервере для создания корпоративного сайта. Если вы далеки от этих проблем, то можете отключить сразу весь раздел, а если заинтересовались, то вот его содержимое:
  - **Служба FTP** (File Transfer Protocol (FTP) Service) — служба, которая обеспечивает создание FTP-узлов, предназначенных для передачи файлов по сети, и дает возможность обновлять локальный веб-сайт другим удаленным пользователям. Это лишняя дыра в безопасности, потому что вы и так сможете поменять файлы на своем диске, а для пользователей локальной сети можно открыть общую папку. Сервер FTP — более сложная программа со своими правами доступа, которая удобна в разнородных сетях;
  - **Служба WWW** (World Wide Web Service) — непосредственно сервер, который будет управлять страничками и может быть установлен локально;
  - **Оснастка IIS** (Internet Information Management) — утилита, которая позволяет администрировать сервер IIS через обозреватель;

- **Документация** (Documentation) — материалы о публикации содержимого узла и администрировании веб- и FTP-серверов. Компонент на первый взгляд не несет угрозы, но при его включении устанавливаются сценарии ASP, через которые просматривается документация, а любые сценарии могут быть уязвимы. Я сам их не проверял, но думаю, другие проверяли качество кода, и ошибок там не должно быть, но все же, оно вам нужно?
- **Служба SMTP** (SMTP Service) — служба, позволяющая передавать сообщения электронной почты с вашего компьютера, в том числе и пользователям с других компьютеров, а также получать рассылки/новости, которые в последнее время потеряли свою актуальность. Устанавливать SMTP-службу не стоит, если вы не собираетесь ее использовать. Если сомневаетесь, то тоже не ставьте, в случае необходимости это можно сделать в любой момент.

- **Print and Document Services** (Другие службы доступа к файлам и принтерам в сети) — по умолчанию устанавливается только служба, которая позволяет работать с ресурсами Windows-систем. В этом разделе вы можете подключить дополнительные службы, которые позволяют Macintosh- и UNIX-клиентам печатать документы на любом доступном принтере.
- **Сетевые службы** (Networking Services) — набор специализированных служб и протоколов для работы с сетью, большинство из них используется только на сервере и для клиентского компьютера не нужны:
  - **DHCP** (Dynamic Host Configuration Protocol, протокол динамической конфигурации хоста) — устанавливает DHCP-сервер, который автоматически назначает временные IP-адреса клиентским компьютерам. Используется в больших сетях для облегчения администрирования адресации;
  - **DNS** (Domain Name System, служба имен доменов) — сервер преобразования DNS-имен (не путать с именами компьютеров) в IP-адреса;
  - **WINS** (Windows Internet Naming Service, служба имен Интернета для Windows) — сервер NetBIOS-имен, позволяющий их регистрировать. Это как раз и есть имена компьютеров;
  - **Простые службы TCP/IP** (Simple TCP/IP Services) — поддержка таких служб TCP/IP (Transmission Control Protocol/Internet Protocol, протокол управления передачей/протокол Интернета), как Character Generator, Daytime, Echo и т. д. В большинстве случаев они не нужны даже на сервере;
  - **Служба контроля допуска QoS** (QoS Admission Control) — контроль QoS (Quality of Service, качество предоставляемых услуг передачи данных). Эту службу обязательно нужно отключить, потому что она отнимает от каждого соединения часть пропускной способности, что тормозит связь. При этом подавляющее большинство программ ее не использует.
- **Служба индексирования** (Indexing Service) — набор программ, которые позволяют производить быстрый поиск в файлах. Занимает много лишнего места на диске, так что если вы редко пользуетесь поисковой системой Windows, нужды в ней нет.

- **Службы Windows Media** (Media Features) — компонент, который обеспечивает потоковую передачу файлов мультимедиа по сети. Если вы не занимаетесь вещанием звука или видео, то не стоит его устанавливать.
- **Simple Network Management Protocol (SNMP)** — протокол SNMP (Simple Network Management Protocol, простой протокол сетевого управления), используется для наблюдения за работой сетевых устройств и позволяет выводить результаты обработки на рабочую станцию сетевой консоли.
- **Игры** (Games) — стандартные игры Windows, такие как "Сапер" или "Косынка".
- **Telnet Server** — программа Telnet-сервер, которая предназначена для организации удаленного администрирования компьютером с помощью утилиты, схожей с командной строкой (Telnet-клиент). Далеко не всегда нужно делать так, чтобы ваш компьютер был доступен для удаленного администрирования. В домашних условиях, я бы сказал, это вообще не нужно. Не вижу смысла устанавливать этот компонент.
- **Telnet client** — вот это как раз утилита, с помощью которой и подключаются к Telnet-серверу. Не знаю, почему эти два пункта не объединили в одну группу. Но то, что их ставят отдельно, имеет смысл. Ведь если вы не хотите, чтобы вашим компьютером управляли, вам может понадобиться возможность управлять другими компьютерами через Telnet.
- **Windows Gadget Platform** — новая "фишка" Windows, которая позволяет отображать гаджеты на рабочем столе.
- **Windows Virtual PC** — установив этот компонент, а точнее, целую программу, вы сможете запускать виртуальные компьютеры внутри ОС Windows. Приятно, что этот компонент стал доступен в ОС, ведь это бесплатно. Раньше эта технология стоила больших денег, если ставить отдельные программы. А сейчас достаточно включить этот компонент.

В зависимости от версии Windows, у вас может быть несколько иной набор компонентов, или они могут быть иначе организованы. Описанная здесь структура имеет место в Windows 7. Большинство из описанного в равной степени относится и к Windows XP/Vista, потому что в сервисах происходит не так много изменений. Чаще всего добавляются новые сервисы и оптимизируются старые.

Не все из перечисленных программ влияют на производительность компьютера. Это и логично, ведь как может повлиять на производительность игра? Скорость работы процессора не зависит от количества игр на жестком диске. От этого может зависеть только ваша производительность, если вы очень много времени тратите на игры, а не на работу.

Лишнюю нагрузку на процессор дают только работающие фоновые процессы, запускаемые во время загрузки ОС. Все они съедают драгоценные такты, которые могли бы пойти на более важные расчеты.

Но список, который вы видите в рамках оснастки **Программы и компоненты** (Programs and Features), еще не полный. Очень многие программа скрыты от удаления. Чтобы их увидеть, необходимо отредактировать файл sysoc.inf из папки \Windows\Inf.

В этом файле после строки `[Components]` идет описание всех установленных компонентов, например, так:

```
WBEM=ocgen.dll,OcEntry,wbemoc.inf,hide,7
```

Обратите внимание на параметр `hide` перед последней запятой. Благодаря ему мы не видим данный компонент и не можем его удалить. Чтобы программа отображалась в списке, необходимо просто удалить это слово, тогда строка примет следующий вид:

```
WBEM=ocgen.dll,OcEntry,wbemoc.inf,,7
```

Уберите слово `hide` во всех строчках, и все компоненты станут доступными для удаления.

4.6.4. Автозагрузка

Помимо сервисов автоматически могут запускаться и другие программы, и все они отнимают лишние ресурсы. Нажмите кнопку **Пуск** (Start), в строке поиска введите команду `msconfig` и нажмите клавишу <Enter>. Перед вами откроется окно настройки системы (см. рис. 4.3). Мы уже рассматривали эту утилиту, когда затрагивали тему вирусов *(см. разд. 4.1.4)*. Перейдите на вкладку **Автозагрузка** (Startup), где перечислены все автоматически запускаемые программы. Убедитесь, что в перечне находятся только те программы, которые вы используете достаточно часто.

Например, если у вас установлен Microsoft Office, то в этом списке будет утилита, позволяющая запускать офисные программы быстрее. Это происходит за счет загрузки определенных библиотек на этапе старта компьютера, и при запуске самих приложений уже не будет этих затрат. Очень хорошо. Но что, если ваш компьютер используется в основном для игр и только иногда для написания какого-то реферата? В этом случае мы будем при каждом старте зря терять ресурсы — время на загрузку лишнего кода и память для его хранения. Лучше отключить эту утилиту и освободить память, и пусть, например, Microsoft Word грузится на секунду дольше.

4.6.5. Дамп памяти

Что еще можно улучшить? При системном сбое по умолчанию до перезагрузки системы создается дамп памяти. Это значит, что ОС сохраняет на диске (в отдельном файле) все содержимое оперативной памяти. Данное действие необходимо разработчикам, чтобы определить причину ошибки, но мы же не программисты и исследовать байт-код самой ОС не будем. Поэтому я рекомендую не тратить время (достаточно большое) на создание файла-дампа и сэкономить место на диске, т. е. отключить эту возможность.

Для этого щелкните правой кнопкой мыши по строке **Компьютер** (Computer) в главном меню ОС и в появившемся контекстном меню выберите пункт **Свойства** (Properties). Перед вами откроется окно свойств системы. Перейдите на вкладку **Дополнительно** (Advanced) и нажмите кнопку **Параметры** (Settings) в разделе **Загрузка и восстановление** (Startup and Recovery). В появившемся окне (рис. 4.17)

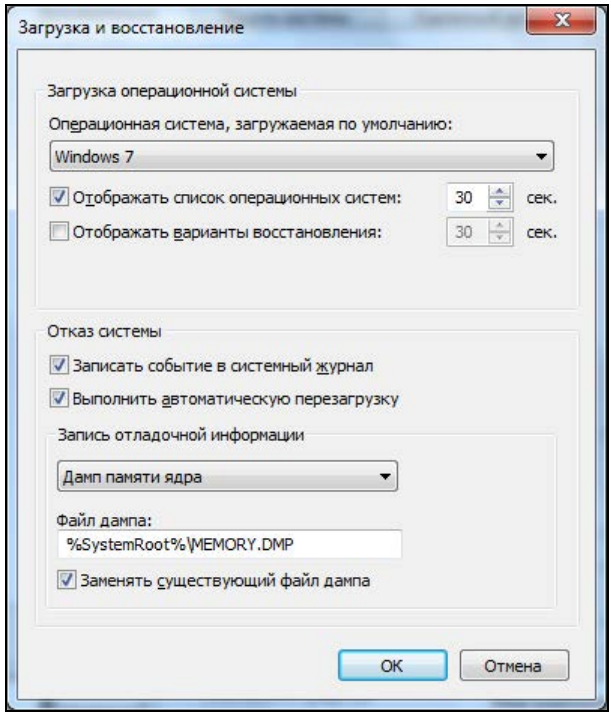


Рис. 4.17. Окно настройки загрузки и восстановления

в области **Запись отладочной информации** (Write debugging information) выберите пункт **отсутствует** (**(none)**).

4.6.6. Красоты

Когда мы устанавливаем новую версию ОС, то хочется увидеть всю ее красоту и почувствовать комфортабельность (как у любимого автомобиля), но симпатичный внешний вид — это не всегда удобство и скорость. Для повышения производительности иногда приходится жертвовать красотами, если ваш компьютер изначально не справляется с операционной системой.

Для отключения лишних эффектов снова щелкните правой кнопкой мыши по строке **Компьютер** (Computer) в главном меню Windows и в появившемся контекстном меню выберите пункт **Свойства** (Properties). В уже знакомом окне свойств системы перейдите на вкладку **Дополнительно** (Advanced) и нажмите кнопку **Параметры** (Settings) в разделе **Производительность** (Performance). Если у вас Windows 7, то перед вами откроется окно, как на рис. 4.18. Это окно не сильно изменилось по сравнению с предыдущими версиями ОС, просто добавились новые эффекты. Отметьте переключатель **Обеспечить наилучшее быстродействие** (Adjust for best performance). В списке эффектов будут сняты флажки со всех пунктов.

Таким образом, мы отказываемся от визуальных эффектов, зато позволяем компьютеру работать, не теряя эффективности.

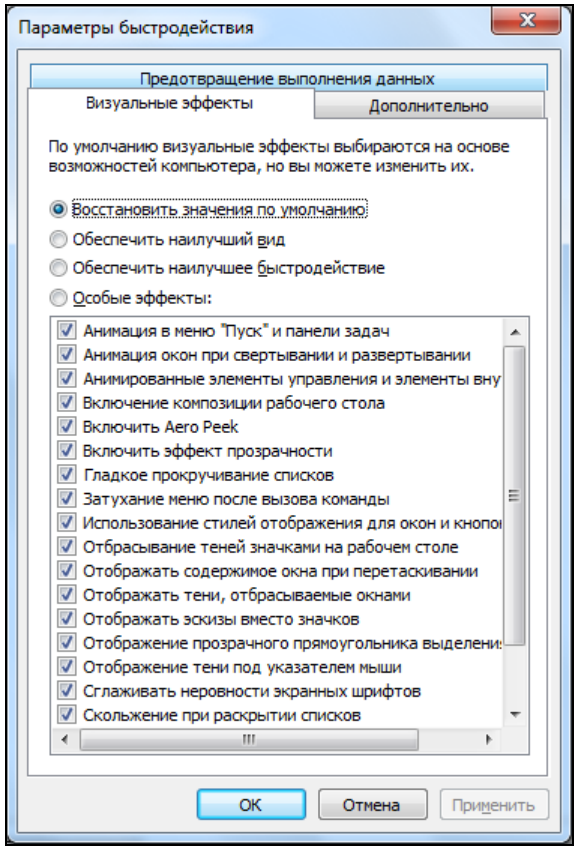


Рис. 4.18. Окно настройки производительности

Прорисовка рабочего стола тоже отнимает время. Допустим, что у вас работает несколько тяжеловесных программ, отнимающих много памяти, и нужно запустить еще одну. Для этого щелкаем по значку **Свернуть все окна** (Show Desktop) и видим, как долго ОС перерисовывает рабочий стол. Это особенно заметно, если в системе не хватает памяти или выполняется какой-нибудь ресурсоемкий процесс. На прорисовку картинки рабочего стола просто не остается сил. Наилучшее ускорение — вообще не использовать фон, а установить простой цвет заливки.

В *главе 1* мы говорили о том, что смотреть на "голый" рабочий стол не очень приятно, и какие-то красоты должны присутствовать в системе. Но фон нужно подбирать тщательным образом, дабы он прорисовывался быстрее. Если вы работаете с разрешением 1024×768, а фоновая картинка имеет размер 800×600, то система должна растягивать ее на всю поверхность экрана. Хотя растянутый вариант кэшируется ОС и на скорости это сказывается не сильно, но на качество картинки может повлиять значительно. Более удачным по производительности вариантом будет использование рисунка такого же размера, что и экран.

4.6.7. Лишние копии

В Windows, начиная с 2000/XP (Server/Home Edition), появилось очень много средств для упрощения жизни пользователя. Например, при инсталляции ОС все драйверы копируются на жесткий диск. Это удобно, потому что сразу после установки оказывается, что не все устройства были опознаны, а некоторые вообще могли быть еще не подключены (принтеры, сканеры, съемные носители и т. д.). Раньше приходилось каждый раз вставлять CD с дистрибутивом, а теперь при первом же подключении система сама находит драйвер в кэше на диске и устанавливает его.

Все это хорошо, если у вас винчестер на 150 Гбайт. А если только 30 Гбайт, как у меня, и со временем места начинает категорически не хватать? Нужно очистить кэш драйверов, тем более что он занимает очень много места, хотя производительность от этого не увеличивается.

Итак, когда Windows отработал какое-то время, и все необходимые драйверы установлены, кэш можно очистить. Если что-то понадобится, можно в любой момент воспользоваться дистрибутивом. Кэш драйверов находится в двух папках:

- \Windows\Driver Cache\i386 — здесь находятся самые распространенные драйверы, и занимают они более 70 Мбайт. Основной и самый объемный файл в этом каталоге — driver.cab (архив драйверов);
- \Windows\system32\dllcache — в большинстве своем это распакованный driver.cab из директории \Windows\Driver Cache\i386. Если архив еще можно оставить, то разархивированная версия абсолютно не нужна, потому что может достигать 500 Мбайт.

Прежде чем удалять файлы, лучше всего установить файловый кэш равным 0. Для этого выполните команду:

```
sfc /cachesize=0
```

Если вы уже достаточно опытный пользователь и не помните, когда последний раз обращались к справочной системе, то можно удалить файлы помощи. Они тоже занимают немало места (более 30 Мбайт), а информации несут в себе мало. Проще найти поддержку в Интернете через поисковик. У меня вообще иногда складывается ощущение, что даже начинающие пользователи не пользуются файлами справки и первым делом идут на форумы за помощью.

Я пытался найти что-нибудь полезное в файлах помощи Windows (помню, у меня была какая-то проблема с сетью лет пять назад, и я решил воспользоваться файлом помощи), но ничего путевого не нашел. Большинство советов при решении проблем заключается в том, чтобы проверить кабели и включено ли питание. Ну просто гениальная помощь.

На каждом диске в скрытой папке System Volume Information есть файл, в котором сохраняются точки восстановления. Что это значит? Регулярно, при установке неподписанных драйверов система устанавливает точку восстановления. Если что-то пойдет не так, то ОС можно откатить к предыдущему состоянию. Это достаточно мощное нововведение в Windows XP, но меня оно спасало только один раз. По-

следние версии Windows от Microsoft достаточно надежны, и если она рушится, то чаще всего навсегда. У меня три компьютера дома и с тех пор, как я перешел на Windows Vista, мне только один раз пришлось откатить систему на компьютере детей с Windows 7.

Во время настройки ОС (сразу после установки) такие опорные точки нужны. Но когда система сконфигурирована и удачно работает, вероятность ее сбоя уменьшается практически до нуля. Точки восстановления занимают достаточно много места, и чтобы освободить его, можно вручную очистить папки System Volume Information на каждом диске, но лучше воспользоваться оснасткой **Восстановление системы** (System recovery), в которой можно не только самостоятельно создавать, но и удалять точки восстановления. Но советую все же иметь одну опорную точку, чтобы можно было откатиться к этому состоянию.

Приняв все меры предосторожности, отключим автоматическое создание точек восстановления. Для этого щелкните правой кнопкой мыши по строке **Компьютер** (Computer) и выберите в появившемся меню пункт **Свойства** (Properties). В открывшемся окне перейдите по ссылке **Защита системы** (System Protection) слева и сбросьте флажки со всех дисков в группе **Автоматические точки восстановления** (Automatic restore points). Теперь создание точек восстановления полностью ложится на вас.

4.6.8. Форсирование выключения

При выключении локального компьютера может возникнуть ситуация, когда какая-либо программа не хочет выгружаться из памяти. В этом случае ОС долго и нудно (по умолчанию 20 секунд) дожидается завершения этого процесса. Чаще всего ждать бессмысленно, потому что это уже похоже на зависание.

Если на сервере продолжительное время невозможно остановить сервис, то задержка может оказаться полезной. Например, если в момент попытки выключить компьютер база данных обрабатывает долгий запрос, то ожидание будет вознаграждено, если запрос завершится корректно.

На домашнем компьютере очень редко бывают такие сервисы, а пользовательские программы, в основном, закрывают вручную до начала перезагрузки или выключения. Поэтому лучше уменьшить время ожидания. Для этого открываем в реестре строку **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control** и изменяем параметр `WaitToKillServiceTimeout` с `20000` на `5000` (т. е. 5 секунд). Для дома этого будет более чем достаточно.

4.7. Защита от вторжения

Мы уже познакомились с защитой от вирусов *(см. разд. 4.1)* и оптимизацией ОС Windows *(см. разд. 4.6)*. И то, и другое напрямую связано с безопасностью системы. Поэтому, не повторяясь, рассмотрим только связь этих действий между собой.

Даже выполнение предложенных мер не гарантирует полной безопасности. Все в мире меняется и развивается, поэтому желательно постоянно изучать что-то новое. Я связан с компьютерами уже около 20 лет, но постоянно читаю книги и различные руководства в Интернете.

Вы должны четко представлять себе, что настройки Windows не во всех случаях оптимальны. Правила защиты несовместимы с принципами производительности. Для обеспечения максимальной безопасности требуется множество проверок, шифрование, полный аудит и т. д. Все это отнимает ресурсы и во включенном состоянии тормозит систему так, что даже на самом мощном компьютере КПД (коэффициент полезного действия) может быть ниже 50%.

Прежде чем защищаться, нужно оценить: а действительно ли информация настолько важна? Если да, то нужно обозначить круг данных, которые наиболее значимы, и направить усилия на их защиту. Следует ранжировать данные по степени важности, а потом в зависимости от этого принимать решение и выполнять соответствующие действия. Но об этом мы поговорим чуть позже.

Лирическое отступление по поводу безопасности Windows... Многие ругают эту компанию за большое количество уязвимостей и за слишком ламерский интерфейс. Давайте сначала определимся со вторым — ламерством. А кто из нас не проходил через эту стадию? Благодаря ламерскому интерфейсу компьютеры стали настолько популярны и доступны всем — как говорится, и старикам, и младенцам.

Посмотрите на современные версии Linux — они такие же простые и так же стремятся к ламерству. Еще лет восемь-десять назад установить UNIX-подобную систему было достаточно сложно, и моя мама с этим не справилась бы, но это не значит, что она не должна иметь возможность работать или играть за компьютером. Благодаря Windows и ее простоте я могу жить в одном городе и общаться через Интернет со своими родителями за тысячи километров от меня, и если точнее, то на другом континенте. Несмотря на то, что я живу в Канаде, у меня много друзей в России, с которыми я общаюсь и работаю над одними и теми же проектами.

По поводу безопасности — UNIX-подобные системы также не без изъяна. В них тоже находят ошибки, особенно в конфигурации по умолчанию. Нет ничего идеального, но к этому нужно и можно стремиться постоянно (а не сидеть сложа руки и ждать, когда нам дадут что-то готовое), и только в этом случае можно чего-то добиться.

Посмотрим на Android, который построен на базе Linux и должен унаследовать всю надежность и безопасность открытых технологий. Он-то унаследовал, но из-за популярности ОС Android на мобильном рынке под него начали писать троянские программы, вирусы и различные шпионы.

Посмотрим на Apple, которая построила свою ОС на одной из самых безопасных систем — BSD. Родитель действительно безопасен, но он и не популярен. ОС от Apple развивается очень быстро и получила уже большую популярность, и для нее тоже стали появляться вирусы. Так что отсутствие злостных программ на данный момент не значит, что они не появятся в будущем, если ОС станет популярной.

Построение действительно безопасной системы потребует множества уровней защиты и сложных систем контроля. Все это требует больших денег. И вот тут возникает вполне логичный вопрос — а оно вам нужно? Информация на вашем компьютере стоит таких затрат? Мой компьютер защищен ровно настолько, насколько это мне необходимо, и до сегодняшнего дня этой защиты было достаточно.

Когда Microsoft создавала свою первую ОС Windows 95 (до этого был MS-DOS), то компания сделала ее персональной, наверно потому, что она работала на персональных компьютерах. Когда в ОС добавили сетевые возможности, то в компании просто не подумали, что при подключении компьютера к жестокому миру (а Интернет — отражение нашей реальности) нужно уделять больше внимания безопасности.

Microsoft создала удобную и простую ОС и постепенно начала двигаться в сторону безопасности, отлаживая свои программы. Видимо компании нужно было на методе собственных ошибок понять, что может угрожать компьютеру.

А вот теперь мы поговорим о различных угрозах, которые могут настигнуть ваш компьютер, и разберем различные методы борьбы с этими угрозами.

4.7.1. Вирусы и трояны

Все, что я говорил про защиту от вирусов, в равной степени относится и к троянским коням, шпионам и других зловредным программам, которые могут нанести ущерб информации или компьютеру.

Троян — это программа, которую чаще всего распространяют в письмах с заманчивым содержимым. На самом деле, большинство программ сейчас распространяют через почту, но троянские программы имеют более целенаправленный эффект на определенного пользователя, поэтому могут использовать слабости конкретного человека.

Если пользователь активизировал трояна (прикрепленный файл), то в системе появляется автоматически запускаемая программа, которая открывает черный ход для хакера. Трояны пытаются любыми способами попасть в автозагрузку компьютера, чтобы оставаться активными даже после перезагрузки системы. Через эту дверь хакер может получить доступ к компьютеру и управлять им. Бывают трояны, которые только ищут пароли и высылают их на определенный e-mail.

В отличие от вирусов, такие программы редко распространяются самостоятельно, в основном их рассылают целенаправленно для взлома определенной машины. Но бывают и такие экземпляры, которые наподобие вирусов распространяют себя, создавая для злоумышленника целые сети из зараженных машин.

Если выполнять все правила защиты от вирусов, то вы так же уменьшаете вероятность заразиться трояном. Большинство антивирусных программ сканирует диск не только на вирусы, но и на трояны. Это тоже говорит о сходстве этих двух видов бациллоносителей.

4.7.2. Оптимизация

Что касается оптимизации, то в *разд. 4.6* мы очень подробно говорили об объектах, на которые надо направить свои действия (автоматически запускаемые и редко используемые компоненты). Программы содержат погрешности, потому что их пишут люди, а людям свойственно ошибаться. Если хакер найдет ляпсус в какой-либо программе, запущенной на вашем компьютере, то он сможет проникнуть в систему или сделать еще что-то не очень хорошее. Именно поэтому вы должны запускать только те программы или сервисы, которые необходимы, особенно при работе в сети.

Получается, что оптимизация тоже может хорошо сказываться на безопасности. Но это далеко не всегда так. Чаще всего ради экономии ресурсов пользователи отключают антивирусы или сетевые экраны. Иногда это возможно, но лучше все же оставлять антивирусы включенными.

4.7.3. Сложные пароли

Все специалисты по компьютерной безопасности в один голос просят пользователей делать сложные пароли, но мало кто следует этим рекомендациям. Нельзя использовать в качестве пароля имена, читаемые слова или даты рождения. Такие комбинации легко взламываются простым перебором по словарю, и если он хорошо составлен, то процедура не отнимет много времени.

При создании пароля желательно генерировать случайные комбинации, в которых будут присутствовать строчные и прописные буквы, а также цифры и различные допустимые символы. Длина пароля должна быть не менее 8 символов, а лучше — более 12. Тогда для подбора хакеру нужно будет потратить намного больше времени.

С ростом производительности компьютеров увеличивается и скорость перебора, поэтому вполне возможно, что через пару лет будет мало и 16 символов.

Когда нужно придумать пароль, я запускаю какой-либо текстовый редактор (достаточно стандартного Блокнота (Notepad)) и случайным образом набираю на клавиатуре любые символы в разном регистре. Как теперь запомнить полученный шифр? А напрягаться и не надо. У меня для таких случаев есть одна страничка в OneNote, которая хранит пароли для всех интернет-сайтов. Достаточно только сохранить в нем пароль, предварительно написав краткий комментарий (для какого сайта или программы используется).

Хотя многие специалисты не рекомендуют хранить пароли в текстовом формате, я это делаю без проблем. На работе у меня нет OneNote, и там все хранится в файле. Главное — хорошо спрятать такой файл. Как это сделать? Читайте рекомендации, как прятать особо важные файлы, в *разд. 4.7.9*.

Единственное, что я могу порекомендовать — не хранить пароли в системе. Те, кто доверяются Windows и разрешают ей запоминать шифры и ключи, сильно рискуют. Защита, встроенная в ОС, достаточно надежна, но в этом случае хакеру заведомо

известно, где искать пароли (положение фиксировано), и при определенных условиях злоумышленник сможет украсть все пароли, особенно если в системе найдется подходящая уязвимость, и вы работаете от имени администратора.

Начиная с Windows 2000, пароли хранятся в базе данных учетных записей безопасности (Security Accounts Manager, SAM), и к этому файлу нельзя получить доступ. Но это мнимая защита, потому что формат этого файла ни для кого не секрет, и существуют атаки, которые ищут пароли в памяти компьютера или в файлах подкачки. К тому же, есть способы обхода защиты Windows и доступа даже к таким файлам. Программисты Microsoft латают свои ошибки, и сейчас уже намного сложнее получить доступ к этой базе данных.

Но не все так просто, даже получив доступ к файлу, пароли извлечь будет невозможно, потому что они зашифрованы необратимым шифром. Это самый большой шаг в сторону безопасности, сделанный еще в Windows 2000. Чтобы узнать, правильно ли введен пользователем пароль, его шифруют таким же необратимым алгоритмом и сравнивают результат с тем, что сохранен в базе. Если результат (его называют хэш) совпадает, то пароль верный.

В UNIX-системах используется схожий алгоритм, и там хэши хранятся вообще в открытом виде, доступном для суперпользователей. Но это не значит, что системы уязвимы. За счет необратимости алгоритма пароль можно узнать только перебором символов.

Когда впервые была внедрена практика использования необратимого шифрования, она казалась очень надежной, потому что требовала только полного перебора, который может занять месяцы (зависит от используемых вычислительных мощностей). Но кто-то очень умный решил создать большую таблицу, в которой каждому возможному значению хэша было создано соответствующее значение открытого пароля. В принципе, нужно было банально произвести атаку перебором. Если это числовой пароль, то нужно взять все возможные числа и сгенерировать для них хэш, только сохранить результат в базе данных и больше уже не нужно генерировать, просто подыскиваем в базе нужный пароль для хэш-значения с минимальными затратами.

Я где-то видел сайт, на котором можно было скачать заархивированную базу данных для хэша, и она была достаточно приличного размера. Только она уже не имеет никакой пользы. Дело в том, что специалисты по безопасности не стали стоять на месте. Больше пароль в чистом виде никто уже не шифрует. Вместо этого к паролю добавляется какой-нибудь мусор, и только потом шифровать необратимым образом. Этот мусор назвали солью (salt), потому что мы как бы подсаливаем пароль.

Чтобы понять всю соль, допустим, что ваш пароль — qwerty. Перед созданием хэш-значения, например с помощью популярного сейчас алгоритма MD5, мы должны просто добавить к паролю какое-нибудь значение, скажем, 12345. Получается, что мы создаем хэш для qwerty12345. Для такой строки хэш-значение будет равно A3A49DD303841BB6292AE756DFA114. На языке C# код шифрования выглядит следующим образом:

```
MD5CryptoServiceProvider provider = new MD5CryptoServiceProvider();
byte[] hashedbytes =
provider.ComputeHash(Encoding.UTF8.GetBytes("qwerty1235"));
StringBuilder hash = new StringBuilder();
foreach (byte b in hashedbytes)
  hash.Append(b.ToString("X"));
Console.WriteLine(hash.ToString());
```

Программисту эта соль практически не мешает. Каждый раз, когда пользователь вводит пароль, нужно к нему прибавить соль, зашифровать с помощью MD5 и сравнить результат с тем, что хранится в базе данных. А вот хакеру такой трюк добавляет проблем. Нужно знать, какая соль использовалась, как она использовалась, и, скорее всего, придется генерировать новую базу данных всех возможных значений.

Существует множество аппаратных решений для хранения паролей, например, специализированный съемный носитель, который защищен шифром, доступ к которому регламентирован. В этом случае нужно помнить только пароль для этого устройства.

Надежность физических устройств аутентификации намного выше. Если пароль, который вы вводите при старте компьютера, легко украсть и использовать, то аппаратную конструкцию подделать сложнее и дороже (если сама система сложная). Таким образом, намного эффективнее отстаивать подступы к компьютеру с помощью специализированных устройств, чем защищать вход в Windows паролем. Без такого механизма компьютер даже не запустится, а без пароля на Windows можно будет загрузиться с дискеты или компакт-диска. Думаю, что мои рекомендации по данному вопросу уже очевидны.

Сложность вскрытия пароля может быть увеличена за счет частой его замены. Многие специалисты по безопасности советуют это делать ежемесячно, ежеквартально или ежегодно. Как часто — зависит от секретности данных. Предполагается, что такая учащенная смена даст два преимущества к безопасности:

- если взломщик каким-либо образом получил доступ к паролю, то время его использования будет ограничено и закончится в момент очередной смены пароля;
- усложняется подбор пароля. Многие автоматизированные системы перехвата атак могут достаточно легко определить, когда на отдельную учетную запись авторизуются несколько раз подряд. Чтобы обойти такое препятствие, хакеры проверяют пароли с определенной задержкой. Это замедляет взлом, но, в конце концов, даст результат, если пароль несложен и не меняется. При частой смене вероятность успеть его подобрать становится очень низкой. Пока хакер подбирает украденный хэш, пользователь его уже заменяет новым.

Допустим, что хакер не знает хэша, а просто пытается перебором подобрать пароль к вашей системе. И тут снова может спасти частая смена. Чтобы увидеть это на примере, представим, что пароль может содержать только числа. Допустим, что на первоначальном этапе он был равен 7 000 000. Хакер тупым перебором прошел от 0 до 6 000 000, а в этот момент пароль меняется на 5 000 000. Дальнейшее сканирова-

ние хоть до миллиарда не даст результата, потому что новый пароль уже находится вне диапазона проверки.

В реальной жизни пароли содержат буквы, цифры и определенные символы, что дает большее количество комбинаций, а значит, требует увеличения времени подбора. Меняйте пароли на вход в систему чаще, и вы затрудните работу хакерам. Я меняю основные пароли примерно каждые полгода и иногда внепланово, при возникновении подозрительных ситуаций. Тьфу, тьфу, тьфу (ну вот, оплевал себе левое плечо), пока проблем не было, и надеюсь, что не будет.

На работе у нас политика защиты более жесткая, потому что мы работаем с персональной информацией миллионов пользователей сайта, там смена паролей происходит каждые три месяца. При этом осуществляется проверка, чтобы каждый последующий пароль не совпадал с предыдущими пятью паролями. Это значит, что не получится выбрать пару паролей и менять их между собой. Но с другой стороны многие идут на хитрость — добавляют в конце пароля цифру, которую банально увеличивают на 1 каждые три месяца. Не очень хорошее решение.

Давайте рассмотрим, как можно создать сложный пароль, и при этом его несложно было бы запоминать. Наиболее часто я встречался с созданием паролей на основе подмены локализации. Этот способ очень удобен для нас, русскоязычных пользователей, потому что в наших компьютерах используются две раскладки клавиатуры. Просто придумываем слово или даже выражение подлиннее, включаем английскую раскладку и пишем, глядя на русские буквы.

Например, выбираем в качестве пароля "возможно все". Теперь пишем это в английской раскладке без пробела и получаем "djpvj;yjdct". Вот этот бред уже никакой словарь содержать не будет и его можно получить только полным перебором.

У меня на работе, наверное, самые сложные пароли, потому что вокруг все англоговорящие, и для них мои пароли в стиле "J[j[jb1,enskrfHjvf" ничего не значат. Я без проблем пишу по-русски вслепую и мне не нужны русские буквы на клавишах, поэтому канадцы удивляются, когда я при них ввожу такой бред на большой скорости. А ведь здесь всего лишь написано "Охохои1бутылкаРома". Это просто пример того, как я выбираю пароли, реально же они у меня еще длиннее и обязательно включают заглавные буквы и цифры.

Еще один метод — допустим, что вы хотите назначить в качестве пароля слово generation. А что, слово достаточно длинное, но простое, и может быть легко взломано по словарю. Как усложнить пароль? Посмотрите на клавиатуру и набирайте вместо букв слова generation буквы, находящиеся немного выше. Например, прямо над буквой g находиться буква t, а над буквой e находиться цифра 3 и т. д. Таким образом получиться пароль: t3h34q589h. Такой пароль запоминается легко, а по словарю подобрать его нереально.

Вместо клавиш сверху можно взять клавиши, находящиеся справа, и тогда пароль generation превратится в hrmrtsyopm. Тоже нелегкая задача для хакера, но один недостаток — не содержит цифр.

А если еще и сделать некоторые из этих букв в верхнем регистре, то пароль усложнится сразу в два раза. Например, вы можете установить в верхнем регистре третью и восьмую буквы и получить hrMrtsyPm.

Вот такими простыми методами можно соорудить легко запоминаемый, но сложный для подбора пароль.

4.7.4. Пароли по умолчанию

Нет, я не буду повторяться про сложность пароля. Это уже и так ясно. Я хочу сказать, что в системе не должно быть имен пользователя и паролей по умолчанию. Например, в MS SQL Server есть системная учетная запись с именем sa (system administrator) и без пароля. Если администратор не изменил ее параметры, то любые шаги на усиление безопасности бесполезны.

Компания Microsoft создала эту учетную запись для нашего удобства и во время установки сервера баз данных настоятельно рекомендует менять пароль. Но администраторы игнорируют любые предупреждения, а когда система оказывается взломанной из-за неряшливости администратора, все начинают винить производителя. Такая же проблема была и в MySQL.

В Windows 7 есть гостевая учетная запись, и слава богу, что по умолчанию она отключена. Не вздумайте включать ее без особой надобности, а если решите использовать, то никогда не давайте больших прав, особенно на запись данных на диск или создание чего-либо.

Допустим, что ваш знакомый захотел вам переслать по сети некий файл. Вы доверяете ему и открываете доступ на запись, и вроде бы ничего страшного нет. А если через эту учетную запись работает 1000 человек? Где гарантия, что кто-то из них не удалит все каталоги? Даже среди двух пользователей один может оказаться злоумышленником, шутником или просто мною :).

4.7.5. Обновления

Я уже упоминал, что ошибки есть везде, просто в некоторых ОС их находят, а в других даже не ищут. ОС Windows — самая распространенная, и в ней работает большинство пользователей, поэтому хакеры именно здесь ищут ошибки и стараются взломать именно ее. Когда найдена прореха, появляется возможность проникнуть на чужой компьютер.

Корпорация Microsoft в последнее время много внимания уделяет безопасности системы и старается свести к минимуму нежелательные последствия от своих ошибок. Для этого регулярно выкладываются обновления и исправления для ОС и всех продуктов фирмы.

Повторю, что процедура обновления программ помогает защититься от проникновения вирусов *(см. разд. 4.1.3)*. Точно так же она приходит на выручку и при попытке вторжения со стороны хакеров. Безопасность — она и в Африке безопасность, и чаще всего не имеет значения, от чего вы защищаетесь — от вирусов или от хакеров.

Некоторые отключают обновления системы потому, что используют нелицензионное ПО. Подумайте, а этот риск того стоит?

4.7.6. Открытые ресурсы

Когда мы работаем в сети, то хочется обмениваться информацией, не отходя от монитора. Старый дедовский способ путешествия от компьютера к компьютеру с дискетой уже никого не устраивает, тем более что эти носители информации абсолютно ненадежны, и постоянно возникают ошибки чтения.

Начиная с Windows 2000, ресурсы стали труднее досягаемыми. Microsoft, наконец, запретила безымянный доступ по сети. Теперь можно подключиться к удаленному компьютеру, только зная имя пользователя и пароль, или если кто-то специально откроет гостевую учетную запись, чего я настоятельно не рекомендую делать.

Да и диски открывать уже нельзя. Но многие умудряются пускать на свой компьютер любых пользователей под одной и той же учетной записью (чаще всего уже существующей гостевой записью Гость (Guest)) и открывать доступ к папкам, указывая возможность полного доступа для всех. Эти действия мотивируются тем, что никогда не знаешь, что может пригодиться. Это невероятно глупо.

Вы должны четко разграничивать права, и для каждого пользователя, который входит в систему, заводить свою учетную запись. Открывая доступ к папке, разрешайте к ней обращаться только определенным пользователям и группам, а не всем. На моем рабочем компьютере есть только одна папка с полным доступом для всех. Я ее называю Babrujsk, где находится общедоступный мусор, не представляющий для меня никакой ценности. Другие папки я открываю исключительно для чтения и только конкретному человеку. Если кому-то нужен доступ на запись, то он помещает файл сначала в общую папку, а я сам его переношу, куда надо.

В моей домашней сети, к которой могут подключиться только те, кто знает не очень простой пароль для Wi-Fi-маршрутизатора, тоже нет никаких открытых ресурсов. У меня на компьютере есть несколько открытых папок, но при этом нет учетных записей для гостей или других пользователей. Заводить учетную запись для того, чтобы ко мне могли подключиться жена или дети, бессмысленно. Они и так знают мой локальный пароль. Вот именно его они и используют.

То имя пользователя, которое вы используете при входе в систему, точно также можно использовать и при подключении удаленно через сетевое окружение. Я своей жене и детям доверяю, поэтому жена знает мой пароль и может подключиться к моему компьютеру в любой момент, поэтому для них учетные записи я не заводил.

А вот если нужно обменяться данными с кем-то другим, кто приходит ко мне домой, я просто на время активирую учетную запись гостя, для которой установлен пароль 11 и есть доступ к одной только папке, или использую передачу файлов через Windows Live Messenger (в Северной Америке это самый популярный клиент), почту или даже флешки.

Старайтесь не предоставлять лишних прав на доступ даже во временное пользование. Тут же вспоминается случай, когда мне удалось получить у лучшего провайдера города почти круглосуточный выход в Интернет всего за 4 доллара в месяц. Уже много лет назад, когда я учился в институте, оптимальным способом доступа был ночной Интернет. Всего 12 долларов — и неограниченное присутствие с 0:00

до 8:00 утра (был период, когда тариф зависел от времени суток, сейчас он встречается у провайдеров реже). Ежедневно столько времени мне было ненужно, поэтому мы сбросились втроем и заходили в сеть по очереди.

Скоро выяснилось, что пользоваться Интернетом можно всем троим одновременно, и на сервере нет проверки на доступ нескольких человек с одного аккаунта. Но и этого оказалось мало. В конце рабочего дня администратора провайдера (в 17:00) я обратился в службу поддержки и попросил проконсультировать по поводу плохого дозвона. Меня долго инструктировали, а потом дали возможность проверить качество доступа. Для этого ограничение с 8:00 было продлено до 18:00. После этого уставший администратор забыл вернуть время на место, и в течение двух месяцев у троих человек был неограниченный доступ с 0:00 до 18:00. Потом мы упустили из виду продление договора, и нашу учетную запись просто закрыли.

Мораль достаточно проста — нельзя открывать ресурсы, а если вынуждены это сделать, то не забывайте закрыть. В моем случае не было взлома, и провайдер не мог ничего мне сказать, а вот администратор, скорее всего, лишился работы.

О том, как управлять пользователями и ресурсами, написано уже много книг. Если вы являетесь администратором сети или в ваши обязанности входит распределение прав доступа хотя бы на одном компьютере, то обязательно ознакомьтесь со специализированной литературой. Я же дал только общие рекомендации, исходя из личного опыта, который не может быть всесторонним.

4.7.7. Закройте ворота

Допустим, что у вас есть локальная сеть и для обмена информацией вы открыли папку, которая будет видна не только соседним компьютерам, но и в Интернете. Чтобы ограничить проникновение извне, нужно запретить доступ к файлам из Интернета.

Простейший способ попасть в настройки сети — это щелкнуть правой кнопкой мыши по значку сетевого соединения в области уведомлений панели задач (в районе часиков) и выбрать в появившемся меню **Центр управления сетями и общим доступом** (Open Network and Sharing Centre). Если у вас значка соединения нет, то придется щелкать мышью или нажимать клавиши чуть больше. Рекомендую воспользоваться клавиатурой. Нажмите кнопку **Пуск** (Start) и в строке поиска наберите `центр управления сетями и общим доступом` (в английском варианте все намного короче — `Network`; если Windows не найдет этот Центр с первого введенного слова, то набирайте это название, пока поиск не приведет к нужному результату). В этом окне щелкните по вашему соединению и потом в появившемся окне нажмите кнопку **Свойства** (Properties) — рис. 4.19.

В списке **Отмеченные компоненты используются этим подключением** (This connection uses the following items) перечислены все протоколы и сервисы, через которые можно получить доступ к сети (для некоторых типов подключения этот список находится на вкладке **Сеть** (Networking)). Сбросьте флажок **Служба доступа к файлам и принтерам сетей Microsoft** (File and Printer Sharing for Microsoft

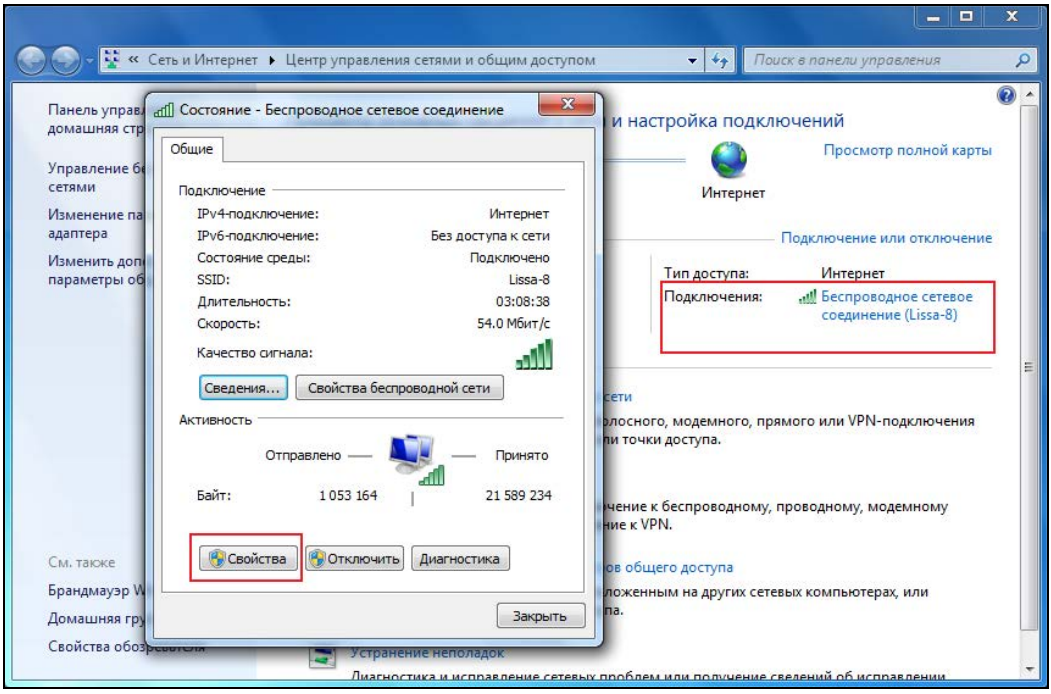


Рис. 4.19. Окно вызова свойств соединения

Networks). Теперь служба запрещена, и из Интернета нельзя будет обращаться к открытым локальным ресурсам.

4.7.8. Настройки

Теперь рассмотрим некоторые настройки Windows, которые также могут повысить защищенность системы. Когда вы устанавливаете ОС, то некоторые параметры настроены не на безопасность, а на повышение скорости работы. Для настольной системы я считаю такой подход оправданным. Это позволяет повысить производительность, но для сервера, где хранится больше важных данных, эти настройки неэффективны.

Самая большая ошибка, которую надо исправить — это путь к файлу explorer.exe. Ищем в реестре следующий раздел:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon

Обратите внимание, что в параметре `Shell` просто указано имя файла. А где этот файл? Подразумевается, что он должен быть в системе. Но это не всегда так, потому что если бросить в корень системного диска зло-файл с таким же именем, то будет выполняться именно он *(см. разд. 3.5.2)*. Ошибка исправляется просто — достаточно изменить значение параметра на полный путь, т. е. C:\Windows\explorer.exe.

Помню, как в начале 2000-х годов один из моих коллег доставал меня своей музыкой, а слушал он то, что мне не очень нравится. Неприятно 8 часов на работе внимать всякую ерунду. Чтобы отомстить, я написал небольшую программу, удаляющую все MP3-файлы, которую назвал так же, как именуется Screen Saver по умолчанию, и забросил ее в систему коллеги. Большинство пользователей после установки ОС не меняет заставку экрана. Таким был и мой коллега. Как только пришло время запустить хранитель экрана, так моя программа очистила диск от ненавистной музыки. Теперь я развлекаю отдел и слушаю то, что мне по душе.

Никогда не используйте Screen Saver, устанавливаемый по умолчанию. Он легко перезаписывается, и любой троян или вирус может подменить этот файл и выполнять в ваше отсутствие все, что вздумается.

При работе с системой, в которой недостаточно памяти, неиспользуемые страницы сохраняются на диске. При выключении компьютера эта информация не удаляется. В таких страничках памяти могут оказаться очень важные данные, а хакер может прочитать их. Чтобы этого не произошло, при выключении компьютера желательно очищать страницы. Для этого перемещаемся в реестре в следующий раздел:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management

Здесь должен существовать параметр `ClearPageFileAtShutdown` (если нет, то нужно создать такой параметр типа `DWORD`), значение которого по умолчанию равно `0`, и данные не стираются. Установите значение `1`, и выключение из-за очистки будет происходить дольше, но содержимое страниц памяти будет недоступно.

4.7.9. Невидимость

Сейчас мы поговорим о том, как спрятать в системе какой-либо файл. Для начала войдите в папку \Windows\System32. Посмотрите, сколько здесь файлов. Много? Даже слишком. И больше половины имеют расширение dll. Если появится еще один подобный файл, то никто этого даже не заметит. Только не надо называть его passwords.dll (слишком подозрительно). Имя не должно быть вызывающим, например, chkprofit.dll, тогда никто не обратит на него внимание.

Где-то я видел рекомендацию, что скрытый файл можно назвать kernel.dll. В системе есть библиотека kernel32.dll, и любой хакер знает, что никаких файлов типа kernel.dll или kernel16.dll не должно быть. Поэтому желательно придумать свое, не вызывающее подозрений имя, которое будет похоже на существующие в системе имена, но не должно отличаться только цифрами.

Несмотря на расширение dll, файл нужно воспринимать, как текстовый, и открывать для работы в текстовом редакторе, например в Notepad (Блокнот). Так как имя знаете только вы, то и найти его будет сложно среди тысячи системных файлов.

Файл с паролями можно хранить не только в каталоге \Windows\System32, но и в любом другом системном подкаталоге Windows или Program Files. Желательно, чтобы в папке было как можно больше всякого мусора, тогда среди него тяжелее

найти пароли. В результате мы получаем достаточно хорошо скрытый файл, но он содержит текст.

Есть более эффективный способ, который не стоит ни копейки — CyD Archiver XP (рис. 4.20). Я написал этот архиватор лет 10 назад, но так и не довел до продажного вида. Что бы не было — ни себе, ни людям, я решил отдать его тебе бесплатно. Установочный пакет можно найти в электронном архиве в каталоге Soft (архив расположен на FTP-сервере по адресу **ftp://85.249.45.166/9785977507905.zip**), а регистрационный код будет такой: er4n04731y4re4.

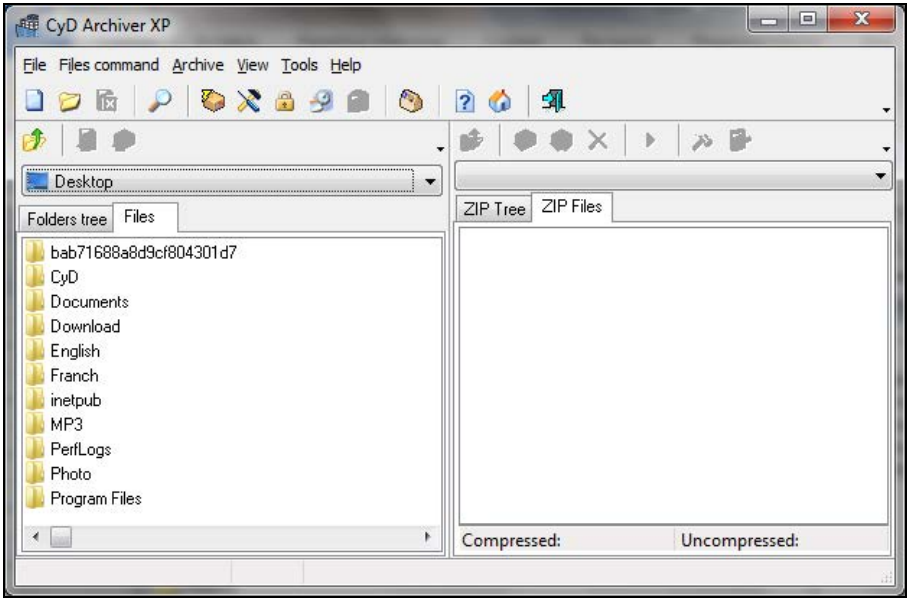


Рис. 4.20. Главное окно программы CyD Archiver XP

Чтобы воспользоваться этим способом, нужно выполнить следующие шаги:

1. Создайте текстовый файл, в котором будут храниться пароли. Этот файл может называться, как угодно.
2. Создайте архив с помощью программы CyD Archiver XP. Для этого достаточно выбрать файл и выполнить команду меню **File commands | Add to new archive** (Файловые команды | Добавить в новый архив). Запустится мастер создания архива. Для указания имени архива используйте те же правила, что были описаны для создания секретного файла. Это значит, что файл должен иметь расширение dll и не вызывать подозрений. CyD Archiver XP не обращает внимания на расширения, поэтому файл может иметь совершенно любое имя.
3. Для большей надежности установите пароль.
4. Перенесите файл в папку \Windows\System32.

Теперь файл скрыт, и при этом он нечитабельный. Многие архиваторы даже не смогут его открыть, потому что изменено расширение, зато с помощью CyD Archiver XP файл без проблем распаковывается.

Но есть архиваторы, которые тоже игнорируют расширения. Я бы не советовал вам CyD Archiver XP, если бы в нем не было еще одной удобной возможности — мягкое разрушение архива. Любой ZIP-файл начинается с заголовка, и первые два символа должны быть "PK". Видимо это сокращение от слова packet (упакованный). Запустите CyD Archiver XP и выберите команду **Break | Restore** (Сломать | Восстановить). Перед вами откроется окно, в котором нужно указать заархивированный файл. Щелкните по кнопке с тремя точками и с помощью стандартного диалога открытия файла найдите созданный вами архив. Теперь нажмите кнопку **Patch** (Поставить заплатку), и программа заменит первые два символа (сигнатуру файла) случайными.

Все архиваторы, которые я видел, перед раскрытием файла ZIP-архива проверяют его расширение на соответствие формату ZIP и сигнатуру, которая должна быть равна "PK". Если хотя бы одно из этих условий неверно, то файл считается неархивным и не открывается. Программа CyD Archiver XP не делает такой идентификации и может работать даже с "запорченным" таким образом архивом.

С помощью CyD Archiver XP можно прятать не только отдельные файлы с паролями, но и целые папки секретных документов. Главное, чтобы архив имел подходящее название и небольшой размер. Файлы слишком большого размера вызовут лишнее подозрение.

Если выполнить все эти простые действия, то получится достаточно защищенный файл, который сложно найти. Но пока что его выдает дата корректировки. Большинство системных файлов не модифицируется, а значит, дата изменения будет достаточно старой по сравнению с нашим файлом. Проблема решается любой специализированной утилитой или все тем же CyD Archiver XP, где нужно выбрать меню **File | Set file access time** (Файл | Установить время доступа). Просто не забывайте после внесения исправлений в файл изменять его дату.

Когда мне нужно перенести какие-то важные данные на флешке, то я редко копирую файлы в чистом виде. Чаще всего я архивирую все данные и как минимум меняю расширение с zip на что-нибудь менее приметное, ну хотя бы dat, и порчу заголовок архива, чтобы не сразу же было видно, что файл в реальности является архивом.

Это примитивная защита, но достаточно эффективная. Она не спасет, только если кто-то целенаправленно будет искать важные файлы на флешке. Даже если я потеряю ее и кто-то увидит мои файлы, их, скорее всего, удалят, как что-то непонятное. Если же вы хотите передать финансовую информацию, то здесь надежнее будет все же воспользоваться шифрованием.

4.7.10. Мнимая защита BIOS

Практически все BIOS имеют возможность установить пароль на вход в систему. Такая защита хороша тем, что если злоумышленник не знает пароля, то запустить компьютер будет невозможно. Но эта защита мнимая, потому что ее легко обойти. Вся информация BIOS сохраняется после выключения компьютера только за счет батарейки на материнской плате. Если эту батарейку вытащить и подождать не-

сколько секунд (для большей надежности можно замкнуть контакты в разъеме), то все настройки BIOS сбрасываются, в том числе и пароль.

Для старых версий BIOS (например, Award) было достаточно много универсальных паролей, которые работали всегда. Начиная с версии 4.51, такого списка больше нет, но безопасность системы при этом увеличилась не сильно.

Пароль BIOS может обеспечить минимальную защищенность, только если системный блок хорошо защищен, например, находится в другой комнате, в сейфе, под большим амбарным замком.

4.7.11. Шифрование

Шифрование — один из самых надежных способов защиты информации, особенно, если должное внимание уделить ключу, который должен иметь не только приемлемую длину (от этого зависит стойкость шифра от перебора), но и храниться в недосягаемом для хакера месте. Если данные будут украдены, то просмотреть их без ключа будет невозможно, потому что в большинстве случаев понадобится взлом через перебор паролей, а это может потребовать слишком много времени, и ценность результата будет несоизмерима с затратами.

У меня нет такой информации, которая стоила бы того, чтобы затратить сверхусилия на подбор пароля для потерянного шифра. Даже исходные коды программ, которыми я очень сильно дорожу, проще и дешевле написать заново.

Во всем мире сейчас достаточно часто воруют ноутбуки, в которых может храниться полная и исчерпывающая для хакера информация. Без шифрования украденная информация становится легкой добычей.

При неправильном создании ключа эффект от шифрования становится отрицательным, потому что такой код легко будет подобрать и уровень безопасности становится невысоким, но при этом излишне расходуются ресурсы, и компьютер начинает работать медленнее.

В большинстве криптографических программ ключ генерируется случайным образом и максимальной длины. В этом случае система сама заставляет вас использовать наибольшую защищенность. Если автоматической генерации нет, и код выбирается пользователем самостоятельно, то при определении ключа вы должны следовать всем рекомендациям, описанным в *разд. 4.7.3*.

Практически все современные операционные системы умеют шифровать целые диски. Для решения этой проблемы есть и специализированные программы сторонних разработчиков, которые зачастую обладают большими возможностями. Но шифровать абсолютно все диски со всеми данными нет смысла, потому что процесс отнимает ресурсы и компьютер будет без особой нужды работать медленнее.

Вы должны правильно ранжировать информацию и шифровать исключительно то, что необходимо. Если используемая вами программа умеет работать только с дисками, то лучшим способом будет завести отдельное устройство для секретных данных и кодировать только его. Предположим, вы храните пароли или секретные

файлы в системе (например, в папке Documents (Документы)), то шифровать придется весь системный диск. А т. к. системные файлы используются достаточно часто самой ОС Windows, то это может понизить производительность компьютера.

Встроенная в Windows служба шифрования может работать с отдельными папками и даже файлами. Но при этом нельзя зашифровать системные папки, что является большим минусом. Если вы собираетесь пользоваться встроенными в Windows возможностями криптографии, то ни в коем случае не храните секретные данные в системе.

Есть отдельные программные решения, которые шифруют целые диски, включая системные данные, например CryptoDisc. Она шифрует полностью диск и запускается сразу после старта компьютера и до ОС. Вы вводите пароль, который используется для расшифровки, программа начинает расшифровывать диск и запускать с него ОС. Без знания пароля жесткий диск практически бесполезен.

Вернемся к шифрованию самой ОС Windows. Оно доступно, только если диск отформатирован, как NTFS. В файловой системе FAT32 данный сервис работать не может.

Чтобы зашифровать папку или файл, щелкните по ним правой кнопкой мыши и в появившемся меню выберите пункт **Свойства** (Properties). На вкладке **Общие** (General) нажмите кнопку **Другие** (Advanced), и перед вами откроется окно дополнительных атрибутов. Установите флажок **Шифровать содержимое для защиты данных** (Encrypt contents to secure data). После этого все данные будут кодироваться, и при этом незаметно для вас. Остальные пользователи не смогут прочитать эти данные.

Не забывайте регулярно делать резервную копию шифруемых данных. Если целостность ОС будет нарушена и запуск станет невозможным, то восстановить тайнопись будет нельзя. Конечно же, резервную копию тоже надо беречь от посторонних глаз, потому что нет смысла шифровать то, что легко можно получить в естественном виде, но другим способом.

Шифровать нужно не только диски, но и информацию, передаваемую по сети, особенно по открытым каналам. Интернет создавался, как открытая сеть, и в ней очень много способов получить чужие данные. Одним из вариантов является использование программ-сниферов, которые прослушивают трафик и перехватывают сторонние пакеты. Для работы подобных программ нужно установить их на такой компьютер, через который проходят чужие данные.

Если поставить снифер на свой локальный компьютер, который имеет выход в Интернет через модем, то можно будет увидеть только свой трафик. Но если установить такую программу на сервер провайдера, то окажутся видимыми данные всех его пользователей.

Вся корреспонденция, которой вы обмениваетесь через сеть, по умолчанию передается в открытом виде. Вы должны сами позаботиться о ее защите. В большинстве почтовых клиентов уже встроены средства для шифрования писем с помощью технологии PGP (Pretty Good Privacy, достаточно хорошая секретность) или OpenPGP.

Этот метод основан на шифровании с открытым ключом. Рассмотрим, как работать с PGP.

Вы генерируете пару не связанных между собой ключей: открытый и закрытый. С помощью открытого ключа можно закодировать данные, но для расшифровки нужен только закрытый ключ, который не может быть подобран простыми алгоритмами. Вы публикуете свой открытый ключ, после чего любой пользователь может зашифровать сообщение и отправить его вам. Даже если кто-нибудь его перехватит, для чтения нужна расшифровка, которая возможна только с помощью закрытого ключа, а он есть только у вас.

Никогда не публикуйте свой закрытый ключ, и можете считать, что ваша корреспонденция будет защищена на все 100%, т. к. расшифровка становится возможной только с помощью полного перебора. Даже при использовании сети из самых мощных компьютеров для подбора ключа длиной 256 бит (32 символа) будет потрачено непомерно много времени. Если вы не пересылаете правительственные документы, исходные коды Windows или номера кредитных карточек с миллионными вложениями, то ни один хакер не будет тратить такие ресурсы на взлом. Если подбирать пароль с помощью простого домашнего компьютера (пусть даже самого быстрого), хакер раньше состарится, чем узнает текст сообщения. К тому времени добытая информация станет уже никому ненужной.

4.7.12. Учетные записи

Для доступа к компьютеру, на котором установлена Windows 7, нужно знать имя и пароль какой-либо учетной записи. В системе по умолчанию активна только одна запись — администратора. Если к вашему компьютеру никто не подключается, то так и должно быть. Единственное, что могу посоветовать, — переименовать ее, указав, например, свое имя.

Встроенная учетная запись администратора является самой главной и обладает всеми правами (ну или почти всеми). Если оставить имя по умолчанию, то злоумышленник будет заведомо знать его, и останется только подобрать пароль. О безопасности компьютера можно забыть, если пароль простой, т. к. профессиональный хакер быстро найдет его по словарю с помощью специальных утилит.

Для управления учетными записями нужно запустить оснастку **Управление компьютером** (Computer management). Для этого выберите меню **Пуск | Панель управления | Администрирование | Управление компьютером** (Start | Control Panel | Administrative tools | Computer Management) или щелкните правой кнопкой мышки на строке **Компьютер** (Computer) в главном меню ОС и выберите в меню пункт **Управление** (Manage). Перед вами откроется окно, как на рис. 4.21.

Перейдите в раздел **Управление компьютером | Служебные программы | Локальные пользователи и группы | Пользователи** (Computer management | System tools | Local Users and Groups | Users). Переименуйте учетную запись администратора. Для этого нужно щелкнуть по ней правой кнопкой мыши и в появившемся меню выбрать команду **Переименовать** (Rename).

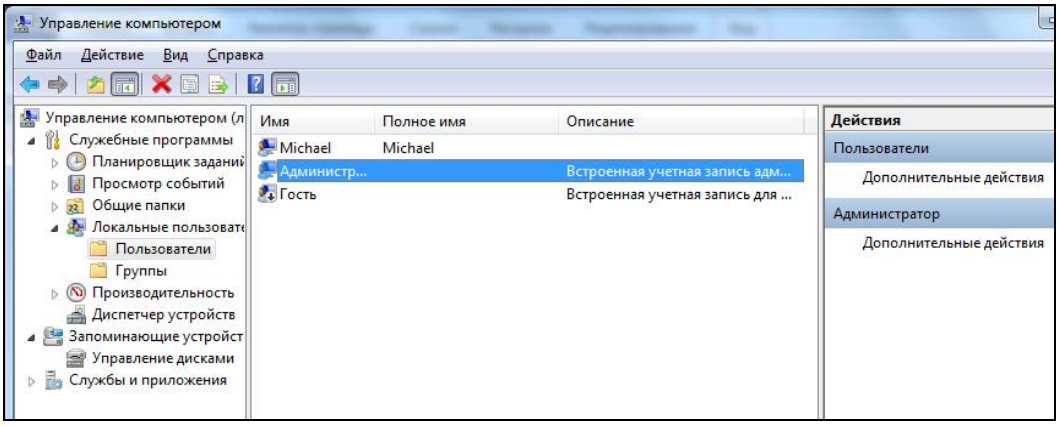


Рис. 4.21. Оснастка **Управление компьютером**

Вы должны следить, чтобы в системе были активными только те учетные записи, которые действительно используются. Я не раз слышал, как взламывали корпоративные серверы с помощью учетных записей уволившихся сотрудников, т. к. обиженные и недовольные зачастую ищут способы отомстить за несправедливость. Корпоративная безопасность выходит за рамки данной книги, и этот случай приведен только как пример.

На домашних компьютерах тоже бывают случаи взлома через неиспользуемые учетные записи, созданные, например, кем-то из друзей, злоумышленником через троянскую программу или даже вирус. А некоторые пользователи сами создают несколько записей, но в результате используют только одну.

Чем больше записей в системе, тем больше вероятность, что у одной из них будет слабый пароль, который легко подобрать по словарю. Кто-то обязательно выберет простой пароль. В Интернете легко найти утилиты и словари, которые содержат наиболее употребляемые пароли. Чтобы перебрать весь словарь, много времени не нужно. Как показывает практика, больше эффекта дает перебор по словарю 100 пользователей, чем проверка одного полным перебором.

Администраторы сети должны уделять больше внимания учетным записям и для облегчения жизни использовать политики. Но это уже более сложные настройки, и мы не будем их касаться.

4.7.13. Физический доступ

Я уже говорил, что взлом может быть как удаленным, так и локальным. Чтобы злоумышленник не получил физический доступ к технике, серверы зачастую размещают в отдельной комнате, которая оборудована сигнализацией. Таким образом, никто не сможет просто сесть за клавиатуру защищенного сервера и воспользоваться его ресурсами. Администраторы сами управляют такими комплексами по сети, а правонарушитель сможет произвести взлом только удаленно.

В 90-х годах прошлого столетия, когда компьютеры стоили достаточно дорого и были доступны единицам, я видел, как в одной фирме компьютер находился в

большом сейфе. Приходя на работу, программист открывал сейф и работал за компьютером, который находился внутри.

С ноутбуками намного тяжелее. Если стационарный компьютер занимает много места и солидно весит, то ноутбук легкий и переносной. Нет проблем взять его подмышку и отнести к себе домой. Для защиты от воровства в большинстве переносных компьютеров встроен разъем для подключения кабеля Kensington Lock. Таким способом легко прикрепить ноутбук к столу или к какой-либо неподвижной части офисной мебели, и злоумышленник уже не сможет просто забрать ваш ноутбук, который будет, как собака на привязи — пока хозяин не откроет замок, гулять не побежишь.

Сейчас все больше получают популярность центры обработки данных. Компании специализируются на том, что строят целые здания специально для серверов. Любая другая компания может арендовать серверы или даже целые помещения в этом здании. В таких местах арендуют помещения не только маленькие компании, у которых не хватает денег на собственные центры, но и крупные компании. Просто это реально выгодно.

4.8. Восстановление утерянных данных

Каждый, кто достаточно долго работает с компьютером, не раз сталкивался с проблемой потерянных данных. Файлы могут пропадать по причине отключения электричества или банального удаления не того файла. В любом случае, если потеряны данные, полученные в результате долгого и кропотливого труда, хочется их восстановить, а не делать работу заново.

В мою недолгую, но очень насыщенную бытность администратором я не раз встречался с ситуацией, когда барышни печатают со скоростью 1000 символов в минуту. Правда, такая белиберда получается :). Такие девушки (да и мужчины этим страдают) сначала делают, потом думают, поэтому рука быстрей мысли тянется к кнопке удаления, а вслед раздается жуткий крик: "Ой, я удалила квартальный отчет!!!" Создавать заново? Я думаю, что не стоит. Можно попытаться восстановить данные, и если заняться этим сразу, то процесс восстановления не отнимет много сил и времени.

Не забывайте, что бывают и физические поломки носителей информации. Например, на жестких дисках со временем образуются испорченные области, и данные становятся нечитаемыми. Помимо этого, существует вирусная опасность. В последнее время количество вирусов и их разновидностей растет. Если появится такой "микроб", который найдет уникальный способ проникновения в систему (например, через дыру в безопасности Windows) и начнет уничтожать данные, то можно потерять все.

Если информация потеряна из-за физической неполадки дисков, то их восстановить будет проблематично. В остальных случаях можно попытаться.

4.8.1. Как удаляются файлы

Когда вы удаляете файл, то ОС Windows переносит его в корзину. Корзина — это всего лишь скрытая папка Recycle, которая существует на каждом диске, и при удалении файл переносится в ближайшую из них, а ближайшая находится на том же диске, что и удаляемый файл. Таким образом, операция происходит быстро, но не окончательно. В любой момент можно заглянуть в эту корзину и вернуть файл на место в целости и сохранности.

Когда происходит очистка корзины или просто удаление файла с удержанием клавиши <Shift>, тогда файлы удаляются с диска без помещения в корзину. Но даже в этом случае физически файлы не уничтожаются. Они остаются на месте, просто секторы на диске помечаются свободными. В FAT16 при удалении первая буква имени файла заменялась значком "~". Поэтому в утилитах восстановления типа undelete нужно было найти требуемый файл и сделать обратную подмену первой буквы. Если вы ее не помните, можно указать что угодно, кроме символа "~".

В FAT32 сохраняется полное имя, и оно отображается в утилитах восстановления файлов, файл просто помечается как удаленный. Но смысл от этого не меняется. Когда вы пытаетесь что-то удалить, это еще не по-настоящему. Просто первый сектор помечается как свободный. После этого ОС может использовать его в своих целях для записи новых файлов.

Пока не производилось записей в освобожденные секторы, вы можете без проблем воскресить любой удаленный файл. Вероятность полного восстановления достаточно высока, если на вашем жестком диске достаточно свободного места, и вы не производили каких-либо больших копирований/установок и перезагрузок. С каждой такой операцией шансы падают, поэтому вы должны браться за дело как можно быстрее. Отсутствие свободного места на диске увеличивает вероятность того, что ОС запишет какие-либо данные поверх удаленных.

4.8.2. Полное удаление

Получается, что даже после удаления можно восстановить множество данных. А если они секретные? Допустим, что вы хотите выбросить старый винчестер, и чтобы хакер, который найдет этот диск, не смог увидеть ваши секретные данные, решили все с него удалить. Вы смело стираете данные и вытаскиваете устройство из компьютера. После этого никаких операций записи на диск не будет, и абсолютно все данные могут быть восстановлены без особого труда. Так что вы зря потратили время на чистку диска.

На моем компьютере очень много информации, которую я не хотел бы оставить в доступном для других виде, поэтому перед тем, как выбросить диск, я и вам рекомендую выполнить с ним следующие действия:

1. Удалить все секретные файлы.
2. Заполнить ненужной информацией на 70—80%. Можно даже записать до 100%, чтобы уж "наверняка".
3. Запустить дефрагментацию.

Если даже во время выполнения п. 2 какие-то файлы останутся доступными для восстановления, то после дефрагментации уже ничего не вернешь. В момент ее выполнения происходит большое количество операций чтения/записи данных, а свободные 20% пространства будут использованы для временного хранения данных. После такой процедуры можно с 99% уверенностью сказать, что данные восстановить будет нереально.

Где-то я читал, что даже если в сектор записывалась информация поверх удаленной, изначальные данные все же можно восстановить. Лично я с трудом себе это представляю, поэтому подтвердить не могу. Но для собственного успокоения можно как раз и запустить дефрагментацию.

Для окончательного уничтожения информации на жестком диске существуют специальные утилиты, которые на место удаляемого файла записывают беспорядочный мусор. Эти программы удобны и просты в использовании, но после их установки стирание будет происходить дольше, потому что при простом удалении достаточно только поставить специальную метку *(см. разд. 4.8.1)*, а при установленной утилите нужно еще записать на диск информацию того же объема, что и удаляемый файл, чтобы уничтожить все следы.

Я не использую утилиты полного стирания файлов, т. к. они зря расходуют ресурсы. А если производитель говорит, что на место удаленного файла мусор записывается дважды, то таким программам я вообще не доверяю (одного раза должно быть вполне достаточно!). Да я и никогда не занимаюсь ничем нелегальным, чтобы уничтожать какие-то данные бесследно.

4.8.3. Утилиты восстановления данных

Самый простой способ восстановить данные — использовать специализированную утилиту. Такие программы имеют простой графический интерфейс, чаще всего напоминающий Проводник Windows (Windows Explorer). Вы просматриваете каталоги в поисках удаленных данных, и как только нужный файл найден, просто нажимаете кнопку восстановления.

Мы уже знаем, что между удалением и восстановлением должно пройти как можно меньше времени и операций записи на диск, поэтому вы должны заранее подготовиться к непредвиденным ситуациям. Допустим, что у вас пропал файл. Вы заходите на веб-страничку, скачиваете и устанавливаете программу, но в этот момент уже происходит запись на диск, и нет гарантии, что не затрутся нужные кластеры.

Если вы потеряли данные, и при этом отсутствует утилита восстановления, то не устанавливайте программу на тот диск, на котором находился погибший файл. Необходимо свести к минимуму операции записи на это устройство, чтобы не использовались освобожденные кластеры.

Вы должны найти и инсталлировать программу заранее, а я постараюсь помочь вам сделать правильный выбор и рассказать о существующих на данный момент средствах.

EasyRecovery

Это самая мощная утилита в этом классе, она имеет наибольший размер дистрибутива — менее 40 Мбайт. Раньше программу можно было скачать с сайта разработчика **http://www.krollontrack.com/data-recovery/**, но теперь она там недоступна, а вместо программы на сайте предлагают только сервисы по восстановлению данных. То есть саму программу не дают, а за деньги восстановят что возможно.

Наверно поэтому программа не обновлялась давно, но ее можно найти на сайте **www.download.com** (**http://download.cnet.com/EasyRecovery-Professional/3000-2242_4-37386.html**).

Программа стоит достаточно дорого, но иногда ее возможности просто необходимы, и убытки от потерянных документов или отчетов могут превысить затраты на ее приобретение в несколько раз.

Профессиональный пакет позволяет не только восстанавливать утерянные данные, но и реанимировать испорченные документы MS Office. Допустим, что на жестком диске образовался плохой кластер. В этом случае не откроется файл, располагающийся в этой области, а он, вероятно, содержит критически важную информацию. С помощью EasyRecovery ее можно вернуть к жизни. Конечно, в результате могут потеряться данные, попавшие в испорченный кластер, но файл можно будет открыть и увидеть незатронутую часть документа. Зачастую достаточно небольших изменений (переформатирование стилей, восстановление куска текста), и документ снова готов к использованию.

Этот пакет включает много утилит для диагностики и устранения неисправностей различных носителей. Кроме того, вы можете восстанавливать даже сообщения электронной почты.

Запустив программу, вы сразу ощутите, что это одна из самых старых утилит, потому что в ней большое количество возможностей и все продумано до мелочей. Отпугивает только цена. Ваша задача — соизмерить затраты от потери данных и приобретения пакета. Если информация вам слишком дорога, то вы должны купить эту программу уже сейчас.

File Recovery

Это самая простая и удобная утилита, доступная по адресу **http://www.lc-tech.com/**. Она поддерживает основные файловые системы: FAT12, FAT16, FAT32, NTFS, VFAT. Возможна работа даже со сжатыми или зашифрованными томами и папками NTFS.

Самая простая лицензия стоит 60 долларов, а самая дорогая — 150 долларов. Это вполне приемлемо для такого продукта, который сможет сэкономить вам время в случае непредвиденной ситуации.

4.8.4. Восстановление данных с носителей

На компакт-дисках или флеш-накопителях информация также не уничтожается, а только помечается. И вы теми же методами можете восстановить якобы стертую

информацию. Некоторые программы явно предупреждают о возможности восстановления данных. А в серьезные пакеты для работы с компакт-дисками даже входят утилиты для восстановления стертых файлов.

Во всех программах для записи компакт-дисков, которые я видел, по умолчанию используется быстрый метод стирания, при котором информация полностью не затирается. Если вы хотите выкинуть диск, но информация на нем все еще важна, то для очистки используйте полный метод. Но я вместо этого беру ножницы и ставлю несколько глубоких царапин на поверхности диска, чтобы их невозможно было восстановить полировкой.

4.9. Реанимация

Сколько раз я видел, как выбрасывают вполне рабочие компоненты компьютера или диски, которые еще можно восстановить с минимальными затратами. Один знакомый коллекционирует такие компоненты и возвращает их к жизни. У него дома стоят целые коробки с реанимированными жесткими дисками, приводами CD-ROM и различными платами. Если посмотреть на его компьютер, то в голову приходит только одно название — "Восставший из Ада", потому что нет ни одного винтика, который был бы куплен новым, все собрано из неработающего железа. Глядя на комнату, создается впечатление, что человек живет после третей мировой войны, а такие условия очень часто ассоциируют с хакерами.

Некоторые компоненты действительно проще выкинуть, но процесс реанимации уже практически мертвого железа может оказаться интересным, а главное — появится возможность сказать друзьям, что эта часть компьютера была восстановлена из пепла собственными руками.

4.9.1. Вентиляторы

Любой вентилятор со временем изнашивается и начинает скрипеть и издавать неприятные звуки. Многих пугает этот шум, но не стоит падать в обморок. Сначала приложите ухо к системному блоку и постарайтесь определить, откуда идет звук. Если сзади, то это вентилятор блока питания, если из центра, то виновник — кулер. Обе проблемы решаемы, но вторая проще, потому что вентилятор на процессоре легче снять, а для вскрытия блока питания нужно раскрутить намного больше винтов.

Если определить источник звука невозможно, но через некоторое время после начала работы шум исчезает, то, скорее всего, это вентилятор на процессоре. Его пропеллер — более нежный и чаще выходит из строя.

Почему шумят вентиляторы? Есть две причины:

- из-за пыли ухудшилась смазка, что приводит к более сильному трению движущихся частей;
- разболтались ось и втулка вентилятора, и крыльчатка бьет о стенки.

Обе причины устраняются простой смазкой, и для этого нужно всего лишь несколько капель обычного машинного масла. Но в первом случае этой процедуры хватит надолго, а во втором — на достаточно короткий срок.

Увеличение трения встречается чаще. В компьютере постоянно собирается пыль, и его регулярно надо чистить, пылесосить, протирать. Но лень — самый страшный враг, из-за которого мы очень редко вскрываем корпус.

Рис. 4.22. Отверстие на вентиляторе

Если вентилятор зашумел, и по близости нет сервисного центра, то проблему можно решить за пять минут. Вскрываем корпус и снимаем с процессора вентилятор. Очищаем его от пыли, протираем и внимательно осматриваем. Сбоку должно быть небольшое отверстие, как показано на рис. 4.22.

В фирменных вентиляторах Intel такое отверстие очень часто прячется сверху под наклейкой. Чтобы оно стало доступным, нужно отодрать этот кусочек фольги.

Если отверстие найдено, то капаем в него немного масла и возвращаем кулер на место. При отсутствии дырочки постарайтесь капнуть масло через какую-нибудь щель между осью крыльчатки и втулкой. После этого вентилятор должен заработать, как новый.

Восстановление вентилятора на блоке питания схоже с этим процессом для кулера, только разбирать надо дольше, и специальных отверстий для смазки практически не бывает.

Итак, даже если вентилятор работает достаточно тихо, но вы открыли крышку системного блока, то протереть и добавить капельку масла в вентилятор на процессоре не отнимет много времени, зато продлит его жизнь и сделает работу компьютера чуть тише.

4.9.2. CD- и DVD-диски

Поверхности диска довольно уязвимы и со временем портятся.

Самое сложное — восстановить боковую часть. Она тонкая, и если нет хорошей защиты, то влага постепенно разрушает поверхность диска, и он становится нечитаемым.

Плоскость, на которой нарисован рисунок, тоже очень важна. Она является как бы отражателем, и если появится царапина, то диск может читаться с ошибками. Как CD-, так и DVD-диски восстанавливаются обычным лаком для ногтей. Возьмите темный лак и обработайте повреждение. Я таким образом восстановил не один фильм.

Нижняя поверхность тоже достаточно нежная, и на ней также появляются царапины, ухудшающие отражение лазера. Здесь уже нельзя ничего закрашивать. Жела-

тельно избавиться от царапины. Если она неглубокая, то проблема решается полировкой поверхности. Как это сделать? Берем зубную пасту и бархатным лоскутком или любым другим мягким материалом натираем царапину. Чаще всего это помогает.

4.9.3. CD-приводы

Вот представьте себе, сидите вы, работаете и одновременно слушаете какую-нибудь музыку с CD или просто копируете данные с компакт-диска, а в этот момент происходит страшный, но не смертельный взрыв в системном блоке. Это всего лишь лопнул компакт-диск.

Почему взрываются диски? Современные приводы читают носители на скорости, в пятьдесят и более раз превышающей скорость, принятую при разработке стандарта CD. Старые компьютерные диски не рассчитаны на такие параметры, поэтому пластик не выдерживает и постепенно лопается. Трещинам на поверхности диска способствуют и царапины. Со временем трещины становятся критичными, и диск просто разрывает.

Большинство аудиодисков тоже не рассчитаны на работу на такой скорости, потому что для качественного воспроизведения звука с упреждающим чтением данных в буфер достаточно и 2X скорости. В музыкальных центрах и других специализированных проигрывателях не используется такая высокая скорость, поэтому диски работают долго и стабильно даже при наличии трещин, а на компьютере появляется вероятность взрыва.

Чистка после взрыва

Если диск разорвался, то весь привод изнутри будет покрыт кусками диска. Их нужно аккуратно вычистить. Для начала попытайтесь открыть крышку CD-ROM. Если не получится, то на передней панели найдите маленькое отверстие. Возьмите тонкую, но длинную иголку или спицу (обязательно жесткую) и аккуратно вставьте в отверстие. Попробуйте нащупать что-то наподобие шестеренки и, слегка подталкивая, попытайтесь провернуть ее. Крышка немного приподнимется, и ее уже можно будет открыть руками.

Теперь нужно вытащить все остатки. Если скорость привода небольшая, то есть вероятность, что диск раскололся на несколько больших частей, и их легко будет извлечь. В противном случае диск рассыпался на маленькие кусочки, многие из которых размером с песчинку. Такое уже извлечь без вскрытия привода невозможно.

Если вам не повезло, и диск превратился в порошок, то прежде всего выключите питание компьютера и снимите крышку с системного блока. Отключите все кабели от CD-привода (предварительно запомните, как они подсоединены) и вытащите его, открутив крепеж. На коробке привода очень много предупреждений о нежелательности вскрытия, но не стоит обращать на них внимание, просто в этот момент CD-ROM должен быть отключен от питания.

Большинство приводов открывается простым откручиванием четырех винтов снизу коробки и снятием верхней крышки и передней панели. Ваша задача — вытряхнуть весь мусор и собрать устройство. После этого все будет работать, как новое, если во время взрыва не сорвало или не испортилась линза, или не нарушилась электроника.

Чистка линзы

Со временем приводы CD-ROM начинают плохо читать диски. Это связано с грязью и пылью, которая является главным нашим врагом. Как бы вы не старались, рано или поздно пачкается линза, через которую пропускается лазерный луч.

Для исправления ситуации есть специальные чистящие компакт-диски. По внешнему виду они ничем не отличаются от всех остальных, разница только в том, что на нижней поверхности у них прикреплена мягкая щеточка. Когда привод пытается прочитать диск, то щетка сбрасывает всю грязь с линзы.

Но чистящие диски помогают не всегда. Если грязь въевшаяся, то придется вскрывать привод и мыть линзу вручную. Для этого лучше всего использовать вату и простую воду. Нежелательно применять в качестве моющего средства ничего спиртосодержащего, потому что линза не стеклянная и может потускнеть.

4.9.4. Жесткие диски

Жесткие диски в последнее время стали менее надежны. У меня три диска еще 97—99 годов выпуска, и все они до сих пор работают, как новенькие, и без испорченных блоков. С повышением плотности записи блоки стали миниатюрными, но их качество оставляет желать лучшего. Мы регулярно встречаемся с ситуацией, когда из-за этого невозможно прочитать информацию, и необходимые данные теряются.

Почему появляются испорченные блоки? Они есть всегда, даже на абсолютно новых дисках. Так как кластеры на диске слишком маленькие, любая пылинка или неверное движение считывающей головки убивает их. Производители заранее закладывают определенный процент брака, и на диске есть резервные блоки. Пока они есть, перенос из плохих участков происходит незаметно, но когда запас заканчивается, то уже с помощью специальных программ можно визуально наблюдать испорченные области.

Большинство пользователей запускает сканирование диска (scandisk), в процессе которого испорченный блок помечается, как неиспользуемый, а информация переносится в другое место. Но через месяц или даже меньше рядом с этим местом появится еще один плохой блок. Так можно долго сканировать и постоянно помечать испорченные области.

Чаще всего плохие области образуются в конце диска, и если сократить его размер процентов на 10—20, то диск еще долго проработает, как новый, и, скорее всего, не будет напоминать о случившихся проблемах.

Иногда винчестер помогают восстановить специализированные утилиты диагностики и ремонта от производителя. Но, судя по моей практике, такое восстановле-

ние — явление временное, и через некоторое время диск все равно начинает сбоить. Поэтому данное решение можно использовать лишь как промежуточный вариант, когда нет возможности купить новый диск.

Чтобы воспользоваться программой производителя, вы должны четко знать модель диска и найти нужную утилиту на его сайте. Прежде чем использовать ее, ознакомьтесь с документацией.

4.10. Взлом программ

Защита и взлом программ — это вечная война между программистами и хакерами. Программисты хотят получать за свой труд деньги, и это вполне законно. Каждый должен на что-то жить и не может раздавать продукты своего труда бесплатно. Если человек выбрал программирование своей профессией, то она должна приносить доход и обеспечивать достойное существование ему и его семье.

Просто так раздают свои разработки только программисты-любители, которые занимаются этим в свободное от работы время, и при этом не обеспечивают своих пользователей полноценной помощью, а отдают программы в таком виде, в каком есть. Бывают случаи, когда компании специально распространяют бесплатный софт, а зарабатывают или на поддержке (как это часто бывает в сообществе Open Source), или на других сопутствующих продуктах, или на рекламе, но такая бизнес-модель применима далеко не во всех классах программ.

Хакеры категорически не хотят платить за программы. Если человек взламывает программу из-за отсутствия денег, то это еще можно простить. Но если это происходит ради получения выгоды или просто ради процесса, то это уже преступление, и должно быть наказуемо. Хотя, с точки зрения закона, преступлением являются оба случая.

Лично я не понимаю, когда некоторые возмущаются тем, что компании продают программы, тогда как должны раздавать бесплатно. Никто же не возмущается тем, что пекарни продают хлеб, а не раздают бесплатно, или "АвтоВаз" продает то, что они называют автомобилями, а не раздают просто так.

Программное обеспечение — это такой же продукт, который требует множества усилий для того, чтобы его произвести на свет. Это работа большого количества людей, которые отдают себя работе по 8 часов в день, а кто-то и больше.

Я не понимаю возмущения тем, что компании, производящие софт, зарабатывают слишком много. Далеко не все. К тому же, производители программного обеспечения — далеко не самые богатые компании. Самый богатый человек в мире по последним данным является владельцем сотовой компании. Никто же не требует бесплатных сотовых услуг.

В общем, лично я считаю, что за программное обеспечение нужно платить, как и за любой другой продукт. Точно так же нужно платить за книги, на выпуск которых большое количество людей тратят свои силы. Над этой книгой работаю не только я один. Над ней работали большое количество людей, включая редакторов и дизай-

неров, за что им большое спасибо. Если вам нравится программный продукт или книга, то не воруйте, а скажите свое реальное спасибо — купите эту программу/книгу.

Это было небольшое (может даже и большое) лирическое отступление в мир прав и порядка, а сейчас пора уже переходить к самой теме взлома. В данной книге мы затронем только основные принципы, которые хакеры применяют при взломе программы. Эта информация дается исключительно в познавательных целях и не рекомендуется к использованию на практике, особенно в корыстных целях. Хотя будут рассматриваться только простые методы, я надеюсь, что эта тема окажется для вас интересной и поучительной.

4.10.1. Почему ломают?

Большинство программ, выпущенных под грифом Shareware, должно работать определенное время или рассчитано на ограниченное количество запусков. Они защищены простейшим счетчиком или элементарным математическим алгоритмом проверки даты. Обойти такую преграду достаточно просто и не составит труда даже неопытному пользователю.

Почему нередко защита такая простая? Потому что программист-одиночка не будет тратить на это много времени и сил. Нужно придумывать что-то оригинальное и новое, чтобы хакеру было сложнее взломать программу. Если уделить большое внимание этому вопросу, то не останется времени на реализацию функциональной части софта. И тогда программист не сможет конкурировать с монстрами от корпораций и специализированных фирм, у которых уже есть опыт борьбы и наработанные алгоритмы защиты. Продукты, созданные в этих фирмах командами разработчиков, имеют более стойкую защиту, нежели простая накрутка, но это не значит, что ее взломать нельзя. Это будет не по силам начинающему хакеру, а профессионал, который уже не один раз вскрывал эту программу и знаком с алгоритмами, используемыми в данной фирме, быстро найдет изменения и взломает снова.

Обратите внимание, даже Microsoft до появления активации в Windows XP защищала свои программы простым серийным номером, который проверяется математически. Алгоритм прост, как три копейки, потому что нет смысла выдумывать серьезные вычисления. Нет такой обороны, которую не прорвали бы хакеры.

Если взлом будет слишком сложен, то купивший одну лицензию может распространить серийный код по всему миру. Вы скажете, что такой код легко определить и узнать, кто его размножил! Нет, в Интернете такие серийные номера, в основном, существуют на программы, которые куплены по ворованным кредитным картам. Так что вы не сможете найти настоящего виновника.

Нет смысла защищаться, все равно в этой войне победит нападающий. Нужно сделать так, чтобы покупать лицензионный софт стало выгоднее, чем воровать. Цена должна соответствовать содержимому. Если эти условия будут соблюдаться, то люди начнут покупать программы, а не будут взламывать или пользоваться крэками. Если программа не стоит своих денег, то, как бы вы не защищали, ее все равно

не купят. В этом случае, если хакер не сможет ее взломать, то просто перейдет на другую программу. Благо, в наше время есть выбор практически для всего.

Некоторые фирмы пытаются встроить в свои продукты поддержку ключей и шифрования или привязку к оборудованию, но и такие системы оказались беззащитными. Если что-то невозможно взломать, то программа не получит распространения. Одна из причин, почему ОС Windows стала популярной — простота, удобство и легкость взлома. Крэки появлялись в Интернете раньше, чем новая версия. Таким образом, количество пользователей стало очень большим, и некоторые из них оплатили лицензию. Лучшая реклама для продукта — это отклики владельцев. Чем больше пользователей (легальных и нет), тем выше популярность. Бороться с хакерами бесполезно, а иногда и просто ненужно. Зарабатывать деньги следует качеством, а не строительством полосы препятствий.

Давайте посмотрим, как устроена простая защита и как ее обходят хакеры. Если вы программист и разрабатываете собственные продукты под грифом Shareware, то эти рекомендации могут вам пригодиться.

4.10.2. Срок службы

Простейший способ заставить программу работать — продлить ее срок службы. Как я уже говорил *(см. разд. 4.10.1)*, защита Shareware-программ чаще всего примитивна и в основном строится на счетчике запусков или на количестве используемых дней. Второе предпочтительней. Почему? Сейчас объясню.

Разработчики очень часто допускают ошибку при проверке даты. При установке программы в реестр (или другое место хранения) записывается текущая дата, а при запуске проверяется, не превышает ли текущая дата параметр установки плюс определенное число дней? Если условие выполняется, то лимит вышел. Вот тут и есть скрытая ошибка. Переведите системную дату в компьютере на 01.01.2018 года и установите программу. Затем верните календарь в нормальное положение, и используйте софт в течение 10 лет (теперь программа будет работать до 01.01.2018 плюс разрешенное число дней). За это время она просто устареет, а ее возможности могут больше не понадобиться, ведь технологии меняются за несколько лет.

Жаль, что такую ошибку допускают только начинающие программисты. Профессионалы в специализирующихся на Shareware-программах фирмах уже давно придумали более эффективные методы проверки периода работы программы. Тут уже простым переводом часов не обойтись.

4.10.3. Накручивание счетчика

Если вы столкнулись со счетчиком запусков программы, то попробуйте другой способ — "мониторинг реестра". Для этого вам понадобится зайти на сайт **http://www.sysinternals.com/**. Здесь, в разделе **Процессы и потоки**, есть программа Regmon, которая доступна для свободного скачивания.

Компанию Sysinternals организовал знаменитый специалист по "внутренностям" ОС Windows — Марк Руссинович (Mark Russinovich) вместе с Брайсом Когсвеллом

(Bryce Cogswell). С недавних пор Марк работает в Microsoft, и поэтому не удивляйтесь, если сайт **sysinternals.com** приведет вас на сайт этой компании в раздел (**http://technet.microsoft.com/en-us/sysinternals**). Я так понимаю, Microsoft купила Sysinternals.

Давайте разберем работу с Regmon на примере накрутки счетчика программы, которая уже закрыта и не распространяется. Не будем останавливаться на названии и производителе, чтобы не испортить его продажи.

Надо запустить по очереди программу Regmon, а потом взламываемую программу. В окне Regmon появятся все события, связанные с обращением к реестру:

- **Time** — время;
- **Process** — программа, обратившаяся к реестру;
- **PID** — идентификатор процесса;
- **Path** — путь;
- **Operation** — операция;
- **Path** — путь к реестру/файлу или объекту.
- **Result** — результат.

> ***Примечание***
>
> С недавних пор эту программу убрали с сайта, и теперь ее заменила ProcessMonitor (рис. 4.23).

Самое первое, что нужно поискать — строки, в которых поле **Process** равно `deskt` (это имя запускаемого файла) и поле **Request** равно `SetValueEx`.

В момент запуска программы считывают настройки и параметры, а `SetValueEx` означает запись в реестр. Так что же можно записать во время загрузки? Только счетчик. Если хорошо посмотреть на рис. 4.23, то сообщение под номером 1435 соответствует поставленному условию. Обратите внимание на поле **Other**. Там стоит значение `18`, которое пишется в реестр. Запись происходит по адресу: **HKEY_CURRENT_USER\Software\Desktop\ProductID**.

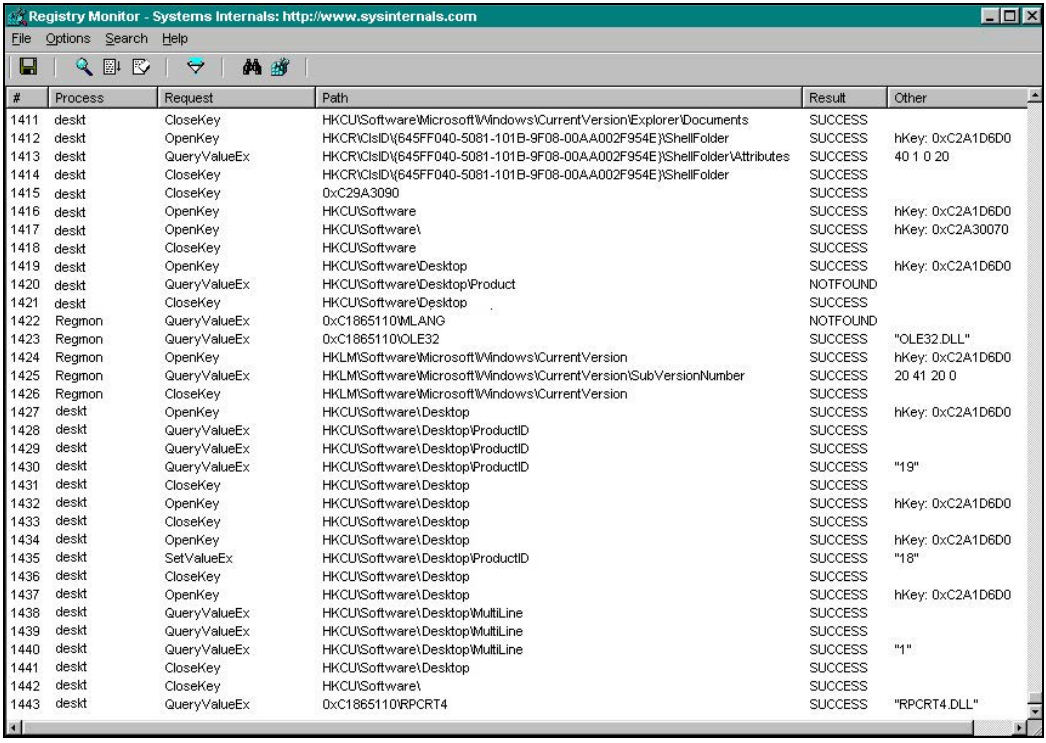
Теперь посмотрите немного выше (номер 1430). По этому же адресу происходило чтение параметра, значение которого оказалось равным `19`. Это говорит о том, что счетчик работает в обратном порядке, и когда он достигнет нуля (может и отрицательного значения), программа перестанет запускаться. Теперь вы сможете спокойно вернуть программу к жизни, вручную изменив этот счетчик. Попробуйте сразу увеличить его до 10 000, некоторые программы могут это прозевать. Если счетчик работает на увеличение (например, до 100), то можно поставить там значение –10 000 и тогда надоест ждать, когда наступит предел.

Точно так же корректируются и даты. Например, можно поправить один параметр в реестре для старых версий программы The Bat! так, что она будет работать бесконечно, показывая, что у вас осталось –5000 дней.

Если у вас возникли проблемы с мониторингом, то чтобы не переустанавливать программу, можете просто попробовать удалить из реестра все значения, связанные

с ней, очень часто это помогает. Пробный период может начаться заново, и вы продлите жизнь программы еще на 30 дней (или сколько дает программа).

Если используется счетчик запусков, а не дата, то можно сделать даже проще. После установки программы начальные параметры запишутся в реестр. Запустите regedit и найдите эти параметры в строке **HKEY_CURRENT_USER\Software** плюс имя фирмы или программы. Выделите раздел и экспортируйте его в файл. Когда закончится лимит запусков, просто выполните импорт этого файла, и все настройки вернутся в начальное состояние, так что можно будет снова и снова использовать любимую утилиту.



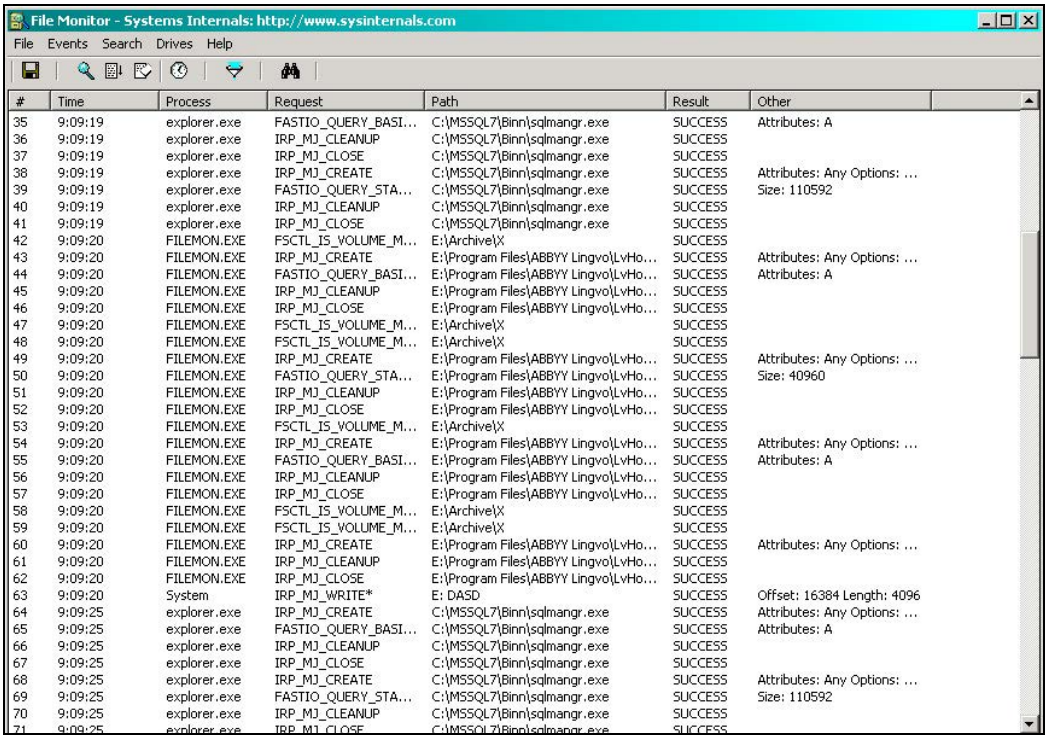
#	Process	Request	Path	Result	Other
1411	deskt	CloseKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Documents	SUCCESS	
1412	deskt	OpenKey	HKCR\CLSID\{645FF040-5081-101B-9F08-00AA002F954E}\ShellFolder	SUCCESS	hKey: 0xC2A1D6D0
1413	deskt	QueryValueEx	HKCR\CLSID\{645FF040-5081-101B-9F08-00AA002F954E}\ShellFolder\Attributes	SUCCESS	40 1 0 20
1414	deskt	CloseKey	HKCR\CLSID\{645FF040-5081-101B-9F08-00AA002F954E}\ShellFolder	SUCCESS	
1415	deskt	CloseKey	0xC29A3090	SUCCESS	
1416	deskt	OpenKey	HKCU\Software	SUCCESS	hKey: 0xC2A1D6D0
1417	deskt	OpenKey	HKCU\Software\	SUCCESS	hKey: 0xC2A30070
1418	deskt	CloseKey	HKCU\Software	SUCCESS	
1419	deskt	OpenKey	HKCU\Software\Desktop	SUCCESS	hKey: 0xC2A1D6D0
1420	deskt	QueryValueEx	HKCU\Software\Desktop\Product	NOTFOUND	
1421	deskt	CloseKey	HKCU\Software\Desktop	SUCCESS	
1422	Regmon	QueryValueEx	0xC1865110\MLANG	NOTFOUND	
1423	Regmon	QueryValueEx	0xC1865110\OLE32	SUCCESS	"OLE32.DLL"
1424	Regmon	OpenKey	HKLM\Software\Microsoft\Windows\CurrentVersion	SUCCESS	hKey: 0xC2A1D6D0
1425	Regmon	QueryValueEx	HKLM\Software\Microsoft\Windows\CurrentVersion\SubVersionNumber	SUCCESS	20 41 20 0
1426	Regmon	CloseKey	HKLM\Software\Microsoft\Windows\CurrentVersion	SUCCESS	
1427	deskt	OpenKey	HKCU\Software\Desktop	SUCCESS	hKey: 0xC2A1D6D0
1428	deskt	QueryValueEx	HKCU\Software\Desktop\ProductID	SUCCESS	
1429	deskt	QueryValueEx	HKCU\Software\Desktop\ProductID	SUCCESS	
1430	deskt	QueryValueEx	HKCU\Software\Desktop\ProductID	SUCCESS	"19"
1431	deskt	CloseKey	HKCU\Software\Desktop	SUCCESS	
1432	deskt	OpenKey	HKCU\Software\Desktop	SUCCESS	hKey: 0xC2A1D6D0
1433	deskt	CloseKey	HKCU\Software\Desktop	SUCCESS	
1434	deskt	OpenKey	HKCU\Software\Desktop	SUCCESS	hKey: 0xC2A1D6D0
1435	deskt	SetValueEx	HKCU\Software\Desktop\ProductID	SUCCESS	"18"
1436	deskt	CloseKey	HKCU\Software\Desktop	SUCCESS	
1437	deskt	OpenKey	HKCU\Software\Desktop	SUCCESS	hKey: 0xC2A1D6D0
1438	deskt	QueryValueEx	HKCU\Software\Desktop\MultiLine	SUCCESS	
1439	deskt	QueryValueEx	HKCU\Software\Desktop\MultiLine	SUCCESS	
1440	deskt	QueryValueEx	HKCU\Software\Desktop\MultiLine	SUCCESS	"1"
1441	deskt	CloseKey	HKCU\Software\Desktop	SUCCESS	
1442	deskt	CloseKey	HKCU\Software\	SUCCESS	
1443	deskt	QueryValueEx	0xC1865110\RPCRT4	SUCCESS	"RPCRT4.DLL"

Рис. 4.23. Окно программы Regmon

Почему мы говорим только о реестре? Да потому, что это самый распространенный и очень удобный способ сохранить параметры приложений. Но этот метод не единственный. Некоторые современные и большинство старых программ используют для сохранения простые файлы.

Для решения этой проблемы отправляемся по уже знакомому адресу **http://www.sysinternals.com/** и скачиваем программу File Monitor (в том же разделе **Процессы и потоки**). Эта утилита предназначена для мониторинга обращений к файлам.

С File Monitor можно работать абсолютно так же, как и с Regmon, только здесь вы можете отслеживать обращения к файлам, чтение и запись различных параметров (рис. 4.24).



#	Time	Process	Request	Path	Result	Other
35	9:09:19	explorer.exe	FASTIO_QUERY_BASI...	C:\MSSQL7\Binn\sqlmangr.exe	SUCCESS	Attributes: A
36	9:09:19	explorer.exe	IRP_MJ_CLEANUP	C:\MSSQL7\Binn\sqlmangr.exe	SUCCESS	
37	9:09:19	explorer.exe	IRP_MJ_CLOSE	C:\MSSQL7\Binn\sqlmangr.exe	SUCCESS	
38	9:09:19	explorer.exe	IRP_MJ_CREATE	C:\MSSQL7\Binn\sqlmangr.exe	SUCCESS	Attributes: Any Options: ...
39	9:09:19	explorer.exe	FASTIO_QUERY_STA...	C:\MSSQL7\Binn\sqlmangr.exe	SUCCESS	Size: 110592
40	9:09:19	explorer.exe	IRP_MJ_CLEANUP	C:\MSSQL7\Binn\sqlmangr.exe	SUCCESS	
41	9:09:19	explorer.exe	IRP_MJ_CLOSE	C:\MSSQL7\Binn\sqlmangr.exe	SUCCESS	
42	9:09:20	FILEMON.EXE	FSCTL_IS_VOLUME_M...	E:\Archive\X	SUCCESS	
43	9:09:20	FILEMON.EXE	IRP_MJ_CREATE	E:\Program Files\ABBYY Lingvo\LvHo...	SUCCESS	Attributes: Any Options: ...
44	9:09:20	FILEMON.EXE	FASTIO_QUERY_BASI...	E:\Program Files\ABBYY Lingvo\LvHo...	SUCCESS	Attributes: A
45	9:09:20	FILEMON.EXE	IRP_MJ_CLEANUP	E:\Program Files\ABBYY Lingvo\LvHo...	SUCCESS	
46	9:09:20	FILEMON.EXE	IRP_MJ_CLOSE	E:\Program Files\ABBYY Lingvo\LvHo...	SUCCESS	
47	9:09:20	FILEMON.EXE	FSCTL_IS_VOLUME_M...	E:\Archive\X	SUCCESS	
48	9:09:20	FILEMON.EXE	FSCTL_IS_VOLUME_M...	E:\Archive\X	SUCCESS	
49	9:09:20	FILEMON.EXE	IRP_MJ_CREATE	E:\Program Files\ABBYY Lingvo\LvHo...	SUCCESS	Attributes: Any Options: ...
50	9:09:20	FILEMON.EXE	FASTIO_QUERY_STA...	E:\Program Files\ABBYY Lingvo\LvHo...	SUCCESS	Size: 40960
51	9:09:20	FILEMON.EXE	IRP_MJ_CLEANUP	E:\Program Files\ABBYY Lingvo\LvHo...	SUCCESS	
52	9:09:20	FILEMON.EXE	IRP_MJ_CLOSE	E:\Program Files\ABBYY Lingvo\LvHo...	SUCCESS	
53	9:09:20	FILEMON.EXE	FSCTL_IS_VOLUME_M...	E:\Archive\X	SUCCESS	
54	9:09:20	FILEMON.EXE	IRP_MJ_CREATE	E:\Program Files\ABBYY Lingvo\LvHo...	SUCCESS	Attributes: Any Options: ...
55	9:09:20	FILEMON.EXE	FASTIO_QUERY_BASI...	E:\Program Files\ABBYY Lingvo\LvHo...	SUCCESS	Attributes: A
56	9:09:20	FILEMON.EXE	IRP_MJ_CLEANUP	E:\Program Files\ABBYY Lingvo\LvHo...	SUCCESS	
57	9:09:20	FILEMON.EXE	IRP_MJ_CLOSE	E:\Program Files\ABBYY Lingvo\LvHo...	SUCCESS	
58	9:09:20	FILEMON.EXE	FSCTL_IS_VOLUME_M...	E:\Archive\X	SUCCESS	
59	9:09:20	FILEMON.EXE	FSCTL_IS_VOLUME_M...	E:\Archive\X	SUCCESS	
60	9:09:20	FILEMON.EXE	IRP_MJ_CREATE	E:\Program Files\ABBYY Lingvo\LvHo...	SUCCESS	Attributes: Any Options: ...
61	9:09:20	FILEMON.EXE	IRP_MJ_CLEANUP	E:\Program Files\ABBYY Lingvo\LvHo...	SUCCESS	
62	9:09:20	FILEMON.EXE	IRP_MJ_CLOSE	E:\Program Files\ABBYY Lingvo\LvHo...	SUCCESS	
63	9:09:20	System	IRP_MJ_WRITE*	E: DASD	SUCCESS	Offset: 16384 Length: 4096
64	9:09:25	explorer.exe	IRP_MJ_CREATE	C:\MSSQL7\Binn\sqlmangr.exe	SUCCESS	Attributes: Any Options: ...
65	9:09:25	explorer.exe	FASTIO_QUERY_BASI...	C:\MSSQL7\Binn\sqlmangr.exe	SUCCESS	Attributes: A
66	9:09:25	explorer.exe	IRP_MJ_CLEANUP	C:\MSSQL7\Binn\sqlmangr.exe	SUCCESS	
67	9:09:25	explorer.exe	IRP_MJ_CLOSE	C:\MSSQL7\Binn\sqlmangr.exe	SUCCESS	
68	9:09:25	explorer.exe	IRP_MJ_CREATE	C:\MSSQL7\Binn\sqlmangr.exe	SUCCESS	Attributes: Any Options: ...
69	9:09:25	explorer.exe	FASTIO_QUERY_STA...	C:\MSSQL7\Binn\sqlmangr.exe	SUCCESS	Size: 110592
70	9:09:25	explorer.exe	IRP_MJ_CLEANUP	C:\MSSQL7\Binn\sqlmangr.exe	SUCCESS	
71	9:09:25	explorer.exe	IRP_MJ_CLOSE	C:\MSSQL7\Binn\sqlmangr.exe	SUCCESS	

Рис. 4.24. Окно программы File Monitor

Напоследок хочу обратить ваше внимание, что запись счетчика может происходить не только при старте, но и при выходе из программы. Счетчики дат вообще могут не изменяться, но их тоже можно попытаться вычислить.

Я показал пример с использованием старых утилит, сейчас же RegMon и FileMon удалены с сайта. Они были объединены в одну большую утилиту Process Monitor. Эта программа может следить сразу за всем — изменениями в файлах и реестре одновременно.

4.10.4. Полный взлом

Если вы хотите избавиться от всех предупреждений о регистрации, создав видимость, что вы это сделали, и получить все возможности программы, тут уже без дизассемблера, ассемблера и машинных кодов не обойтись.

Дизассемблер — программа, превращающая машинные коды в более удобный вид (язык ассемблера). Для понимания команд ассемблера нужно уметь программировать, но для взлома простой защиты можно обойтись и без этого.

Мы не будем углубляться и рассмотрим только основные моменты, но этого будет достаточно для опытного программиста, чтобы проникнуть в программы достаточно большой сложности. А если вы являетесь пользователем, то сможете преодолеть простейшую защиту, и ничего более.

Итак, для работы нам понадобятся следующие инструменты:

- W32Dasm — желательно не ниже версии 8.9;
- Turbo Debugger от фирмы Borland — идет со средами разработки. Лучше всего использовать DOS-вариант, который поставляется со старыми языками программирования этой фирмы типа Borland C++ 5.02;
- DiskEditor — можно любой вариант, но я люблю от "дяди Нортона". Утилиты этой фирмы сейчас принадлежат компании Symantec (**http://www.symantec.ru/**).

Меньше слов, больше дела. Запустите программу W32Dasm. Выберите из меню **Disassembler** (Дизассемблер) пункт **Open file to Disassemble** (Открыть файл для дизассемблирования). Откройте необходимый exe-файл. Я опять возьму ту же программу, что и в *разд. 4.10.3*. Во время загрузки происходит превращение машинных команд в язык ассемблера, и на экране появляется код программы, который может прочитать только программист.

Теперь переходим к самому взлому. Для начала нужно попробовать найти коды. Для этого выберите меню **Search | Find Text**. Введите слово `Regist` и запустите поиск. Когда подобный контекст будет найден, просмотрите список результатов. Если не видите ничего интересного, то продолжайте поиск. Вы должны обнаружить текст, связанный с регистрацией, например, сообщение об удачно введенном коде.

Посмотрите на рис. 4.25, на котором показан снимок результата моего поиска. W32Dasm нашел текст "Enter registration code". Я думаю, это то, что надо. Программисты, знающие язык ассемблера, могут просмотреть команды. Если с этим у вас проблемы, то исследуйте строки, начинающиеся с символа `*` (звездочка).

Итак, начинаем по программе отыскивать такие звездочки. Следующая строка абсолютно ничего не говорит. Опускаясь еще ниже, можно увидеть текст:

```
* Possible StringData Ref from Code Obj ->"EGCD1"
```

Даже не зная программирования, можно догадаться, что введенный код будет сравниваться с "EGCD1". Это логично, потому что мы сначала нашли сообщение "Введите регистрационный код", и тут же группа непонятных символов. Что мешает проверить эту строку, как регистрационный код?

Ну а если вы знаете программирование, то по коду сможете узнать, что первые 5 символов введенного ключа должны быть "EGCD1", а остальные могут быть любыми.

Это идеальный вариант, когда происходит простое сравнение. Хуже, когда используется математика, тогда уже нужен большой опыт. Но давайте посмотрим немного дальше. Вы найдете следующие строки "Software", "Desktop" и "ProductID". Мне это напоминает ключи реестра, с которыми мы уже встречались при мониторинге с помощью программы Regmon: **Software\Desktop** — путь в реестре, а `ProductID` — строковый параметр. Почему строковый? Да потому, что еще ниже я нашел комбинацию символов "sdjFE2fih3erj3J". Это значит, что если такая строка есть в реестре, то программа считается зарегистрированной. Вот так. Даже если для проверки кода используется математика, вы сможете ее обойти, отыскав что-нибудь подобное.

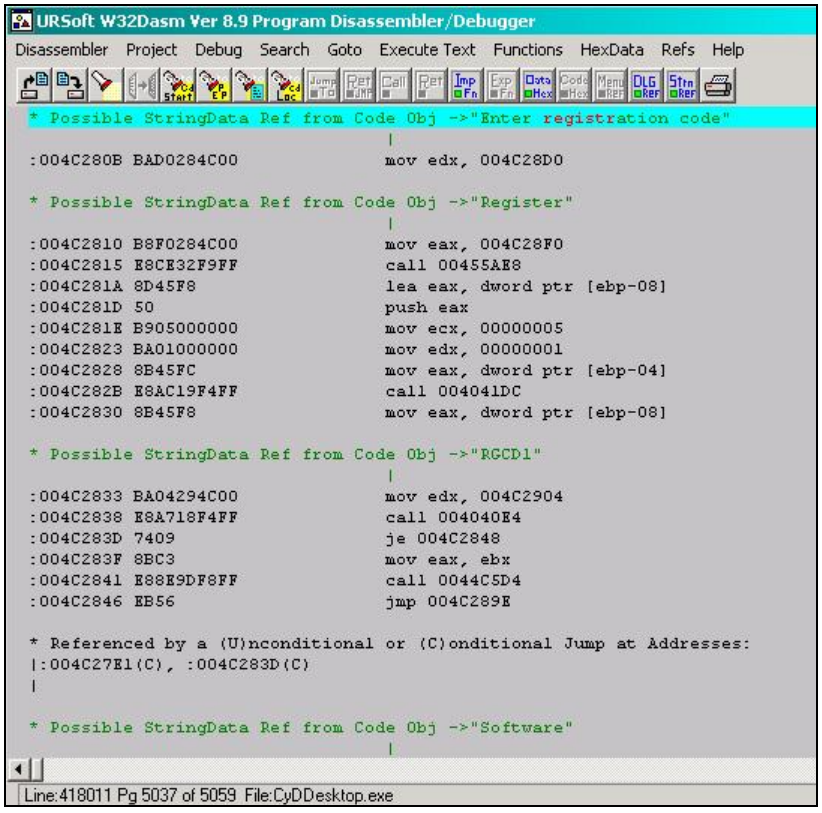


Рис. 4.25. Окно программы W32Dasm

Это все элементарные варианты защиты. Однако, несмотря на простоту, они используются очень часто.

4.10.5. *Сложный взлом*

Если вы ничего не нашли, то тут уже без средств отладки не обойтись. Придется запускать Turbo Debugger (или другую программу, но мне нравится именно эта) и искать регистрацию, отлаживая программу.

Я не буду тут вдаваться в подробности, а дам пару советов для программистов:

- Попробуйте поискать все вызовы функций `MessageBoxA`. Чаще всего рядом с программным кодом регистрации будет хотя бы один вызов этой функции, в основном, для сообщения об удачном завершении процесса.
- Ищите последовательность кодов выхода из программы. Посмотрите, откуда они вызываются. Если программа выработала свой ресурс, то она не запустится, а значит, где-то должен быть принудительный вызов закрытия. Когда найдете, поднимитесь немного выше и поищите команду перехода. Она обязательно должна быть, потому что всегда используется алгоритм типа "Если программа не зарегистрирована, то перейти на выход, иначе работать дальше". Ваша зада-

ча — заменить условный переход на безусловный (`jmp`) по адресу продолжения выполнения программы.

Контроль регистрации может быть сколь угодно сложным, но практически всегда он заканчивается простой проверкой типа "если регистрация прошла успешно, то продолжить выполнение, иначе — выйти".

Около 10 лет назад я купил игру. Регистрационный код, который был на коробке, почему-то не подошел, а дело было вечером, и в службу поддержки звонить поздно. Поиграть очень хотелось, поэтому, недолго думая, я запустил отладчик. Проглядев код, который проверял регистрацию, я ничего не понял. Ассемблер я тогда знал на уровне основных команд и понять алгоритм проверки не смог. Просмотрев код дальше, я увидел заветную проверку `cmp` и условный переход на продолжение игры. Задача состояла в том, чтобы заменить условный переход на безусловный. На это понадобилось пять минут.

Таким образом, я взломал свою первую и единственную программу, хотя и заплатил за нее положенные деньги. На следующий день я узнал, как регистрировать игру, но несмотря на это пользовался измененным исполняемым файлом, потому что не хотелось каждый раз вводить ключ. Я заплатил деньги не для того, чтобы мучиться с кодами, а чтобы спокойно играть.

Хочу обратить ваше внимание, что я не старался научить вас взламывать все подряд и не призываю к этому. Если вы пользуетесь плодами чужого труда, значит, он стоит того, чтобы за него заплатить. Некоторые жалуются на очень высокие цены на программное обеспечение. Если вас что-то не устраивает, всегда есть альтернатива. На данный момент очень много свободных и дешевых программ. Воспользуйтесь тем, что вам по карману, но не взламывайте. Цель данной главы — только показать, как взламываются программы, но применять это в корыстных целях незаконно.

Несколько лет назад я решил отказаться от нелегального софта на собственном компьютере. И вы знаете, я это сделал без проблем. Нужно было только удалить все, чем я не пользуюсь. Из оставшегося я убрал все, что дорого для моего кармана, и нашел этому бесплатную альтернативу. Все, на что хватает денег, я купил и теперь сплю спокойно. У меня в компьютере сейчас осталась только одна платная и дорогая программа, которой не нашлось альтернативы, но скоро накоплю денег и буду пользоваться ею уже легально.

ГЛАВА 5

Интернет для хакера

В этой главе нам предстоит взглянуть на Интернет с точки зрения хакеров. Нет, мы не будем взламывать сайты и воровать информацию, потому что это темы отдельных книг. Про взлом сайтов можно прочитать, например, в книге "Web-сервер глазами хакера" [6]. А вот про воровство информации хорошо написано в Уголовном кодексе Российской Федерации :).

Мы же с вами законопослушные граждане. Вместо этого мы поговорим о безопасности домашнего компьютера. Основной упор будет сделан именно на этот способ организации трудового процесса. С серверами и корпоративными сетями дело обстоит сложнее, но все, о чем мы будем говорить, в равной степени применимо и к коллективной работе.

Кроме того, мы пополним свой багаж замечательными шутками, но уже с использованием Интернета, или просто поучимся, как сделать более комфортным свое пребывание в сети. Мы узнаем, как накручиваются системы голосования и обманываются системы регистрации.

Всю описываемую здесь информацию вы должны рассматривать с двух точек зрения: с целью использования и с целью защиты. Например, мы будем рассматривать, как организованы системы голосования на различных сайтах, и эту информацию можно использовать с целью увеличения голосов. Но если вы веб-программист, то эта информация будет полезна с точки зрения защиты и поможет написать такой скрипт для подсчета голосов, который нельзя (труднее) будет подтасовать.

Когда рассматриваешь систему безопасности, то эта же информация может быть использована для взлома. Например, вы рассказываете о новом замке, вскрыть который можно только бензопилой. С одной стороны, вы хвастаетесь надежной конструкцией, а с другой — даете вору информацию, какой инструмент использовать для проникновения. Любая информация о защите может быть воспринята и как побуждение к взлому, и как мера предосторожности. Я подразумеваю второе, потому что намного сложнее создать нечто неуязвимое, чем разрушить построенное (ломать — не строить). Да и мне интереснее защищать информацию, чем взламывать. Взломом интересуюсь для того, чтобы я знал, от чего я должен защищаться.

Любые сведения о хакерских методах будут полезны программистам и администраторам для организации усиления обороны. Вы не сможете защититься, если не знаете, откуда исходит угроза. С другой стороны, вы должны понимать, как устроен и как работает объект ваших шуток (или взлома). Без понимания таких вещей невозможно организовать ни нападение, ни достойную оборону.

5.1. Форсирование Интернета

Когда мы находимся в Сети, хочется оптимизировать там свое пребывание. Если работа происходит по телефонной линии (dial-up), то скорость обмена информацией невысокая (на современных модемах составляет самое большее 56 Кбит/с). Этот предел достигается очень редко, а бóльшую часть времени мы имеем скорость от 30 до 40 Кбит/с, и то при условии эффективной работы протокола и хорошей линии связи.

При работе по выделенной линии, через DSL или сетевое подключение максимум достигается намного проще, и даже если у вас канал в 64 Кбит/с, что незначительно больше потенциальных 56 Кбит/с простого модема, увеличение скорости будет ощутимым. Но если при доступе через телефонную линию вы чаще всего платите за время пребывания в сети, то при выделенном канале платеж зачастую зависит от количества скачанной информации, и здесь уже хочется оптимизировать поступающий трафик.

Проблема любого соединения в том, что оно может разорваться или сервер может зависнуть, и данные не будут поступать. Если вы в этот момент загружаете вебстраничку, то не так обидно прочитать ее снова после восстановления соединения. Но если к этому времени уже было получено 90% из 100 Мбайт очередного обновления Windows, то скачивать заново информацию такого объема досадно. Чтобы не терять лишнее время и трафик, можно воспользоваться менеджерами закачки типа GetRight или Reget. Но о них мы поговорим в *разд. 5.1.5*. Дополнительную информацию о программах GetRight и Reget и используемых ими технологиях можно прочитать на официальных сайтах **http://www.getright.com/** и **http://www.reget.com/**. Сайт программы GetRight можно увидеть на рис. 5.1.

Мы рассмотрим различные способы повышения производительности, которые способствуют увеличению скорости обмена информацией и уменьшению трафика.

Что не может не радовать, т. к. это быстрое распространение неограниченного и скоростного Интернета. Если еще пару лет назад я мечтал о скорости в 256 Кбит/с, то сейчас в Москве и в Санкт-Петербурге стали распространены подключения к Интернету всего за 100—200 рублей в месяц на скорости 1 Мбит/с и даже более, и при этом трафик никак не ограничен. Вот это счастье!

В 2009 г., когда я уезжал из России, мой провайдер предлагал за 600 руб. скосроть до 10 Мбит/с без ограничений. Сейчас я подключен к сети на скорости 12 Мбит/с у канадского провайдера, а больше и не нужно. Когда работаешь с сетью, далеко не всегда можно получить и 5 Мбит/с. Веб-страницы грузятся и так дочтаточно быстро, потому что они в большинстве случаев не более мегабайта. Реальную скорость

можно ощутить, когда качаешь большие файлы. Но и тут далеко не каждый сервер способен отдавать файлы на скорости 10 Мбит/с и более.

При наличии таких скоростей надобность в программах, позволяющих докачивать информацию, начинает пропадать, и они теряют в популяности. Но пока еще не все подключены к сети по высокоскоростным каналам. Еще очень много людей, которые работают по телефонным соединениям (dial-up или ADSL), особенно за пределами Москвы и Санкт-Петербурга.

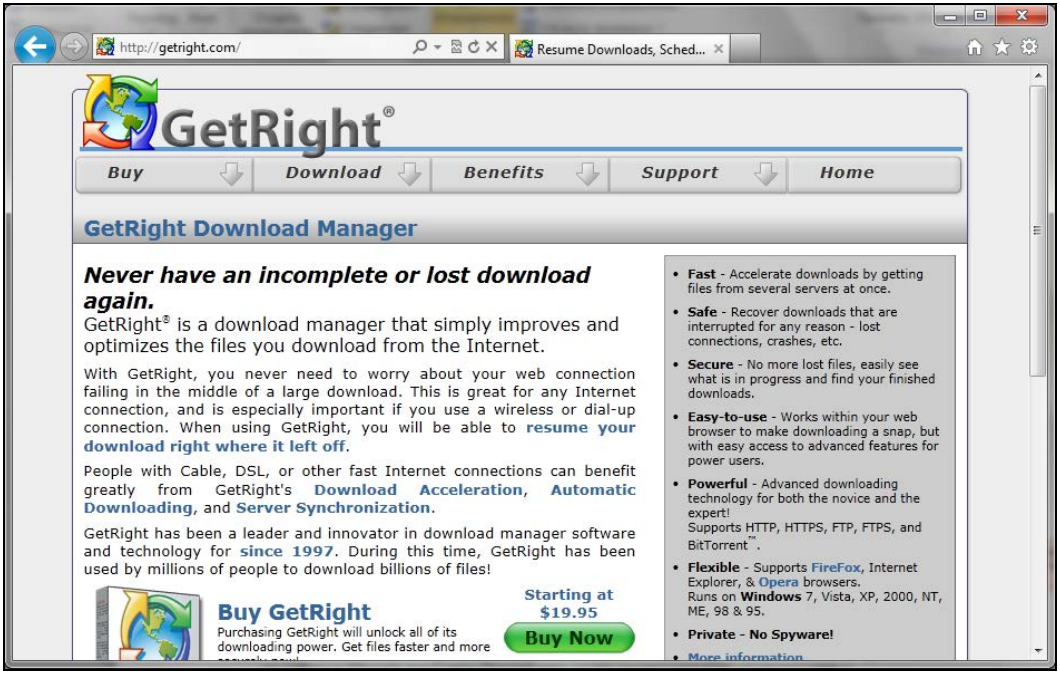


Рис. 5.1. Сайт разработчиков программы GetRight

5.1.1. Форсирование протокола

В основе обмена информацией лежит использование специальных протоколов, а самым распространенным стал TCP/IP (Transmission Control Protocol/Internet Protocol, протокол управления передачей/межсетевой протокол). Мы не будем углубляться в технические дебри, но некоторые теоретические основы придется рассмотреть.

Протокол TCP/IP определяет стандарты связи между компьютерами и соглашения о формате передаваемых данных. Обмен происходит с помощью пакетов определенного размера, который зависит от настроек, установленных в ОС. Помимо данных в каждом пакете присутствует служебная информация: адреса получателя и отправителя, сведения о портах, времени жизни пакета и т. д.

Допустим, что пакет имеет максимальный размер 2000 байт. Если отправлять данные по 1000 байт или даже по 500 байт, то величина пакета будет использоваться

не в полную силу. А если дожидаться окончания его заполнения, то неизбежны задержки. Но мы не можем сильно влиять на этот процесс, поэтому регулирование должно происходить на уровне размера.

Если послать сразу 10 000 байт, то эта информация будет разбита на несколько пакетов размером по 2000 байт и отправлена в сеть с предельным заполнением. Информация пройдет быстро, и на стороне получателя все пакеты будут собраны. Но сеть не идеальна, и если какая-то порция затеряется и не дойдет до адресата, то для завершения сборки последует запрос на повторную отправку, а это лишние затраты времени и трафика.

Если уменьшить допустимый размер пакета, то небольшой объем информации будет происходить более эффективно, а значительные потоки данных (передача крупных файлов) окажутся наиболее затратными, потому что для отправки потребуется больше пакетов. А т. к. каждый из них содержит служебную информацию, то получится слишком много вспомогательного трафика. Это опять же дополнительное время и трафик.

Настроек, влияющих на параметры соединения, достаточно много, но давайте разберем их в процессе изучения тех параметров, которые можно контролировать в Windows. По мере рассмотрения будем знакомиться с теорией, которая необходима для выбора правильного значения.

В Windows 7 протокол TCP/IP работает достаточно быстро, и если вы являетесь счастливым обладателем такой версии, то настройки реестра, описанные в этом разделе, можно прочитать для расширения кругозора.

5.1.2. Форсирование DNS

Каждый раз, когда вы хотите загрузить в Internet Explorer некий сайт, то в качестве адреса чаще всего используете имя сервера. Например, пусть вам необходимо скачать новую версию программы с сайта CyD Software Labs. Для этого в строке URL вы указываете адрес **http://www.cydsoft.com/** и начинаете загрузку. Но реальный адрес компьютера — это не символьное имя, а IP-адрес, который состоит из четырех чисел (для самой распространенной сейчас 4-й версии IP-протокола), разделенных точками.

Так вот, перед чтением сайта Internet Explorer сначала должен определить IP-адрес сервера, символьное имя которого вы указали. Для этого компьютер посылает запрос DNS-серверу с просьбой сообщить ему соответствующий IP. Только после получения ответа начинается реальная загрузка страницы и ее содержимого по сети. Процесс идентификации может занять некоторое время, поэтому пауза может быть ощутимой даже на глаз.

Зачем нужен DNS? Запомнить числовой IP-адрес не всегда легко, поэтому логичнее использовать названия, которые ассоциируются с содержащейся на сайте информацией и его направленностью. Понятные словосочетания запоминаются намного быстрее, и именно для этого была придумана система DNS-преобразования текстовых имен серверов в IP-адреса.

Когда вы собираетесь посетить новый сайт, то использование DNS практически всегда обязательно, но если на каких-либо страничках вы бываете достаточно часто или даже ежедневно, то необходимо отказаться от услуг DNS.

Большинство серверов в сети очень редко меняют свои IP-адреса. Частая смена происходит только на подпольных сайтах с запрещенной информацией, когда владельцы пытаются спрятаться от правосудия. Официальные и вполне легальные сайты годами не нуждаются в изменении адреса. Именно поэтому в таких случаях желательно снизить количество лишних обращений к сети и нежелательных задержек.

У меня все сайты в папке Favorities (Избранное) не используют символьные URL, а везде стоит IP-адресация. Таким образом, после выбора любимого сайта загрузка начинается моментально, минуя определение адреса сервера по его символьному имени.

Как настроить такую адресацию? Для этого нужно выполнить несколько простых шагов:

1. Запустите Internet Explorer.
2. Откройте меню **Избранное** (Favorites) и наведите указатель мыши на ссылку нужного сайта. Щелкните по нему правой кнопкой мыши и в появившемся меню выберите пункт **Свойства** (Properties).
3. Перед вами откроется окно, как на рис. 5.2. В нем на вкладке **Документ Интернета** (Web Document) необходимо запомнить часть адреса в поле **URL-адрес** (URL), которая находится между двойным и одинарным слэшами (наклонными чертами). Например, на рис. 5.2 показан адрес сайта **http://www.cydsoft.com/**, и нас будет интересовать **www.cydsoft.com**.
4. Выберите меню **Пуск** (Start), в поле поиска наберите команду `cmd` и нажмите клавишу <Enter>. Тем самым вы откроете окно, в котором можно выполнять директивы.

   Наберите `ping` *`ИмяСайта`* (например, `ping www.cydsoft.com`), и вы должны увидеть текст типа:

```
Pinging www.cydsoft.com [62.118.251.15]  with 32 bytes of data:
Reply from 62.118.251.15: bytes=32 time<1ms TTL=128
Reply from 62.118.251.15: bytes=32 time=2ms TTL=128
Reply from 62.118.251.15: bytes=32 time=1ms TTL=128
Reply from 62.118.251.15: bytes=32 time<1ms TTL=128
Ping statistics for 62.118.251.15:
  Packets: Send = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
  Minimum = 0ms, Maximum = 2ms, Average = 1ms
```

   В первой строке ответа в квадратных скобках показан IP-адрес. Именно на него вы должны изменить адрес **www.cydsoft.com** в окне свойств ярлыка (см. рис. 5.2). Таким образом, URL превратится в **http://62.118.251.15/** (IP-адрес может меняться). Но прежде чем изменять, я советую протестировать адрес в браузере. Если произошла ошибка, то, возможно, есть какая-то переадресация

(сайт не имеет выделенного IP-адреса) или вы работаете через прокси-сервер, который не смог пропустить IP-адрес (я и с таким встречался).

Если во время выполнения команды `ping` произошла ошибка, то это может быть связано с недоступностью этой директивы в вашей сети. Такое бывает в корпоративных сетях, где для выхода в Интернет разрешены только определенные протоколы и нет возможности использовать ICMP-протокол, необходимый программе ping. В этом случае можно воспользоваться сайтом **http://www.wservice.info/**, на котором можно выбрать пункт **Пинг хоста**, ввести адрес в единственное поле и нажать клавишу <Enter> или кнопку **Выполнить**. Можно также найти другие сайты, предоставляющие такие же услуги, набрав в любимом поисковике что-нибудь вроде "ping online".

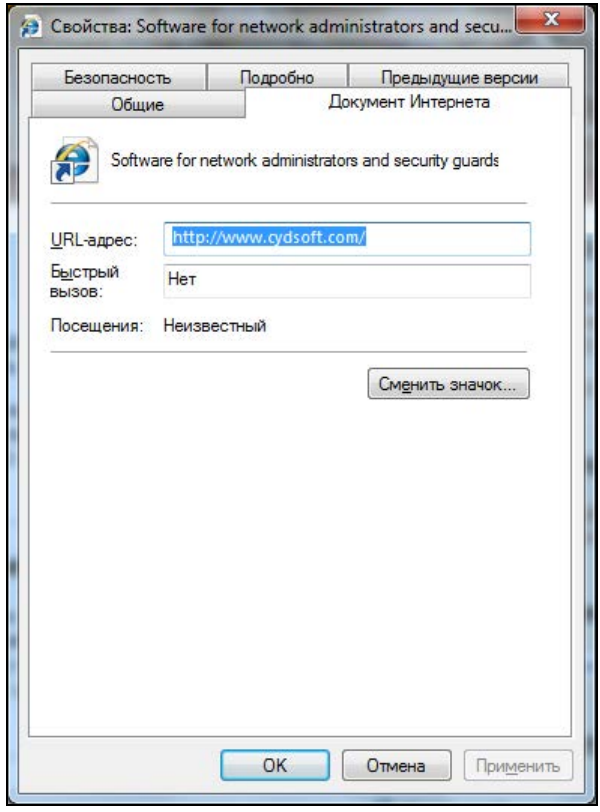


Рис. 5.2. Окно свойств ярлыка

Еще один способ работать с DNS — использование утилиты nslookup. В меню **Start** (Пуск) в строке поиска введите имя этой команды. После запуска утилиты на черном экране консоли появятся две строки:

```
Default Server: Name
Address: 127.0.0.1
```

В первой строке можно увидить имя DNS-сервера, используемого по умолчанию, а во второй строке его IP-адрес. Чуть ниже должен быть символ приглашения для

ввода команд в виде угловой скобки >. Команда определения адреса для домена проста — просто введите имя домена и нажмите клавишу <Enter>. Например:

```
> cydsoft.com
```

Символ > вводить не нужно, он уже отображается на экране. В ответ на это вы увидите IP-адрес данного домена, и его можно использовать в закладках.

Кстати, эта утилита очень удобна для тестирования работы сервера DNS, потому что показывает адрес сервера, который установлен по умолчанию. Далее можно проверить его доступность с помощью утилиты ping.

5.1.3. Локальное кэширование

В Internet Explorer встроена система кэширования, которая позволяет не загружать некоторую информацию при повторном входе на сайт, а брать ее из кэша браузера. Чаще всего не подлежат вторичной загрузке картинки. Так как их объем (в байтах) обычно намного превышает объем текстовой информации сайта, происходит большая экономия трафика и повышение скорости получения данных. Но система кэширования в Internet Explorer несовершенна, и очень часто заново читаются изображения, которые лежат в кэше и не изменились с момента последнего посещения.

Чтобы избавиться от этого недостатка, я рекомендую использовать локальный прокси-сервер. Например, WinProxy, который можно скачать с сайта **http://www.winproxy.cz/**. Локальные прокси-серверы кэшируют информацию намного лучше, хотя и отнимают несколько больше дискового пространства.

Рассмотрим настройку прокси-сервера на примере WinProxy. Скачайте и установите программу. Это выполняется достаточно просто, единственное, на что вам нужно обратить внимание, — это адрес прокси-сервера. По умолчанию задается **http://localhost:3129/** (3129 — номер порта, но в будущих версиях этот параметр может измениться).

Теперь запустите Internet Explorer и наберите в строке URL-адрес **http://localhost:3129/**. Перед вами должна открыться страница администрирования сервера (рис. 5.3). В принципе, можно сразу приступить к работе, но все же я рекомендую познакомиться с доступными настройками. Возможно, вы захотите что-то улучшить или изменить.

Чтобы заставить Internet Explorer работать через прокси-сервер, необходимо запустить браузер и выбрать меню **Сервис | Свойства обозревателя** (Tools | Internet options). Перейдите на вкладку **Подключение** (Connections) и нажмите кнопку **Настройка сети** (LAN settings). Перед вами откроется окно настройки сетевого подключения (рис. 5.4).

Здесь нужно поставить флажок **Использовать прокси-сервер для локальных подключений** (Use a proxy server for your LAN), в поле **Адрес** (Address) введите `127.0.0.1` (такое значение всегда указывает на ваш компьютер), а в качестве порта

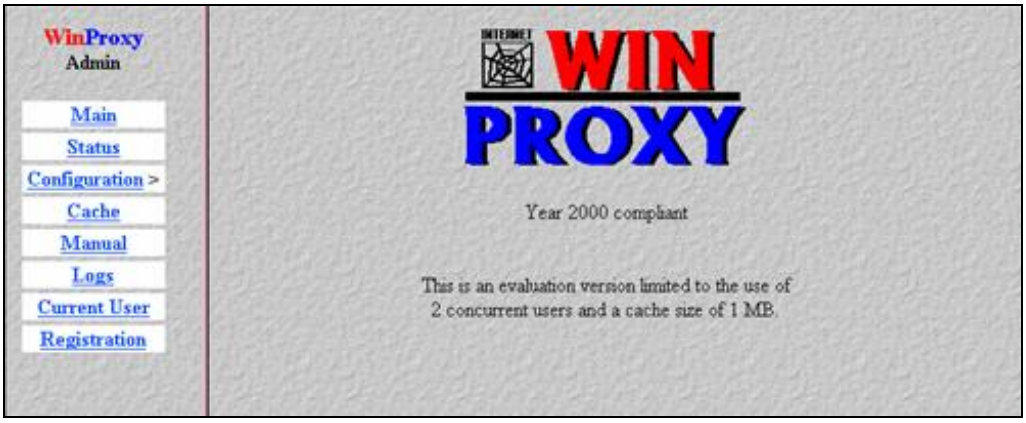


Рис. 5.3. Окно настройки WinProxy

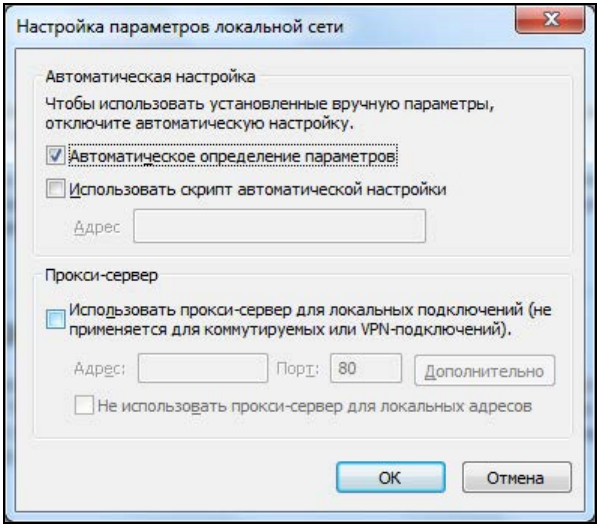


Рис. 5.4. Окно настройки подключения

(поле **Порт** (Port)) укажите `3129`. Сохраните изменения (кнопка **OK**), и теперь ваше соединение будет происходить через локальный прокси-сервер, что имеет свои преимущества и недостатки.

Рассмотрим основные недостатки:

- расходуется лишнее дисковое пространство для хранения кэша прокси-сервера, но на это можно закрыть глаза, потому что накопители сейчас большие и стоят недорого, а ускорить Интернет очень хочется;
- при загрузке сайта не всегда отображается свежая информация. Большинство прокси-серверов не проверяют запрошенную страничку на наличие изменений, а просто возвращают нам ее из кэша. Чтобы получить новейшую информацию, приходится нажимать кнопку **Обновить** (Update) в браузере.

Но есть и неоспоримые преимущества:

- увеличивается скорость загрузки и уменьшается трафик, т. к. бóльшая часть информации берется из кэша прокси-сервера;
- даже при использовании кнопки **Обновить** (Update) очень часто подгружается только текстовая информация и не расходуется трафик на перевывод изображений, которые изменяются очень редко. Чтобы обновить графику, нужно нажимать кнопку **Обновить** (Update) и одновременно удерживать клавишу <Shift>;
- хорошие прокси-серверы кэшируют не только информацию сайта, но и адреса. Это значит, что если вы уже посетили **http://www.cydsoft.com/**, то IP-адрес сохраняется в кэше, и при следующем обращении к сайту будет использоваться он, а не DNS, и загрузка может начаться сразу после указания символьного адреса.

Если вы очень трепетно относитесь к скорости работы в сети и бережете трафик, то я настоятельно рекомендую вам установить прокси-сервер, который обязательно сэкономит вам время и деньги.

5.1.4. Только то, что надо

Несколько лет назад у меня на работе было достаточно прижимистое начальство и ограничивало месячный трафик значением 50 Мбайт на человека. Что такое в наше время 50 Мбайт? Это копейки, которые израсходуются за неделю даже при простом просмотре веб-страниц. И при этом абсолютно ничего не удастся скачать, потому что даже обновления для Windows требуют большего объема.

Чтобы такого ограниченного трафика хватило на месяц хотя бы для просмотра вебстраничек, мне приходится отключать отображение картинок в браузере. Как я уже говорил, графическая информация отнимает большую часть трафика. Если объем текста на большинстве страничек не превосходит 10 Кбайт, то графика может превысить 100 Кбайт.

Для отключения изображений в Internet Explorer нужно выбрать меню **Сервис | Свойства обозревателя** (Tools | Internet options), и перед вами откроется окно для настройки свойств обозревателя. На вкладке **Дополнительно** (Advanced) найдите раздел **Мультимедиа** (Multimedia) и сбросьте флажок **Отображать рисунки** (Show Pictures). После этого в большинстве сайты будут выглядеть не так красиво, но это позволит сэкономить до 70% трафика.

Когда модемы были медленными и скорость загрузки хромала на обе ноги, я также отключал картинки. В них не так много информативности, и в большинстве случаев можно обойтись и без них.

На рис. 5.5 показан сайт компании CyD Software Labs без картинок, а на их месте красуются прямоугольники с маленькой стандартной картинкой в левом верхнем углу, которая указывает на наличие в данном месте изображения. Если захочется посмотреть какое-нибудь изображение, то достаточно щелкнуть по такому прямоугольнику правой кнопкой мыши и выбрать в контекстном меню пункт **Показать**

рисунок (Show picture). Таким образом, можно просматривать картинки выборочно, только те, которые нужны.

Еще одним проглотом в наше время стал Flash. Чтобы отключить его, нужно запретить загрузку компонентов ActiveX, ведь для отображения Flash используется именно ActiveX-компонент. В последнее время я стал больше использовать браузер Safari от Apple, который по моим наблюдениям работает побыстрее.

Рис. 5.5. Сайт **http://www.cydsoft.com/** без картинок

5.1.5. Качать, не перекачать

Если у вас плохая связь, которая регулярно обрывается, то скачать что-нибудь большого размера становится проблематично. Из-за постоянных разрывов приходится повторять операцию снова и снова. И все это — расход времени и денег.

Процесс самой передачи файлов в Internet Explorer тоже реализован не очень эффективно. Даже при хорошей связи скорость можно увеличить за счет разбиения данных на несколько потоков, проходящих разными путями. Корпорация Microsoft реализовала только необходимые возможности, но они далеко недостаточны.

Я рекомендую установить менеджер закачек Reget (**http://www.reget.com/**). Он позволит максимально эффективно использовать ваше соединение. Сначала программа автоматически ищет зеркала, с которых можно получить файл, и выбирает то из них, которое обеспечивает наилучшую связь (или качает сразу с нескольких мест). Ваша связь может быть отличной, но сервер, с которого нужно взять файл, может быть сильно перегружен. С помощью менеджера закачек вы сэкономите много времени.

Работа с программой достаточно проста. Вам надо только установить ее.

Теперь, когда вы щелкаете по ссылке на объект в Internet Explorer, файл будет скачиваться не встроенными в браузер методами, а с помощью программы Reget. Если во время получения данных связь оборвалась, то после восстановления соединения с Интернетом Reget может продолжить процедуру с того же места. Представьте, если вы качаете файл размером в гигабайт, и в момент, когда остался 1%, происходит обрыв. Приходится все делать заново, а потраченные время и деньги вам уже никто не вернет. Даже по самым низким тарифам за трафик на повторное скачивание вы затратите больше, чем на лицензию самой дорогой версии этой программы.

Это основные, но далеко не все возможности Reget. Подробно можно прочитать о программе на сайте **http://deluxe.reget.com/ru/features.htm**. Помните, что это не реклама, а экономия ваших средств.

5.2. Накрутка голосования

Системы голосования на разных сайтах постоянно развиваются, и программисты пытаются закрыть лазейки, чтобы пользователь не смог накручивать счетчики. Допустим, что некая компания проводит интернет-опрос, и вы, естественно, хотите, чтобы победила ваша версия ответа. Как же поступить в такой ситуации? Вариантов много, но все зависит от программы, которая собирает голоса пользователей.

Рассмотрим способы накрутки на примере сайта **http://www.download.com/**. Здесь можно голосовать за любимые программы, отдавая им свое предпочтение. Если вы видите, что ваша избранница имеет плохой рейтинг, то пытаетесь изменить ситуацию и помочь разработчику.

Чтобы понять, как увеличивать, нужно знать, как учитываются голоса. Самый простой вариант — использование cookies (это файлы-плюшки, в которых можно сохранять любую полезную информацию). У каждого сайта свой файл, и его может прочитать только он. К чужим cookies доступа нет. Когда вы отдаете свой голос, то сервер сохраняет информацию об этом в файле cookies. Рассмотрим шаги, которые выполняются при голосовании:

1. Отправка пакета с ответом на вопрос.
2. Сервер обрабатывает ответ и присылает подтверждение.
3. Ваш компьютер сохраняет информацию в cookies.

Таким образом, при следующем голосовании сервер определит по файлу cookies, что вы уже голосовали, и повтор будет невозможен. Но так думают только начинающие программисты. Сейчас мы посмотрим, как на практике разрушится это утверждение.

5.2.1. Вариант накрутки № 1

Пять лет назад система голосования на **http://www.download.com/** не имела абсолютно никакой защиты от подтасовки, и можно было воспользоваться простейшим

способом "быстрого клика": заходите на сайт, выбираете нужный вариант ответа и начинаете быстро нажимать кнопку **Отправить**.

Допустим, вы используете простую телефонную линию, тогда для отправки вашего ответа и получения подтверждения (т. е. файла cookies) нужно время. Если в момент пересылки/получения пакета повторно нажать кнопку **Отправить**, то предыдущая посылка на клиентской стороне считается незавершенной и отменяется, а начинает работать новая сессия обмена данными. Когда на первую отправку придет подтверждение сервера и просьба изменить файл Cookies, то запрос будет отклонен из-за несовпадения сессий.

Следовательно, если быстро щелкать по кнопке **Отправить**, то будут отправляться пакеты с нашими вариантами ответа, а сервер их обработает и добавит полученные голоса (т. е. выполнятся шаги 1 и 2). А вот ваш компьютер станет отклонять подтверждения, и третий шаг будет пропускаться, пока не произойдет одно из следующих событий:

- если вы прекратите быстро нажимать кнопку отправки ответа, то браузер примет файл cookies, полученный в результате последнего нажатия, и сохранит его;
- если между нажатиями кнопки отправки сервер обработал запрос, а ваш компьютер успел принять подтверждение, то файл будет создан, и дальнейшие щелчки станут невозможными.

На выделенных линиях с большой скоростью подключения обмен пакетами происходит быстро, и можно не успеть щелкнуть в очередной раз, а значит, файл cookies будет создан.

В этом случае подойдет другой способ изменения счетчика.

5.2.2. Вариант накрутки № 2

Когда программисты замечают, что систему голосования накручивают первым способом, то они начинают создавать защиту. Самый простой вариант — сразу после отправки ответа отключить кнопку (сделать ее недоступной) с помощью JavaScript, и вторая попытка нажатия станет невозможной. Но если вы знаете JavaScript, то сможете обойти это препятствие.

Чтобы избавиться от блокировки кнопки, нужно сохранить веб-страницу с голосованием на своем диске и удалить из нее код блокировки, написанный на JavaScript. Любая защита на стороне клиента легко обходится, потому что она доступна пользователю, и ее легко убрать.

На самом деле для голосования необходимо всего лишь направить серверу определенный запрос с помощью протокола HTTP. Существуют два типа запросов — GET и POST. В запросах GET параметры передаются через строку URL, а в POST — через заголовок пакета. Если вы знаете какой-либо язык программирования, то можно написать небольшую программку, которая будет в цикле направлять серверу пакеты с вашим голосом.

А что, если защита от повторного голоса сделана на стороне сервера? Так как информация о голосовании сохраняется в файле cookies, достаточно только его уда-

лить. Для этого нужно перейти в папку Users*ИмяПользователя*\Cookies, где *ИмяПользователя* — это имя учетной записи, под которой вы вошли в систему. Здесь находятся файлы, названия которых имеют формат ***ИмяПользователя@адрес.сайта*.txt**. После знака **@** идет адрес сайта, с которого получен данный cookie. Найдите файл с нужным названием и просто удалите его. После этого можно повторять попытку.

Приведенный вариант подходит и в тех случаях, когда вы хотите повторить голосование первым способом *(см. разд. 5.2.1)*, но файл cookie уже существует.

5.2.3. Вариант накрутки № 3

Наиболее жесткая защита организуется через IP-адрес. Если с какого-либо адреса уже проголосовали, то повторить попытку будет невозможно. Если вы пользуетесь подключением dial-up, то IP-адрес назначается вам автоматически при каждом входе в сеть. Достаточно заново подключиться к Интернету, и при этом вам, скорее всего, дадут другой IP, и можно будет повторить голосование.

Если у вас выделенная линия, то единственным (простым) способом будет использование анонимных прокси-серверов. Вам нужно где-нибудь раздобыть большой список таких proxy-адресов (в Интернете их достаточно), а потом через каждый из них отдать свой голос, и он, скорее всего, будет учтен.

Очень часто программисты для защиты от накруток используют IP-адреса и cookies одновременно. В этом случае нужно обязательно удалять соответствующий сайту cookie-файл, иначе система голосования определит подвох.

Применение защиты по IP-адресу — достаточно сложное дело. Очень много пользователей в глобальной сети, которые работают через различные промежуточные сети, но попадают в Интернет через один IP. Например, некоторые корпоративные сети объединяют более тысячи компьютеров, которые для выхода во внешнюю сеть используют прокси-сервер и общий IP-адрес. Если хотя бы один сотрудник такой компании проголосует на сайте, то остальные потеряют такую возможность, и поэтому нельзя будет говорить о какой-либо объективности опроса.

Именно поэтому IP-адреса, используемые системами голосования только для определения источника накрутки, обычно хранятся в базе недолго. Через определенное время вы без проблем сможете проголосовать с того же адреса. Для долговременной идентификации проголосовавших чаще всего используются именно cookies, которые нужно регулярно удалять, а если знать и содержимое, то достаточно просто редактировать.

5.2.4. Вариант накрутки № 4

Следующий вариант требует хотя бы начальных знаний языка разметки страниц HTML. Для примера я выбрал наиболее сложный вариант (но распространенный на больших порталах), когда область голосования организована в виде фрэйма внутри

окна. Получается окно в окне. Это удобно для пользователя, потому что после голосования перезагружается только этот фрейм, а не вся страница.

Итак, заходим на сайт хакеров **http://www.xakep.ru/**. Я выбрал этот сайт, потому что его программисты постарались и сделали хорошую систему голосования. На первой странице всегда проводится какой-нибудь опрос. Обратите внимание на то, что находится в окне голосования. В данном случае чуть выше вопросов идет заголовок "Голосование", а чуть ниже — архив материалов.

Выберите меню **Вид | В виде HTML** (View | Source code) и перед вами появится окно программы Notepad (Блокнот) с исходным кодом страницы. Запустите поиск по слову "Голосование", выбрав пункт меню **Правка | Найти** (Edit | Search). Посмотрите листинг 5.1, где представлен фрагмент HTML-текста, который был найден мною в исходном коде.

Листинг 5.1. Фрагмент HTML-текста из страницы голосования

```
<span class="textHeader1White">Голосование</span></td>
<tr>
  <td height="1" class="decorCellWhite"><img src="i/fon.gif" width="1"
                                          height="1" ></td>
</tr>
<tr>
  <td valign='middle' align='right'>
<table width="98%">
<tr><td><span class="textBodyHome">
<iframe src = "/code/common/vote3/include/iframe_vote.asp?site=SVT5"
  ID="anIframeRez3" NAME="anIframeRez3s" scrolling="no"
  frameborder="0" width="100%" marginwidth="0" marginheight="0"></iframe>
</span></td></tr>
</table><br>
</td>
</tr>
<tr>
<td height="1" class="decorCellWhite"><img src="i/fon.gif" width="1"
  height="1" ></td>
</tr>
<tr>
<td class="decorBodyCell1">
<table border="0" width="100%" cellpadding="0" cellspacing="0">
<tr>
<td class="textHeader1White" height="30" valign="top">/АРХИВ
МАТЕРИАЛОВ/</td>
```

В первой строке красуется надпись "Голосование", а в последней — "АРХИВ МАТЕРИАЛОВ". Значит, между ними где-то есть указание на само голосование. И если оно выполнено в виде фрейма, то искомая ссылка будет расположена внутри тега `<iframe>`.

Найдите строку, которая содержит слово `iframe`, и в ней вы увидите следующую конструкцию:

```
Src = "/code/common/vote3/include/iframe_vote.asp?site=SVT5"
```

В кавычках указан адрес голосования. В данном случае он начинается со слэша (косой черты). Это значит, что перед ним нужно добавить имя сайта **http://www.xakep.ru**. Если бы в начале уже стояли символы "http://", то ничего корректировать не надо было.

Итак, адрес системы голосования выглядит следующим образом:

http://www.xakep.ru/code/common/vote3/include/iframe_vote.asp?site=SVT5

Само голосование показано на рис. 5.6, которое на главной странице выглядит в виде фрейма.

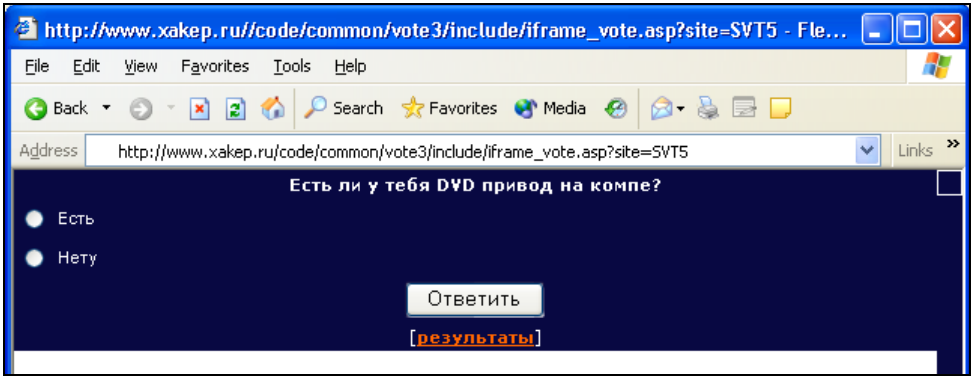


Рис. 5.6. Голосование на сайте **http://www.xakep.ru/**

Снова выберите меню **Вид | В виде HTML** (View | Source code) и познакомьтесь с исходным кодом страницы в программе Блокнот (Notepad) — листинг 5.2.

Листинг 5.2. Содержимое файла голосования

```
<html>
<head>
<meta http-equiv="Content-Type"
      content="text/html;charset=windows-1251">
<meta name="keywords" content="взлом, компьютерная безопасность, хакер,
защита данных, Linux, программирование, трояны, защита от проникновения,
вирусы, уязвимости, операционные системы, Deface, подбор пароля, взлом
мыла, снифер, перехват">

<link rel="stylesheet" href="../../../../local/include/main.css"
      type="text/css">
<script language="JavaScript"
        src="../../../../local/include/scripts.js"></script>
```

```
</head>
<body background="" bgcolor="#FFFFFF" marginwidth="0" marginheight="0"
      topmargin="0" leftmargin="0" rightmargin="0" bottommargin="0">
  <table bgcolor="#FFFFFF" width="100%" cellpadding="0" cellspacing="0"
        border="0"><tr><td>
  <table cellpadding="3" cellspacing="0" border="0" id="votationholder">
    <form action="../vote1.asp" method="post" target="_top">
    <input type="hidden" name="VoteID" value="VVT1051">
    <input type="hidden" name="userip" value="80.80.99.95">
    <tr><td colspan="2" align="center"><b class="textVoteTitle">Есть ли
      у тебя DVD привод на компе?</b></td></tr>
    <tr><td width="10px"><input type="radio" name="VoteOptionID"
      value="OVT1816"></td><td width="100%" align="left">Есть</td></tr>
    <tr><td width="10px"><input type="radio" name="VoteOptionID"
      value="OVT1817"></td><td width="100%" align="left">Нету</td></tr>
    <tr><td colspan="2" align="center"><input type="submit" name="s1"
      class="decorVoteInput" value="Ответить"></td></tr>
    <tr><td colspan="2" align="center">[<a
           href="../vote_results1.asp?site=SVT5" target="_top"
           class="textVtrezlink">результаты</a>]</td></tr>
    </form>
  </table>
  </td></tr>
</table>
<script language="JavaScript">
<!--
   document.domain= 'xakep.ru'
   parent.adjustFrame(window)
  //-->
</script>
</body>
</html>
```

Здесь ищем текст `<form action=`. После него в кавычках должен быть адрес скрипта, который обрабатывает голосование. В данном случае это `../vote1.asp`. Две точки, которые стоят в начале, говорят о том, что в текущем адресе нужно подняться на один уровень выше.

Текущий адрес у нас:

http://www.xakep.ru/code/common/vote3/include/iframe_vote.asp?site=SVT5

Удаляем все, что находится за последним слэшем, потому что это имя страницы и ее параметры.

Должен остаться такой адрес:

http://www.xakep.ru/code/common/vote3/include/

Теперь нужно подняться на уровень выше, т. е. убрать последний слэш и весь текст, предшествующий ему.

Остается следующий адрес:

http://www.xakep.ru/code/common/vote3/

Вот к этой строке нужно добавить то, что мы нашли в кавычках после кода `<form action=`, не забыв, что мы уже использовали часть `../`. Получится

http://www.xakep.ru/code/common/vote3/vote1.asp

Именно в таком виде адрес нужно указать в исходном коде в кавычках после `<form action=`.

У вас должен получиться код типа:

```
<form action="http://www.xakep.ru/code/common/vote3/vote1.asp"
      method="post" target="_top">
```

Теперь снова посмотрите на код из листинга 5.2. Найдите строки, которые содержат текст `<input type="hidden"`. Тег `<input>` говорит о том, что это поле ввода, содержимое которого будет передаваться скрипту. Параметр `type="hidden"` указывает на то, что поле скрыто. Наиболее интересной является вторая строка с таким тегом:

```
<input type="hidden" name="userip" value="182.181.19.5">
```

Через этот параметр передаются IP-адреса. В данном случае это 182.181.19.5. Наша задача — изменять его вручную в коде страницы и передавать серверу свой голос с новым IP. Как это сделать? Очень просто. Для этого нужно выполнить следующие шаги:

1. Сохранить измененное содержимое файла (см. листинг 5.2) на своем компьютере под любым именем, но с расширением htm.
2. Запустить этот файл и проголосовать.
3. Изменить в файле IP-адрес и перейти на шаг 2.

Таким образом можно голосовать сколько угодно, и сервер всегда будет думать, что посылка идет с разных IP-адресов. Несмотря на хорошую реализацию проведения опроса программисты ошиблись, определяя адрес отправителя не во время выполнения скрипта, а заранее, при формировании странички, которая является плодом творения ASP (Active Server Pages, технологии Microsoft для формирования веб-страниц "на лету"), и ее код формируется динамически при обращении к серверу.

Данный пример демонстрирует, как, используя HTML, можно изменить свой IP-адрес. Но такая ошибка встречается далеко не везде и проявляется по-разному. Зная язык разметки HTML-документов, можно отключать скрипты, написанные с помощью JavaScript, которые делают кнопки отправки результата голосования недоступными, и пользоваться первым методом накручивания (описанным в *разд. 5.2.1*). Кстати, в тексте HTML, который я нашел на сайте **http://www.xakep.ru/**, я обнаружил соответствующий код на JavaScript, но он не используется. Видимо, понадеялись на защиту по IP-адресу.

5.3. Социальная инженерия

Социальная инженерия — самое мощное оружие хакера. С его помощью происходили наиболее громкие взломы и создавались самые известные вирусы. Вспомните вирус Анны Курниковой, когда пользователям приходило письмо с вложением и предложением посмотреть фотографию Анны. Я думаю, что любопытство мужчин (а это бóльшая часть пользователей Интернета в те времена), которые запускали прикрепленный файл и таким образом заражали свой компьютер, помогло распространению этого вируса. А это не что иное, как социальная инженерия. Да и девушки могли запускать файл из-за любопытства посмотреть на конкурентку в борьбе за сердце Инрике Иглесиаса :).

Социальная инженерия основана на психологии человека и использует его слабые стороны. С ее помощью хакеры заставляют жертву делать то, что им нужно: заражают машины, получают пароли. Сколько раз я слышал про захваты кредитных карт с помощью простых e-mail-сообщений. Пользователь получает письмо с просьбой сообщить свой пароль, потому что база данных банка порушилась из-за погодных условий, хакера или поломки оборудования. Ничего не подозревающие пользователи зачастую сообщают запрашиваемые данные, потому что боятся потерять информацию.

Знаменитый хакер Кевин Митник был не только хорошим специалистом в ИТ, но и отлично понимал психологию людей и использовал социальную инженерию во всем. Если бы он использовал только навыки хакера, то не думаю, что он стал бы таким популярным.

В современных условиях хакеры редко придумывают что-либо новое, а используют старые и проверенные способы. Очень редко появляется какой-то новый и действительно оригинальный метод. Но, несмотря на это, всегда находятся жертвы, которые верят. Я пользуюсь Интернетом уже очень долгое время, и было время, я ежедневно получал десятки писем с просьбой запустить файл для обновления защиты или для того, чтобы увидеть что-то интересное. А ведь большинство отправителей — пользователи зараженных компьютеров. Значит, кто-то открывает такие вложения и заражает свой компьютер.

В последнее время количество писам немного поутихло и я не знаю, с чем это больше связано — с уменьшением интереса к этому виду хакерского искусства или просто владельцы почтовых серверов научились фильтровать вирусы? Мне кажется, что и то и другое.

Несмотря на широкое использование защитных программных комплексов и антивирусных программ, количество вирусов не уменьшается. Каждый день в сети появляются новые пользователи, которые еще ничего не знают о жестокости этого свободного мира по имени Интернет. Именно они чаще всего попадаются на различные уловки.

В принципе, социальную инженерию можно было бы отнести к системе безопасности и рассматривать в *главе 4*, где мы говорили о защите. Но в данном случае речь пойдет именно о сетевой социальной инженерии.

Я сам не раз применял принципы социальной инженерии, чтобы добиться эффекта от свежей программы-шутки. Описанные далее методы позволят вам использовать шуточные программы из *главы 3*, чтобы подбрасывать знакомым в виде исполняемого файла через e-mail-сообщения.

Итак, давайте рассмотрим некоторые способы, которыми пользуются хакеры. Это поможет вам распознавать их уловки и выделять попытки психологического воздействия от простого общения с людьми. Помните, что социальная инженерия максимально сильна в Интернете, когда вы не можете воочию оценить намерения своего собеседника.

5.3.1. Как он хорош

Мы уже говорили про e-mail-рассылку, в которой нас просят запустить файл во вложении. Я также предупреждал, что этого делать нельзя. Никто не будет посылать картинки через Интернет, как правило, это хорошо замаскированные исполняемые файлы.

Буквально недавно просочилась информация, что в ОС Windows есть ошибка при обработке BMP-файлов, а вчера я услышал об уязвимости JPEG-формата. К файлу картинки может быть прикреплен код, который при определенных условиях в некоторых программах (к ним относится и Internet Explorer) может быть выполнен. Конечно же, этот баг быстро исправили, и если пользователь обновляет свою ОС, то он в безопасности.

Когда вы просматриваете почту, то нужно без сомнений удалять любые письма, содержащие прикрепленные файлы с расширением scr, bmp, jpg, exe, com, pif и т. д.

Особое внимание нужно уделять файлам с заголовком "Mail Delivery". Такие уведомления приходят, когда ваше письмо не дошло до адресата, а вложением является файл с текстом вашего сообщения. Некоторые пользователи открывают это вложение, чтобы увидеть текст и определить, какое письмо не дошло. Это ошибка, потому что в последнее время вирусы стали маскироваться под сообщения в стиле Mail Delivery. Просто просмотрите тело письма, в котором должен быть указан e-mail получателя. Если вы отправляли письмо на этот адрес, то запросите подтверждение о получении вашего сообщения. Если оно не дошло, повторите посылку.

Я вижу много писем, в которых предлагается обновить Windows или какую-либо программу. Корпорация Microsoft и другие производители не занимаются такими рассылками по e-mail. Для обновления всегда нужно скачивать файлы с официальных сайтов, а не брать их из вложения к письму.

Когда мы путешествуем по сети, то на сайтах можно обнаружить яркие и красочные призывы щелкнуть по какой-либо ссылке. В ответ на это у нас просят разрешение на установку программы, без которой невозможно увидеть популярную звезду кино или шоу-бизнеса в обнаженном виде. Соблазн лицезреть это заставляет некоторых дать согласие, и в результате вы получаете вирус.

Помните, за яркими ссылками и настоятельными призывами что-то запустить или установить в 90% случаев прячется зловредный код. В последнее время я стал за-

мечать, что вирусов больше там, где есть порнография, сомнительный контент, и при этом используется непрофессиональный дизайн страницы, плюс большое количество рекламы. Возможно, что вирусы оказываются там без злого умысла, а из-за халатности администраторов сайта. Дилетантские ресурсы Интернета и обслуживаются любителями, поэтому могут содержать, что угодно.

5.3.2. Смена пароля

В последнее время снова начинает набирать ход метод взлома через смену пароля. Я стал больше получать писем с просьбой обновить свои реквизиты на странице банка, и при этом ссылка указывает совершенно на другой сайт, где введенные пользователем данные попадают в руки хакеру.

Недавно мне пришло письмо, в котором использовался очень старый и давно забытый способ социальной инженерии. Письмо имело примерно следующее содержание:

> Здравствуйте.
> Я администратор хостинговой компании XXXXX. Наша база была подвержена атаке со стороны хакера, и мы боимся, что некоторые данные были изменены.
> Просьба просмотреть следующую информацию, и если что-то неверно, то сообщите мне, я восстановлю данные в базе.

После этого следовало перечисление данных обо мне, которые легко получить с помощью сервиса Whois. На любом сайте регистрации доменов есть такая служба, позволяющая определять имя владельца домена. Хакер воспользовался этим сервисом и указал в письме всю найденную информацию, чтобы попытаться завоевать доверие. Помимо этого он указал еще два параметра — имя пользователя и пароль. Конечно же, эти данные хакер не мог знать, поэтому здесь были неверные значения. Большинство пользователей в этот момент теряются, и, волнуясь за свой сайт, естественно, пишут ответное письмо, в котором сообщают лже-администратору (а точнее, хакеру) свои параметры доступа к веб-страницам.

В качестве разновидности такого взлома можно привести классический случай со службой поддержки. Допустим, что вам нужно взломать все тот же хостинг. Вы звоните или пишете e-mail-письмо в службу поддержки с вопросом: "Почему я с такого-то аккаунта не могу зайти в Интернет или на сервер?" При этом нужно указать правильный логин (имя) и любой пароль. Работники службы поддержки обязаны помогать. Увидев ошибку, они поправят вас или вышлют правильный пароль по e-mail.

Если вы используете для общения со службой поддержки электронную почту, то тут главное — подделать e-mail пользователя, аккаунт которого вы хотите вскрыть. Служба поддержки не проверяет адрес отправителя, который фальсифицируется очень легко. Просто SMTP (Simple Mail Transfer Protocol, простой протокол электронной почты) может работать без авторизации, и в качестве отправителя позволяет указывать все, что угодно. Нужно только иметь SMTP-сервер, который не контролирует отправку почты.

Данный метод использует хороший психологический прием: сначала приводится достоверная информация, и только в параметрах доступа заложена ошибка. Таким образом завоевывается расположение и доверие жертвы, и вероятность получить пароль достаточно высока, если пользователь не знаком с таким принципом социальной инженерии. Это подтверждает множество знаменитых взломов в 80-х годах прошлого столетия. Опытные пользователи должны помнить о них, но для многих это новинка, которая может быть опасной.

В настоящее время администраторов (особенно хостинговой компании) обмануть таким способом сложно, но существует еще много других неопытных пользователей.

5.3.3. Я забыл

Не менее эффективным является метод забытого пароля. Есть мнение, что если пароль знают двое, то профессиональный хакер без труда добудет эту информацию. Так работали фрикеры.

Задача фрикера — позвонить по телефону, представиться другом, начальником, подчиненным или просто забывчивым пользователем и попросить напомнить пароль, сославшись на то, что компьютер сгорел, украли, сломался жесткий диск.

Таким образом один раз взломали сайт моих друзей. Над страничками работали несколько человек, живущих в разных уголках страны. Они общались только по e-mail и никогда не видели друг друга. Однажды один из членов команды получил письмо, в котором другой (администратор) просил сообщить пароль, якобы потерянный в связи с поломкой винчестера. Адрес отправителя был подделан, а для ответа предложены совершенно иные координаты. Но на это никто не обратил внимания, и злоумышленник получил пароль доступа к администраторскому разделу и уничтожил важную информацию.

В данном случае достоверный e-mail-адрес ослабил бдительность моего знакомого, и он сам отдал секретный пароль. Я прекрасно понимаю, что секретный пароль должен знать только один человек, иначе безопасность ослабевает. Но когда я участвовал в жизни сайта vr-online, то там все пароли администраторов были доступны всем.

5.3.4. Я свой

Для меня не составляет труда проникнуть в большинство зданий. Как-то я работал в фирме, которая имела четыре отдела безопасности для выполнения различных функций. На первый взгляд охрана была отличной, везде проход по пропускам, но эффект оказался минимальным.

Территориально фирма располагалась на двух площадках — офис в центре и производство за пределами города. Производственная база была обнесена колючей проволокой, на каждом углу охранник, камеры, собаки, за забором несколько метров ровного песка, на котором хорошо видны следы. Единственная проходная имела рамку металлоискателя, такую можно увидеть в любом аэропорту.

Несмотря на такие меры безопасности работники воровали, потому что зарплата была маленькая. От чего защитит рамка? Только от металлических предметов. Но компакт-диски и большинство дискет содержат слишком мало материала, на который сможет среагировать эта рамка. Даже меньше, чем в пуговице. Если настроить такую чувствительность, то металлоискатель будет реагировать на все и всех. Помимо этого, над проходной находился узел связи, где стоял факс. Во время приема документов рамка пищала, поэтому днем ее выключали.

Результат? Утром и вечером легко можно было проносить в карманах носители информации. Если нужно вынести предметы с металлическим покрытием, то это делали днем, когда металлоискатель не работал, а половина охраны находились на обеде.

На производственной площадке существовало очень много запретов. Например, нельзя было носить сотовые телефоны. Но я в течение двух месяцев таскал, и никто не заметил. Как? Очень просто. Сотовый лежал в моей сумке, на самом верху. Охранники досматривали скрытые места, а на то, что лежит на самом виду, просто не обращали внимания. Конечно, меня все же поймали, но сделал это новый сотрудник охраны, потому что он четко придерживался должностной инструкции.

В офисе было не менее весело. В четырнадцатиэтажном здании располагалось еще около 20 фирм. Внизу стоял охранник и проверял пропуска, внешний вид которых различался для каждой организации. Достаточно было только увидеть этот пропуск и распечатать на принтере что-нибудь похожее, и ни один охранник с расстояния 3—4 метра не обратит внимания на отличие.

Когда я только устраивался в фирму, мне пришлось несколько раз посещать офис, а пропуска не было. Чтобы не проходить долгую процедуру получения временного документа, я не стал ничего печатать, а нашел какой-то листик схожего размера и просто показывал его. Ленивая охрана пропускала меня. Пару раз я проходил мимо охраны, просто показывая проездной на автобус. По форме и цвету они были очень похожи.

Когда я уже работал в фирме, то в офисе появлялся редко (раз в полгода). Но когда я бывал там, то заметил, что не все показывают пропуска. Некоторые проходят просто так. После увольнения мне нужно было получить свои деньги. Чтобы не тратить время на получение временного разрешения, я просто сделал "каменное" лицо и пошел через проходную, как будто бываю здесь каждый день. Охрана или не обратила на меня внимания, или просто испугалась останавливать человека с таким наглым лицом.

Очень часто достаточно сделать вид, что вы здесь свой, как никто не будет проверять ваши документы. Милиция, охранники обращают внимание и проверяют только тех, кто ведет себя подозрительно или просто боится. Нахальство позволяет обойти 90% препятствий.

В компьютерной сфере тоже есть, где применить нахальство. Например, однажды у меня украли пароль на почтовый ящик. Даже не представляю, как это произошло, потому что пароль был сложный. Видимо имел место взлом провайдера. Чтобы вернуть свой пароль, я написал письмо в службу поддержки, но мне, конечно же,

отказали. Тогда я написал еще одно письмо, в котором представился сотрудником администрации города и если пароль не будет возвращен, то у фирмы будут большие проблемы.

В данном случае самое главное составить письмо в нужных тонах. Я писал от имени администрации, поэтому письмо содержало заумные слова. В конце письма была подпись:

Фленов Михаил Евгеньевич
Начальник отдела по работе с общественностью
Администрации XXXXX города

Конечно же, администратор поверил мне и испугался, и через некоторое время я получил свой пароль. А ведь я мог так получить и чужой пароль!

Но такой трюк пройдет только с администраторами маленьких серверов и мелких провайдеров. Пароль от ящика на mail.ru или rambler.ru вам никто не скажет, даже на такое страшное письмо. Хотя, я не проверял :).

5.3.5. Новенький и глупенький

Очень много взломов было совершено через образ новенького и глупенького сотрудника. Вам необходимо знать его фамилию или логин, и, желательно, чтобы этот человек был неприметен и его мало кто знал. После этого достаточно представится вместо этого сотрудника администратору и рассказать сказку о том, что вы только устроились и не можете войти на сервер. Системные администраторы любят считать себя хозяевами вселенной, и если им в этом помочь, то любой из них поведает вам все параметры доступа и объяснит, как войти.

Для примера использования этого метода вспомним случай с превращением ночного доступа в Интернет практически в круглосуточный, который мы рассматривали в *разд. 4.7.6*. Основная причина, по которой администратор дал мне доступ — его наивность. Я сыграл на этом, за счет того, что представился глупым пользователем.

5.3.6. Эффективность социальной инженерии

Задача хакера — войти в доверие к защищающейся стороне и выпытать пароли доступа. Для этого используются психологические приемы воздействия на личность. Человеку свойственны любопытство, доверчивость и чувство страха. Любое из них может стать фатальным.

Благодаря излишнему любопытству мы верим призывам открыть прикрепленный к письму файл и самостоятельно запускаем на своем компьютере вирус. В силу нашей доверчивости хакерам удается выпытать секретную информацию. Но самые сильные эмоции вызывает страх. Хакер заставляет нас поверить, что мы можем потерять данные, и мы в ужасе самостоятельно отдаем пароли доступа, в результате чего действительно утрачиваем контроль над секретной информацией.

Хакеры пользуются социальной инженерией незаметно, но эффективно. Вы даже не почувствуете подвоха, когда у вас попросят пароль или секретную информацию, и вы послушно все отдадите.

Чтобы не попасться на удочку, вы должны иметь представление о том, как взламывают другие системы и какие методы при этом используются. Хакеры каждый день придумывают что-то свежее, и необходимо следить за новыми способами.

5.4. Анонимность в сети

При каждом обращении к каким-либо сайтам в журналах сервера, где расположен веб-узел, регистрируются ваш IP-адрес и запросы. Если вы работаете по выделенной линии, то по этому адресу можно за несколько минут узнать домашний адрес и найти вас. Если используется dial-up-соединение через простой модем, то провайдером один и тот же IP-адрес выделяется разным клиентам, но по времени обращения к сайту можно определить, кто именно был подключен в этот момент и с какого телефона. После этого узнать по номеру телефона домашний адрес становится делом техники, потому что большинство провайдеров на данный момент требуют телефонный номер и реальный адрес, даже если вы подключены не по dial-up.

Для хакеров анонимность необходима, чтобы администраторы взламываемых сайтов не смогли вычислить их IP-адрес и, соответственно, найти злоумышленника. Для защиты хакеры используют любые методы сокрытия своего реального IP-адреса или подмены его другим.

Простым пользователям тоже нужна анонимность, чтобы хакеры по IP-адресу не смогли атаковать вашу машину. Получается, что анонимность позволяет защищать компьютер и является частью стратегии безопасности.

Если вы регулярно общаетесь в чате или посещаете каналы IRC (Internet Relay Chat, ретранслируемый чат Интернета), то я рекомендую научиться скрывать свой адрес от любопытных глаз. Люди бывают разные. И если вашему собеседнику в чате не понравится какое-нибудь ваше высказывание, то он может попытаться взломать вашу систему (или хотя бы перезагрузить ее).

Одним из простых средств обеспечения анонимности является прокси-сервер. Это уже давно известный и проверенный способ, но он имеет множество преимуществ и недостатков, о которых стоит поговорить подробнее.

5.4.1. Прокси-серверы

Изначально прокси-серверы (proxy) создавались для кэширования информации. Основные веб-сайты были перегружены, и каналы не справлялись с информацией, да и трафик стоил немалых денег. Чтобы в Европе каждый день не скачивать одну и ту же информацию с сайтов США, провайдер устанавливал у себя прокси-сервер. Теперь, если один пользователь обратился к сайту **http://www.intel.com/**, то при следующем обращении любого пользователя к этому же веб-узлу страницы скачиваются не с **http://www.intel.com/**, расположенного в США, а с прокси-сервера провайдера. Таким образом, провайдеры экономили трафик, а пользователи получали ускорение загрузки данных, потому что не надо было качать данные через океан.

Мы уже рассмотрели, как локальный прокси *(см. разд. 5.1.3)* может повысить производительность работы в Интернете, но это не единственное его преимущество. Прокси-серверы бывают прозрачными и анонимными. В прозрачных прокси пакеты пользователя просто пересылаются дальше на веб-сервер, значит, он видит ваш IP-адрес, и мы не получаем дополнительной защиты.

Как работает анонимный прокси-сервер? Вы посылаете запрос на proxy, а он уже от своего имени запрашивает нужную страничку и возвращает ее вам. Таким образом, хакеру может стать доступным только адрес прокси-сервера, и он будет атаковать его, а такие серверы защищены достаточно хорошо. В большинстве случаев за ними следят профессиональные администраторы. А даже если и взломают, вам-то что? Главное, чтобы ваш компьютер остался в целости и сохранности.

На словах пока все красиво, но реально прокси имеет несколько слабых мест, которые обойти не просто. Рассмотрим основные проблемы.

- Серверы прокси изначально создавались для протокола HTTP (Hypertext Transfer Protocol, протокол передачи гипертекстовых файлов), поэтому иногда используют термин HTTP-proxy. Со временем они начали охватывать протоколы POP (Post Office Protocol, почтовый протокол), SMTP (Simple Mail Transfer Protocol, простой протокол электронной почты) и FTP (File Transfer Protocol, протокол передачи файлов). Но в любом случае этот список ограничен, и тяжело заставить прокси работать с другими протоколами. Для решения этой проблемы есть Socks-серверы, которые схожи с proxy, но об этом мы еще поговорим.
- Не все программы поддерживают работу через прокси- и Socks-серверы, поэтому может потребоваться смена программного обеспечения. Проблема тут еще в том, что Socks-серверы бывают нескольких версий, и программа может не поддерживать нужную версию. В этом случае приходится искать или другой Socks, или иную программу. Обычно выбирают тот вариант, который обходится дешевле.
- Не все прокси-серверы анонимны. Недаром в Интернете появились программы поиска и проверки таких серверов. Прежде чем почувствовать себя в безопасности, нужно убедиться в полной анонимности выбранного сервера. Я в данной книге дал бы список своих серверов, но это бесполезно, потому что прокси регулярно исчезают, и появляются новые.
- Не все прокси-серверы поддерживают протокол шифрования SSL, который необходим для доступа к защищенным областям сайтов, например к странице приема оплаты или администрирования.
- Прокси-серверы могут сохранять в заголовке пакетов IP-адрес отправителя, просто он будет находиться в каком-либо параметре.

Но даже если вы работаете через абсолютно анонимный прокси-сервер, спецслужбы или хакеры смогут вас найти. Все обращения к прокси-серверу сохраняются в журналах, и по запросу данные о вашей активности и IP-адрес могут быть получены заинтересованными лицами. Хакерам такую информацию не дадут, но есть вероятность, что они взломают сервер и сами получат доступ к базе журнала или воспользуются методами социальной инженерии.

От спецслужб защититься можно, используя сервер из какой-нибудь далекой страны Зимбабве, с которой нет дипломатических отношений. Как узнать, в каком государстве расположен сервер? Самый простой и дешевый вариант — воспользоваться службой Whois. Я всегда пользуюсь сайтом **http://www.nic.ru/whois/en/**. Загрузите его (на рис. 5.7 представлен вариант сайта для русскоязычного пользователя), введите адрес в поле **Для полуения информации...** (In order to obtain information...) и нажмите кнопку **OK**. Перед вами появится информация, схожая с представленной в листинге 5.3.

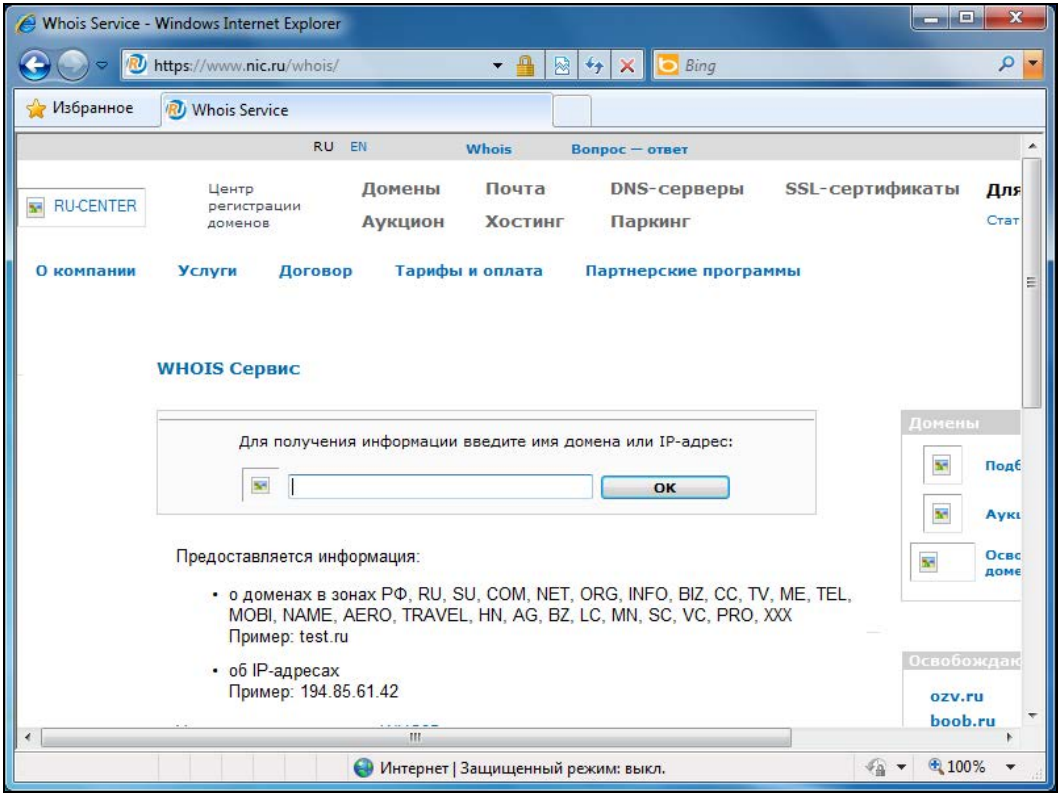


Рис. 5.7. Служба Whois на сайте **http://www.nic.ru/**

Листинг 5.3. Информация об IP-адресе

```
OrgName:     Ford Motor Company
OrgID:       FORDMO
Address:     P.O. Box 2053, RM E-1121
City:        Dearborn
StateProv:   MI
PostalCode:  48121-2053
Country:     US
```

```
NetRange:   19.0.0.0 — 19.255.255.255
CIDR:       19.0.0.0/8
NetName:    FINET
NetHandle:  NET-19-0-0-0-1
Parent:
NetType:    Direct Assignment
NameServer: DNS004.FORD.COM
NameServer: DNS003.FORD.COM
Comment:
RegDate:    1988-06-15
Updated:    1999-12-07

TechHandle: ZF4-ARIN
TechName:   Ford Motor Company
TechPhone:  +1-313-390-7095
TechEmail:  dnsadmin@ford.com
```

В описании явно написано, что адрес зарезервирован за компанией Ford Motor Company. Честно сказать, я не пытался найти эту компанию, а набрал адрес случайным образом. Но я рад, что выпал именно Ford, потому что люблю их машины и с удовольствием ездил в России на Ford Focus, а в Канаде на Fusion. Но вернемся к данным об адресе. Из этой информации можно получить следующие сведения о владельце адреса (приведу самое интересное):

- `OrgName` — название организации;
- `Address`, `City`, `StateProv`, `PostalCode`, `Country` — полная информация об адресе;
- `NetRange` — диапазон адресов, принадлежащих компании;
- `NameServer` — таких записей может быть несколько, и они описывают DNS-адреса серверов, поддерживающих домен. В данном примере есть одна интересная особенность в адресе DNS-сервера — имя выглядит как DNS00*x*.FORD.COM, где *x* — это число 3 или 4. А почему не 1? Вопрос интересный. Возможно, что DNS001.FORD.COM тоже существует, но поддерживает домен в других целях, например, для внутреннего использования в сети компании. Этого я не проверял, но для исследователя это может быть интересным;
- `TechName`, `TechPhone`, `TechEmail` — информация о компании/человеке, занимающемся поддержкой домена.

Способ Whois хорош, но может ошибиться, потому что зарезервировать можно в одной стране, а использовать в любой другой стране. Может происходить перенаправление или туннелирование трафика. Вы обращаетесь по одному адресу, а он вас перенаправляет в совершенно другую точку мира.

Чуть более надежным способом можно считать программы типа Trace Route, которые показывают путь от вас до указанного сервера. Некоторые такие программы могут отображать прямо на карте, как движется пакет, и вы легко можете увидеть, куда он дошел.

Вот так вот выглядит маршрут от той точки, где я сейчас нахожусь (а я еду в метро на работу), до моего блога:

```
Trace route started for flenov.info at 8:18:42 AM
1  192.168.1.1
2  Time out. Host might not allow connection test.
3  74.115.197.129
4  10.0.251.174
5  10.0.251.182
6  198.32.245.112
7  184.10.208.193
8  216.66.3.86
9  98.130.213.18
10  173.83.220.5
Host found in 10 routes
```

Мне повезло, я добился в результате с первого раза того, чего хотел. Во второй строке горит надпись "Time out. Host might not allow connection test". Такое происходит, когда администратор на сервере запретил эхо-пакеты, такие как ping. Этим я хотел показать, что иногда программы типа Trace Route или ping могут не дать результата.

На некоторых больших серверах эхо-пакеты запрещают в целях безопасности. Не сильно понимаю, от чего защищаются сейчас. Раньше у эхо-протокола, а точнее его реализации были узкие места, но сейчас, кажется, его отладили, и уже давно ничего не слышно. Но в принципе, никто не пользуется утилитами ping, то я согласен, нет смысла разрешать.

Вы тоже можете запретить на своем компьютере эхо-пакеты. Но это минимальная и я бы даже сказал мнимая защита. Реально она мало от чего спасает.

5.4.2. Цепочка прокси-серверов

Более надежным способом считается использование цепочек прокси-серверов. В этом случае вычислить ваш реальный адрес будет намного сложнее. Если запросы будут идти через два прокси, то хакеру придется взламывать оба сервера, чтобы просмотреть файлы журналов и найти ваш адрес. Это добавит лишних хлопот и спецслужбам, хотя, поверьте мне, если они взялись за хакера, то их уже ничто не остановит. Эти организации тоже не стоят на месте, их сотрудники могут распутать цепочку и из десяти анонимных серверов.

Создание цепочек для прокси- и Socks-серверов немного отличаются друг от друга, поэтому технологии их настройки лучше всего рассматривать раздельно.

Для начала разберем классический HTTP-Proxy. Посмотрите в настройки Internet Explorer (рис. 5.8). Здесь нет никаких средств для построения цепочки, и мы можем указать только один сервер для каждого протокола.

Чтобы организовать цепочку для прохождения запросов через несколько прокси-серверов, нужно использовать специальные программы, которые могут построить

виртуальный туннель. Для создания такого туннеля прокси должен поддерживать работу с SSL-протоколом (Secure Socket Layer, протокол защищенных сокетов), который позволяет шифровать данные пакетов, и если злоумышленник перехватит данные, то дешифровать будет не просто.

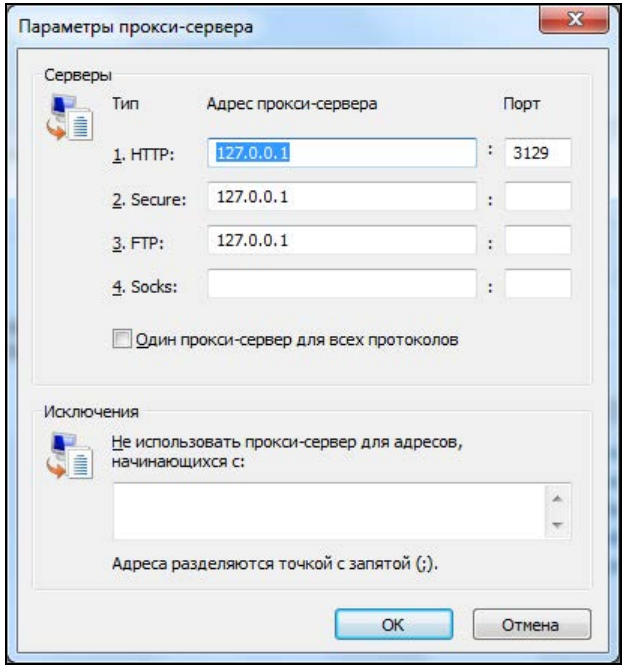


Рис. 5.8. Настройка прокси-серверов в Internet Explorer

Для ручной проверки необходимо через прокси обратиться к любому сайту, поддерживающему SSL-протокол (адрес начинается с "https://"). Чаще всего SSL-стандарт используют для проведения электронных финансовых операций через Интернет (например, принимаются платежи) и в некоторых почтовых сервисах (например, **http://www.hotmail.com/**). Если страничка загрузилась, то сервер поддерживает SSL.

Для создания цепочек HTTP-proxy или Socks лучше всего использовать программу SockChain, которую можно взять по адресу **http://www.ufasoft.com/socks/**. Она достаточно проста в использовании, а на сайте производителя вы найдете информацию по настройке.

5.4.3. Готовые сервисы

Анонимность нужна многим, и это формирует своеобразную потребность в дополнительных услугах. А раз есть спрос, значит, должно быть и предложение. В связи с этим в Интернете появилось несколько компаний, предлагающих своим пользователям абсолютную анонимность.

Самыми популярными из этих сервисов стали:

- Anonymizer (**http://www.anonymizer.com/**) — наверное, самый старый проект;
- Private Web Access (**http://www.bell-labs.com/project/lpwa/**) — сервис компании Lucent;
- Onion Router (**http://www.onion-router.net/**) — проект исследовательского центра ВМС США;
- Freedom Network (**http://www.freedomnetworkusa.org/**) — несмотря на org в имени домена, участие в этой сети очень даже коммерческое.

Это наиболее известные сервисы, но за время работы они уже успели подмочить свою репутацию, потому что даже небольших усилий достаточно, чтобы узнать IP-адрес посетителя. Это уже не раз доказано как аналитиками, так и профессионалами в области безопасности.

Сервис Freedom Network разрабатывался и отлаживался в течение 2 лет. Он обеспечивает максимальные условия сокрытия авторства, но и стоит 50 долларов в год. Чтобы им воспользоваться, необходимо установить специальную программу, с помощью которой вы можете создать несколько псевдонимов и использовать каждый из них для различных нужд. После этого ваша информация будет путешествовать через цепь серверов (наподобие прокси и Socks), каждый из которых снабжен механизмом криптографической защиты. Таким образом, невозможно будет восстановить путь следования вашего пакета и узнать его истинное происхождение.

Во время обмена данными происходит шифрование, в надежности которого можно не сомневаться, потому что сервис канадской компании основан на применении инфраструктуры открытых ключей, не имеющих, в отличие от США, ограничения на длину.

О надежности сервиса говорит и тот факт, что разработчиком комплекса заинтересовались не только спецслужбы США, но и Канады. Да, компания не нарушает законов ни одной из этих стран, но такая анонимность может быть использована хакерами в разрушительных целях, и поимка злоумышленника усложнится.

Такое положение дел не может не огорчать, потому что если компанией заинтересовалось правительство таких стран, то фирма как минимум может снизить безопасность, сохранив для пользователей анонимный доступ, но с возможностью просмотра всех данных со стороны спецслужб. А такое сокрытие авторства уже нельзя считать полным, и оно не будет стоить потраченных 50 долларов в год.

5.4.4. Расскажи-ка, где была

Допустим, что вы посетили некий сайт, подобрали под себя какие-то параметры (например, цветовое оформление) и хотите при следующем входе увидеть плоды своего творчества. Это вполне нормальная ситуация, поэтому и были придуманы файлы cookies.

Каждый веб-сайт имеет право сохранять на локальном диске пользователя информацию в строго определенном файле, к которому имеют доступ только он сам (и никакой другой) и клиент.

Помимо этого, некоторые веб-серверы сохраняют всю вашу активность в своей базе, чтобы навязывать какие-либо товары и услуги, а некоторые используют эту информацию в корыстных целях. Когда вы заходите на сайт, сервер может определить, где вы были до этого, а после выхода — установить, куда переместились. Иными словами, составляются портреты пользователей, и лично меня это не очень устраивает. Я не хочу, чтобы кто-то отслеживал мои действия, особенно сайты, на которых я зарегистрирован и где есть моя контактная информация (например, почтовая служба, требующая при регистрации указать фамилию, имя и отчество, дату рождения и адрес проживания).

Чтобы серверы не собирали о вас информацию, нужно до путешествия по веб выполнить следующие действия:

- отключить поддержку cookies. Некоторым сайтам они необходимы для нормальной работы. Если вы столкнулись с такой ситуацией, то просто воспользуйтесь услугами другого разработчика, благо альтернатив сейчас предостаточно. Но лично я не отключаю cookies, потому что они приносят удобства, а следую остальным правилам;
- при регистрации без особой надобности не вводите свою подлинную информацию. Реальные данные нужны интернет-магазинам для доставки покупок или сервисам оплаты услуг и товаров для проверки правильности регистрации (например, при покупке программ). Остальным серверам (в частности почтовым) мои настоящие данные не нужны. Поэтому в таких случаях вместо имени/даты рождения/адреса я указываю вымышленные реквизиты.

Вся информация, которую мы вводим на веб-сайтах, может быть украдена (уже было достаточно много прецедентов), если администраторы сайта ленивы, а программисты не поддерживают сайт. Вы уверены в сайте? Я не уверен во всем количестве форумов и чатов, существующих в сети, поэтому нигде и никогда не указываю реальные данные, только если это не интернет-магазин, которому нужны реальные данные для отправки товара.

В последних версиях всех современных браузеров появилась новая фишка — приватный режим (private browsing). В IE9 для перехода в этот режим нужно нажать комбинацию клавиш <Ctrl>+<Shift>+<P> или выбрать меню **Сервис | Безопасность | Просмотр InPrivate** (Tools | Safety | InPrivate Browsing) (если вы не видите меню, просто нажмите клавишу <Alt>, и оно появится). В Firefox для запуска приватного режима используется такое же сочетание клавиш, что и в IE9, но только вот меню немного отличается — **Tools | Start Private Browsing**.

В приватном режиме браузер прекрасно работает, только он не сохраняет никакие данные локально на компьютере. После выхода из этого режима или после перезапуска браузера все следы пребывания на каких-либо сайтах исчезают. Если какой-то сайт хочет создать cookie на компьютере пользователя, чтобы сохранить какие-то настройки или имя пользователя и пароль (иногда сайты сохраняют эту информацию, даже когда их не просишь), то печенюшка cookie создается в памяти браузера и нигде не сохраняется.

За приватный режим приходится платить удобством. Так как браузер не сохраняет никаких данных, все имена и пароли всегда приходится вводить заново. Лично я

использую приватный режим очень редко и только на публичных компьютерах. Например, если настраиваю кому-то компьютер и нужно заглянуть в свой online-аккаунт и скачать что-то со SkyDrive или посмотреть в записной online-книжке какие-то настройки, то захожу в свой аккаунт через приватный режим. Использовать его на своем личном компьютере не вижу смысла. Разве что только вы не ломаете сайты и не хотите, чтобы полиция (как же непривычно называть наши правоохранительные органы таким красивым словом) нашла какие-то следы на вашем компьютере.

Если уж вы зашли на какой-то сайт без приватного режима и хотите уничтожить следы своего пребывания, то тут могут возникнуть проблемы. В FireFox достаточно только удалить все данные в настройках программы или выбрать **Tools | Clear Recent History**. В появившемся окне нужно выбрать, что именно вы хотите очистить, и нажать кнопку **Clear Now**. Я слишком глубоко не копал, но беглая проверка показала, что этот браузер удаляет все честно.

В Internet Explorer можно попытаться удалить все сохраненные файлы встроенными средствами, только вот не советую им целиком доверять. Как говорится, доверяй, но проверяй. Сразу после чистки загляните в папки:

- \Users*Имя_пользователя*\AppData\Local\Temp\Cookies\;
- \Users*Имя_пользователя*\AppData\Roaming\Microsoft\Windows\Cookies\;
- \Users*Имя_пользователя*\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ и все папки, которые найдете здесь. Это каталог временных файлов, по которому достаточно легко определить, какие сайты вы посещали.

В IE9 чистку следов явно подправили, и после удаления всех временных файлов средствами IE в этих папках уже не остается мусора. В предыдущих версиях там постоянно оставалось множество файлов и приходилось подчищать вручную.

Если боятся того, что к вам домой зайдут из правоохранительных органов и начнут проверять диски, одной чисткой временных файлов не обойтись. Программы оставляют множество следов, разбросанных по системе и диску. Например, файл подкачки или файл гибернации.

Оперативная память не безгранична, и ОС не может возволить программам выделять больше, чем есть физически, без маленьких хитростей. Такой хитростью как раз и является файл подкачки, который по умолчанию расположен в корне системного диска и называется pagefile.sys. Когда программе требуется много памяти, а у ОС нет физической возможности выделить нужный объем, она может сбросить неиспользуемую информацию из физической памяти на диск в файл подкачки. Получается, что на диск могут уйти большие фрагменты сведений, которые могут содержать даже конфиденциальные данные. По файлу подкачки можно определить много интересного о последней активности на компьютере, потому что программы интенсивно использую его, а ОС не тратит ресурсы на очистку удаленных страниц памяти.

Много полезного можно узнать о дампах памяти после краха систем или о файлах гибернации. Лично я не выключаю свои компьютеры, а отправляю в гибернацию, потому что выход из гибернации на много быстрее, чем холодный запуск системы.

Поднял крышку ноутбука, нажал кнопку включения, и компьютер уже полностью готов к работе уже секунд через 30. То же самое делаю и на работе. Когда мы отправляем компьютер в гибернацию, то он все данные из оперативной памяти сбрасывает в файл hiberfil.sys в корне диска.

Сброс памяти в файл может происходить и при крахе системы, если вы не отключили создание дампов памяти. Да, восстанавливать полную картину того, что вы делали последние несколько часов свободной жизни, по страницам памяти из файлов достаточно проблематично и не легкое занятие, поэтому этим не будут заниматься, если вы взломали сайт нацистов или организации бабушек за 70. Первых государство точно не пожалеет, а о вторых тоже не часто думает.

5.4.5. Анонимность в локальной сети

Если в Интернете вас идентифицируют по IP-адресу, то в локальной сети при передаче пакетов участвует и физический адрес устройства MAC (Media Access Control, управление доступом к среде). Это 48-разрядный серийный номер сетевого адаптера, присваиваемый производителем. Он уникален, потому что у каждого изготовителя свой диапазон адресов.

Когда вы обращаетесь по IP-адресу к какому-либо компьютеру в локальной сети (в рамках одного и того же сегмента), все равно используется MAC-адрес. Самое интересное, что даже его можно подделать, хотя он прошивается в сетевой карте производителем. В ОС Linux для решения этой проблемы даже не надо устанавливать дополнительный софт, а в Windows нужна небольшая специализированная утилита. Такие программы в Интернете лежат "на каждом углу".

Лет 10 назад (когда я писал еще первое издание книги) у меня на работе интернет-трафик подсчитывался по MAC-адресам сетевой карты каждого компьютера. Администраторы, видимо, знают о легкости подмены IP-адреса, а вот про MAC даже не подумали. После установки программы Fantom MAC у моего начальника трафик резко пошел вверх, зато у меня — не изменился.

Как и в случае с подделкой IP, адреса MAC тоже должны быть в сети уникальными. Это значит, что когда компьютер, номер адаптера которого вы хотите использовать, включен в сеть, вы не можете поменять свой адрес, иначе произойдет конфликт. Оборудование не сможет определить точку назначения пакета (кому переслать данные).

Авторизация должна происходить по адресам IP и MAC совместно с логином и паролем пользователя. Только в этом случае можно спать спокойно. Но не стоит забывать о возможности украсть имя/пароль, и тогда злоумышленник сможет использовать чужой трафик. Чтобы избежать и этого, надо за каждым портом коммутатора закрепить определенный адрес. В этом случае, даже если злоумышленник подделает адреса, он не сможет воспользоваться сетью, не подключившись к нужной розетке.

Авторизация только по IP и MAC — достаточно распространенная ошибка администраторов. А большинство из них, зная о простоте подмены IP-адреса, и на MAC не обращает внимания.

Современные драйверы сетевых карт для Windows умеют менять MAC-адрес без дополнительных программ. Нажмите кнопку **Пуск** (Start), в строку поиска программ введите `управление компьютером` (computer management) и нажмите клавишу <Enter>. В появившемся окне слева найдите **Управление устройствами** (Device Manager). Теперь в центральной области окна у вас должно быть дерево из всех найденных в системе устройств. В разделе **Сетевые адаптеры** (Network Adapters) щелкните правой кнопкой мыши по имени сетевой карты, адрес которой вы хотите изменить, и выберите пункт **Свойства** (Properties). В открывшемся окне на вкладке **Advanced** (Дополнительно) можно увидеть список всех параметров, которые вы можете изменить (рис. 5.9). Параметр **Сетевой адрес** (Network Address) как раз и есть MAC-адрес.

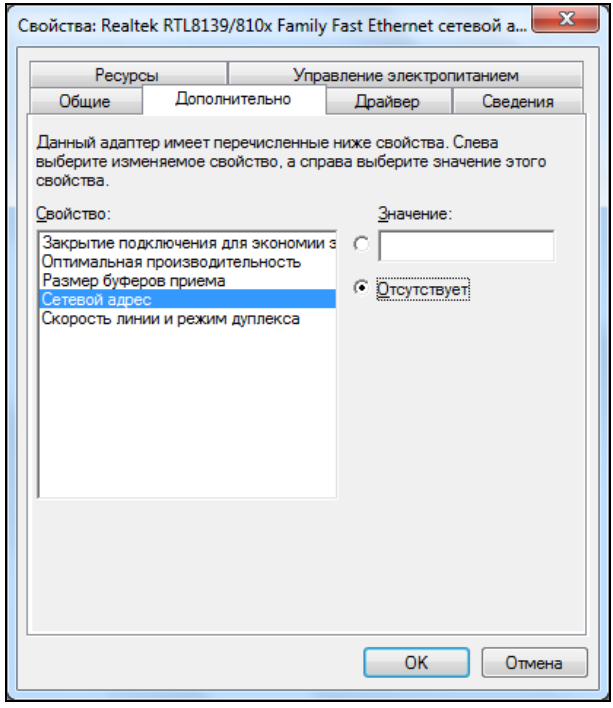


Рис. 5.9. Окно смены MAC-адреса

5.4.6. Обход анонимности

Мы долго говорили о прокси-серверах, и все было прекрасно. Но я не упомянул об одном очень интересном методе, с помощью которого сайт может без проблем узнать реальный адрес пользователя. Для этого у пользователя должна быть установлена виртуальная машина Java, а в браузере — разрешено использование апплетов. Посмотрим, как это работает:

1. Пользователь запрашивает веб-страницу.
2. Вместе со страницей пользователю возвращается Java-апплет, который устанавливает соединение с веб-сервером.

Дело в том, что Java не использует настройки браузера и не будет устанавливать соединение через прокси, а обратится к серверу напрямую. Вот по этому соединению сервер как раз и узнает реальный IP-адрес пользователя. Так что все построения цепочек могут пойти лесом, если браузер может работать с апплетами, а апплеты работают с сетью напрямую, а не через цепочку прокси.

5.5. Анонимная почта

Как отправить письмо, чтобы получатель не смог определить исходящий адрес? Это бывает необходимо для того, чтобы подшутить над ближним и скрыть свои координаты.

Проблема решается достаточно просто, и нужно выполнить всего два действия. Для начала настраиваем свой веб-браузер на работу через анонимный прокси-сервер. Затем регистрируем новый e-mail-адрес в какой-либо бесплатной службе, благо их сейчас в Интернете предостаточно, и вот вам анонимный почтовый ящик. Не забудьте, что не стоит указывать свои реальные данные, потому что некоторые сервисы могут сделать эту информацию общедоступной.

Несколько лет назад существовали специализированные службы для отправки анонимной почты (тогда было мало бесплатных почтовых сервисов), основанные на том принципе, что ваши данные (IP-адрес) не сохраняются в письме, а в качестве имени отправителя можно указать, что угодно. Но со временем надобность в этих сервисах исчезла, потому что появилась возможность спрятать IP-адрес с помощью прокси, а параметры автоматически поменяются, если завести отдельный ящик.

5.5.1. Подделка отправителя

Если необходимо подделать отправителя и послать письмо, например, от имени **jondo@hotmail.com** (это чужой адрес, на который у нас нет пароля), то это легко делается через любой SMTP-сервер, не имеющий защиты от отправки нелегальной почты. Используемый в данном случае протокол передачи e-mail-сообщений (SMTP) по умолчанию не защищен. В бесплатных сервисах, которые распространены в Интернете, администрация делает защиту одним из следующих способов:

- сообщение может быть послано, только если в качестве отправителя стоит адрес этой службы. То есть нельзя передать письмо от имени **jondo@hotmail.com** через сервис **mail.com**, потому что имена доменов не совпадают;
- перед отправкой необходимо сначала принять почту. Когда выполняется доставка сообщений по протоколу POP3, который защищен паролем, на сервере сохраняется IP-адрес проверявшего, и в течение определенного времени с этого компьютера можно отправлять письма. Если у вас нет пароля на адрес **jondo@hotmail.com**, то проверить почту, а значит, и отправить через такой сервер не получится, т. к. контролироваться будут те же параметры (имя и пароль).

Но все это — не проблема, и нам не нужны такие сервисы. У провайдеров, как правило, есть свои SMTP-серверы, которые доступны всем клиентам. Они необходимы для ускорения отправки корреспонденции. И если для посылки e-mail использовать именно его, то не надо будет соединяться с сервером бесплатной почты на другом континенте. Достаточно воспользоваться самым близким, находящимся у провайдера.

У большинства таких SMTP-серверов включена лишь одна проверка — отправитель должен быть подключен через этого провайдера. Если такой контроль установлен, то вы не сможете войти в сеть, воспользовавшись услугой одного провайдера, а отправить письмо через сервер другого. Свяжитесь со службой поддержки и узнайте адрес своего SMTP-сервера.

Например, для всех мобильных пользователей "Билайн" открытым SMTP-сервером является **mail.beelinegprs.ru** (если мне не изменяет память). Этот сервис не запрашивает никаких паролей, но требует, чтобы вы были подключены с мобильного телефона через оператора "Билайн". Наверно поэтому почта постоянно не отправляется, а в ответ приходят сообщения о том, что сервис заблокирован антиспам-системой.

Теперь создайте новый почтовый ящик. В программе Почта Windows Live, например, для этого нужно щелкнуть по кнопке **Добавить учетную запись**. Должен запуститься мастер создания нового почтового ящика. Рассмотрим, что нужно сделать на каждом шаге:

1. Сначала необходимо задать e-mail. Указываем тот адрес, с которого нужно отправить письмо, т. е. **jondo@hotmail.com**. Потом вводим пароль.
2. Затем нужно указать имя, которое будет отображаться в качестве отправителя. Ориентируйтесь на параметры человека, от имени которого вы хотите действовать. А если у вас есть его письма, то лучше взять информацию из них. Например, если в качестве отправителя используется Jon Doe <jondo@hotmail.com>, то вам необходимо ввести все, что находится до e-mail-адреса, в данном случае "Jon Doe".
3. Следует устновить флажок **Вручную настроить параметры сервера...** и нажать кнопку **Далее**.
4. И, наконец, надо ввести сервер входящей и исходящей почты. Для входящей необходимо знать имя и пароль входа на сервер провайдера. Если имя определить легко (чаще всего это сам электронный адрес или то, что находится до знака **@**), то с паролем возникнут проблемы. Мы не будем получать корреспонденцию с этого ящика, поэтому для входящей почты значение не важно. В качестве сервера исходящей почты нужно указать SMTP. Введите адрес, который вам дал провайдер (помните, вы связывались со службой поддержки), или задействуйте любой другой доступный SMTP-сервер.

Если у вашего провайдера нет SMTP-сервера или вы хотите делать рассылки (только не спам, потому что это незаконно), то воспользуйтесь программой CyD Postman (**http://www.cydsoft.com/**) или любым другим инструментом со встроенным SMTP-сервером.

Я покажу, как можно отправить сообщение с помощью CyD Postman.

1. Запустите программу и сразу войдите в настройки, выбрав пункт меню **Options | Program options**. Здесь нужно выбрать вкладку **Build-in Mail Server** и в поле **Send From** указать электронный адрес исходящего письма (рис. 5.10). Нажмите кнопку **OK**, чтобы сохранить изменения.

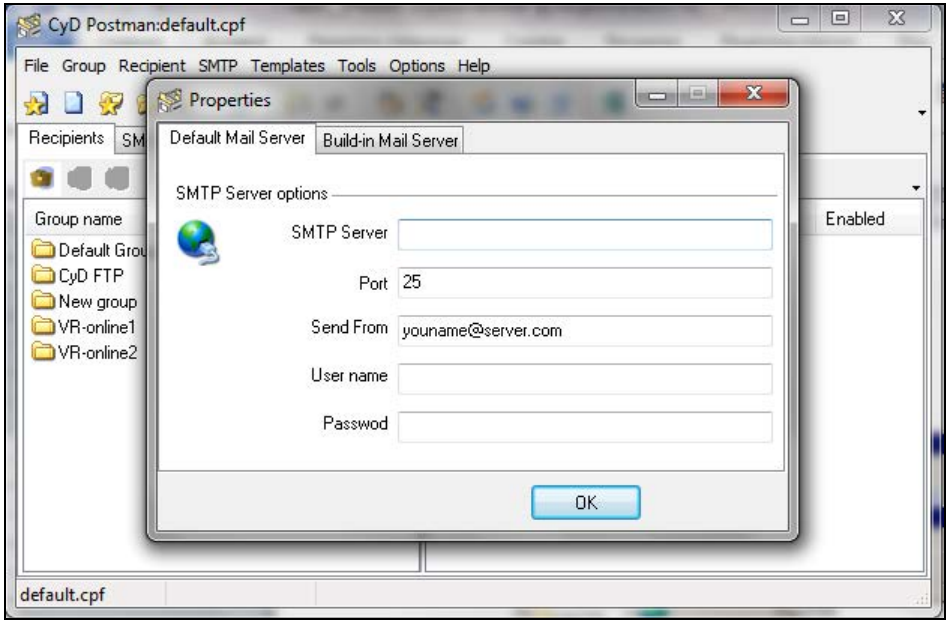


Рис. 5.10. Настройки программы Postman

2. Теперь самое время создать новую группу e-mail-адресов для рассылки. Для этого выберите меню **Group | New group**, введите имя группы и нажмите кнопку **OK**. Можно использовать название по умолчанию, но его лучше оставить для других рассылок, а для анонимных — сформировать отдельную группу, например "Анонимные письма".
3. Выделите группу и создайте в ней нового получателя. Для этого выберите меню **Recipient | New Recipient**. Перед вами откроется окно, в котором главное — заполнить e-mail-адрес. Все остальное нам ненужно. Сохраните изменения.
4. Выделите адресата, которому надо отправить письмо, и выберите пункт меню **Recipient | Send e-mail to selected users**. Перед вами откроется окно простого текстового редактора. Введите сообщение и нажмите кнопку **Send personalized e-mail** с изображением письма (вторая слева на панели инструментов). В следующем окне нужно указать метод отправки. Выберите **Use build in mail server** и нажмите кнопку **OK**.

На первый взгляд может показаться, что для отправки письма с помощью Postman нужно совершить много операций. Но это впечатление обманчиво, потому что половина этих действий — настройки, которые выполняются только один раз.

5.5.2. Подделка текста сообщения

Когда составляете электронное сообщение, необходимо стараться придерживаться того же стиля, как у жертвы. Желательно допускать такие же ошибки, потому что значительные изменения в орфографии бросаются в глаза и могут выдать вас.

Особое внимание нужно уделять приветствию и подписи. Если жертва использует определенный шаблон, то вы должны следовать ему. Например, шаблон сообщения может быть следующим:

> Hi, *Имя получателя*
>
> *Текст сообщения*
>
> ---
> Best regards, Jon Doe

Старайтесь обращать внимание на каждый нюанс. Если после приветствия и перед текстом письма жертва ставит пробел, то и у вас он должен быть. Изучите человека, письмо которого нужно подделать. Это уже из области социальной инженерии, потому что необходимо заставить получателя поверить, что сообщение отправляли не вы, а Jon Doe.

В посланиях очень часто используют смайлики. Каждый пишет их по-своему, и один человек может добавить ":)", а другой — ":)))))))". Обращайте внимание даже на эти мелочи, потому что из них складывается общая картина письма, и по стилю можно определить фальсификацию. Печатный стиль письма, как и письменный почерк, может быть уникальным.

5.5.3. Служебная информация

Несмотря на то, что мы подделали адрес отправителя, и ничто в тексте не будет указывать на вас, вычислить обман довольно просто. Достаточно только просмотреть служебную информацию.

В программе Почта Windows Live щелкните правой кнопкой мыши по любому письму и выберите в появившемся меню пункт **Свойства** (Properties). На вкладке **Подробно** (Details) открывшегося окна можно увидеть служебную информацию сообщения, которая может выглядеть так, как показано в листинге 5.4.

Листинг 5.4. Заголовок письма

```
Return-Path: <vms@tin.it>
Delivered-To: info@cydsoft.com
Received: (qmail 60106 invoked by uid 89); 20 Sep 2004 00:59:11 +0400
Received: from unknown (HELO tomts4-srv.bellnexxia.net) (209.226.175.10)
  by mx2.valuehost.ru with SMTP; 20 Sep 2004 00:59:10 +0400
```

```
Received: from HSE-Toronto-ppp130995.sympatico.ca ([64.228.69.82])
   by tomts31-srv.bellnexxia.net
   (InterMail vM.5.01.06.10 201-253-122-130-110-20040306) with SMTP
   id <200310.VQG998.tomts-srv.bellnexxia.net@HSE-Toronto-
                                                    ppp130.sympatico.ca>;
    Sun, 19 Sep 2004 14:31:10 -0400
Message-ID: <006201c49ed8$bd91ecbb$afbafb30@sjeph>
Reply-To: "=?windows-1251?B?U2hvcDR1?=" <lk@tin.it>
From: "=?windows-1251?B?U2hvcDR1?=" <vms@tin.it>
To:  =?windows-1251?B?wOPg7+jp?= <gz@mail.ru>
Subject: =?windows-1251?B?IsLF183bySIg9O7t4PDo6iE=?=
Date: Sun, 19 Sep 2004 22:11:30 +0400
Organization: =?windows-1251?B?Qmx1ZWxpZ2h0?=
MIME-Version: 1.0
Content-Type: multipart/related;
        boundary="----=_NextPart_000_001E_01C2AA85.597C61B6"
X-Priority: 3
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook Express 6.00.2800.1081
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2800.1081
```

В параметре `Received` перечисляются все серверы, через которые прошло письмо, по этим IP-адресам можно определить источник. В строке `X-Mailer` отображается информация о почтовом клиенте, который использовался при отправке. Если у вас редкий почтовый клиент, то это сразу же бросится в глаза.

Благо, что пользователи очень редко заглядывают в служебную информацию, потому что она сложна для чтения. Но вас она может спасти, если необходима идентификация истинного источника отправки. Для этого нужно сравнить два письма. Как правило, заголовки будут отличаться незначительно, потому что в большинстве случаев письма идут по одному и тому же маршруту.

5.6. Безопасность в сети

Во всемирной сети все процессы взаимосвязаны. Так, анонимность, которую мы рассмотрели в *разд. 5.4* и *5.5*, является начальным этапом безопасности. Если вы незаметны, то и взламывать ваш компьютер никто не будет. Правила защиты от вирусов, предложенные в *разд. 4.1*, и правильные настройки компьютера, описанные в *разд. 4.6*, тоже помогают решать эту проблему.

Но это еще не все. Есть несколько правил, которые вы должны соблюдать, чтобы безопасность была максимальной. Только в этом случае Интернет будет приносить лишь удовольствие от использования, а не проблемы от хакеров.

5.6.1. Закройте лишние двери

В *разд. 4.7* мы рассматривали, как с помощью службы доступа к файлам и принтерам можно добраться до открытых ресурсов компьютера. Немного позже мы по-

знакомимся со способом сканирования сети на предмет просмотра "расшаренных" ресурсов. В целях безопасности вы должны определиться, а нужны ли вам вообще такие ресурсы? Если вы работаете в локальной сети, то служба доступа к файлам и принтерам будет установлена по умолчанию, даже если вы не открываете ресурсы, а используете возможности сервера. Если вы ни с кем не обмениваетесь информацией, то логичным было бы не только отключить эту службу в свойствах соединения, а удалить ее вообще. В этом случае злоумышленник по определению не сможет воспользоваться данной дверью в ваш компьютер.

В *разд. 4.6* мы говорили о том, как можно отключить неиспользуемые сервисы. Это необходимо не только с точки зрения оптимизации работы системы, но и в целях безопасности. Например, я встречал много домашних компьютеров, на которых был установлен веб-сервер (как элемент Internet Information Services), который идет в поставке Windows 2000/XP/Vista/7 и, скорее всего, останется и в будущих версиях. Но большинство пользователей не смогло дать ответ, зачем он нужен? Удалите все ненужные сетевые компоненты, и взлом вашего компьютера через эти форточки станет невозможным, потому что у вас их просто не будет.

На каждом компьютере должны быть установлены и запущены только те службы, которые необходимы. Как правило, я использую экземпляр базы данных основного сервера сети, но иногда мне требуется со своего компьютера работать с локальной базой данных MS SQL Server. Но это происходит очень редко, и чтобы не открывать дополнительные порты и не загружать систему лишними сервисами, SQL Server не загружается автоматически, а запускается вручную только по мере надобности.

Таким образом, оптимизируя систему, мы повышаем ее надежность, стабильность, а главное — безопасность.

Компания Microsoft с недавних пор пошла по пути максимального повышения безопасности компьютеров на базе ОС Windows. Начиная с Windows Vista (в принципе, началось в XP, но серьезные изменения произошли в Vista) компания начала устанавливать далеко не все. Ну а если и ставится какой-то сервис, то не обязательно сразу же запускается.

Например, уже упомянутый IIS, который не нужен на домашнем компьютере, не будет запускаться автоматически. Даже если вы включите его запуск, то он будет стартовать в минимальной конфигурации, и будут задействованы только основные функции. Каждую дополнительную функцию нужно включать самому и это правильный подход, потому что если пользователь включит что-то лишнее, то это уже будет его ответственность.

5.6.2. Хранение паролей

Мало того, что пароли должны быть сложными, а лучше — неподдающимися подбору по словарю, так их еще надо правильно хранить. Я уже дал в *разд. 4.7.3* несколько рекомендаций по сокрытию паролей на локальном диске. Вы можете использовать мои советы или хранить все пароли в памяти, или придумать свой метод надежной защиты.

Где бы вы ни хранили пароли, никогда не доверяйте их системе Windows и программе Internet Explorer. Встроенная защита в них хороша, но все ошибаются, и если будет найдена уязвимость, позволяющая украсть пароли, например из IE, то вы можете распрощаться со своей приватностью. Дело в том, что сервисы Windows и IE постоянно находятся под пристальным вниманием злоумышленников. Взломать Windows — это цель большинства, ведь стоит получить доступ к недрам системы, и ты получаешь доступ к миллионам пользователей по всему миру.

На многих форумах или сайтах есть возможность сделать автоматический вход. В этом случае не надо будет всякий раз вводить пароль. Система сохранит ваши параметры доступа в файле cookie и при каждом входе будет автоматически извлекать их из этого файла. Я говорил, что файлы cookies доступны только одному сайту, и, на первый взгляд, защита будет приемлемой, но только в том случае, если вы не боитесь потери пароля.

Файлы cookies (и пароли в них) чаще всего вообще никак не шифруются, потому что программистам лень. Любой пользователь, севший за ваш компьютер и просмотревший нужный cookie, сможет узнать пароль и натворить от вашего имени бед. Вирусы и троянские программы так же нередко направляют свои усилия на поиск и воровство файлов cookies.

Я в Интернете читал одну статью, в которой кто-то из специалистов по безопасности вроде как продемонстрировал возможность воровства cookies-файлов, принадлежаших другим сайтам. Технология этой атаки не описывалась, но я подозреваю, что имелась в виду атака XSS (Cross Site Scripting, скрипт, обращающийся к разным сайтам), которая достаточно хорошо справляется с данной задачей. Если на сайте есть уязвимость к атакам XSS, то вполне возможно, что cookies будут украдены. Более подробно об этой атаке можно прочитать в [6].

5.6.3. BugTraq

Честно сказать, настоящих хакеров в мире не так уж и много. Большинство взломов совершается подростками, которым нечего делать и хочется где-то применить свои силы. Они в основном используют уже готовые решения, найденные настоящими хакерами. Это значит, что вы должны следить за новыми методами взлома и всеми появляющимися уязвимостями. Я для этого использую сайт **http://www.securityfocus.com/**. Здесь регулярно обновляется информация по этим вопросам и предлагаются способы защиты.

Уже давно ходят споры о том, нужны ли сайты наподобие **http://www.securityfocus.com/**. С одной стороны, они позволяют администраторам получать сведения об уязвимостях, а с другой — хакеры узнают, как можно взломать систему. Я считаю, что такие сайты должны существовать, проблема тут не в этом. Просто большинство администраторов никогда сюда не заходят, а узнают о наличии "тонких мест" в программном обеспечении только тогда, когда их сеть/сайт/сервер взломаны. Даже если вспомнить какую-либо брешь девяностых годов, можно найти в Интернете компьютер или сервер, который содержит эту уязвимость. Я бы таких администраторов увольнял без разговора.

Если вы думаете, что ежедневные проверки обновлений смогут спасти систему, то сильно ошибаетесь. После того как найдена уязвимость и до момента выхода обновления проходит некоторое время, и в этот период опасность проникновения на компьютер максимальная. Любой хакер, узнавший метод взлома, может начать штурм и обязательно добьется успеха. Вы должны раньше него узнать об уязвимости и принять меры по предотвращению вторжения, пока не появится обновление.

Страшно? Похоже на эпидемию? Да, именно так и было лет 10 назад и более. Тогда появление новых уязвимостей нередко сопровождалось эпидемиями, потому что:

- в программном обеспечении и ОС не было хорошо налаженной системы обновления, и с тех пор Microsoft сделала большой шаг в направлении безопасности. Да, как ни странно признавать, но эта компания иногда делает интересные и полезные вещи;
- безопасности уделялось намного меньше внимания, и не было такого широкого движения белых хакеров.

Белые хакеры — это специалисты по безопасности, которые следят за безопасностью, ищут уязвимости, но не используют ошибки в программном обеспечении, а сообщают об этом производителю и нередко помогают в исправлении. Поэтому большинство ошибок в настоящее время публикуется уже после того, как производитель выпустил исправление.

Когда специалисты находят ошибку, то сообщают об этом производителю и не публикуют информацию по уязвимости, пока производитель не выпустит патч. Все это, а также автоматическое обновление систем, позволяет предотвратить эпидемии. Взламывают компьютеры только тех пользователей, которые не обновляют системы или у которых нелицензионные копии продуктов. Но тут уже производитель не несет ответственности.

5.6.4. Брандмауэр

Если текст книги будет читать пессимист, то он будет в шоке от количества предостережений в этой главе. Нужно не только обновлять систему, но еще и ходить по какмим-то сайтам и следить за ошибками в программах. Это так, но только для администраторов. Домашним пользоватлеям незачем задумываться о том, что где-то в Интернете есть лента, в которой выкладывают все ошибки.

Я использую Интернет только для электронной почты и просмотра некоторых вебстраниц, и мне хватает регулярных обновлений системы и даже не нужно заглядывать на сайт **http://www.securityfocus.com/**. Если же вы проводите в сети много времени или ваша работа связана с выходом в Интернет, то нужно прибегнуть к более мощным средствам защиты. Если время пребывания в сети более 8 часов и не связано с работой, то это уже зависимость, которую надо лечить.

Каждый, кто регулярно посещает в Интернете места массового скопления народа, должен защищать свой компьютер. Например, когда вы находитесь в чате, то нет гарантии, что в это же время там не присутствует хакер. Через некоторые чаты или

каналы IRC (Internet Relay Chat, ретранслируемый интернет-чат) можно узнать IP-адрес компьютера любого собеседника и атаковать его. Во времена Windows 95 я регулярно слышал про то, как чей-то компьютер перезагружался сам по себе во время работы в Интернете. Современные ОС более надежны, и при соблюдении правил, описанных в данной книге, вероятность удачного нападения со стороны хакера уменьшается, но остается вполне реальной.

Чтобы защититься от атаки во время работы в Интернете нужны всего три составляющих:

1. Конечно же, стараться не посещать сомнительные места. Хакер ищет жертву для отладки и тестирования новых методов взлома на немодерируемых (неуправляемых) чатах и на каналах IRC. Все крупные сайты, предоставляющие возможность online-общения, обязательно управляют работой сервисов, но даже это не ограждает вас от встречи со злоумышленником. Лично я никогда не пользуюсь такими средствами общения, и ни разу мой компьютер не атаковали хакеры или вирусы. И при этом я никогда не применяю для защиты сетевые экраны или прокси-серверы.
2. Если общение в реальном времени необходимо, то следует скрывать свой IP-адрес. Для этого можно использовать прокси-серверы в Интернете *(см. разд. 5.4)*.
3. Нужно использовать хороший сетевой экран (firewall). Они бывают программные и аппаратные. Для домашнего компьютера приемлемым по цене и надежности вариантом является программная реализация. Аппаратная реализация дома — слишком дорогое и ненужное решение.

Начиная с Windows XP, в систему уже встроены функции фильтрации входящих соединений, что позволяет бесплатно использовать минимальные возможности сетевого экрана. Это необходимо, но далеко недостаточно для того, чтобы чувствовать себя в безопасности. Для большей надежности рекомендуется применять более мощный сетевой экран, который сможет обеспечить ваши потребности по качеству защиты и простоте использования. Во избежание рекламы я не буду давать никаких рекомендаций, а только рассмотрю некоторые наиболее популярные продукты.

- Agnitum Outpost Firewall — отличный сетевой экран российской разработки. Он является одним из лидеров в своем секторе, и не зря завоевал сердца большого количества пользователей по всему миру. Скачать его можно с сайта **http://www.agnitum.com/**.
- Sygate Personal Firewal — хороший экран со всеми необходимыми домашнему компьютеру функциями и удобным интерфейсом. Данный продукт является бесплатным для домашнего использования и при этом позволяет защититься от атак хакеров, троянских коней, атак DoS (Denial of Service, отказ от обслуживания). Сайт разработчика — **http://smb.sygate.com/**.
- McAfee Personal Firewall — экран с приличным сочетанием функциональности и стоимости. Фирма McAfee уже давно специализируется на разработке программ для защиты домашних компьютеров, и в сфере сетевых экранов представила нам достойный продукт. Единственный недостаток (на мой взгляд) — плохое отно-

шение к ресурсам системы, мой компьютер начал подтормаживать. Для скачивания зайдите на сайт **http://us.mcafee.com/**.

- Norton Personal Firewall — если раньше слово "Norton" ассоциировалось с Norton Commander, то теперь это торговая марка, под которой выходит множество средств для диагностики, защиты, восстановления и ремонта всего, что связано с компьютером и программами. Этот сетевой экран обладает, наверно, самым большим количеством необходимых домашнему пользователю защитных средств, но при этом он сложен и неудобен в настройках. Утяжеленный и внешне "страшный" интерфейс и медлительность современных программ от Symantec, на мой взгляд, является самым большим промахом этой компании, из-за которого исчез со сцены легендарный Norton Commander. Я как-то установил на свой домашний компьютр антивирус с сетевым экраном от этой компании, и мой компьютер начал невероятно тормозить. Сайт разработчика — **http://www.symantec.com/**.

С недавних пор функции сетевого экрана реализованы и в продуктах безопасности Лаборатории Касперского. Оценивать по качеству такие продукты тяжело, но по скорости не так уж и сложно. Из всех защитных средств продукты Касперского меньше всего тормозят систему, поэтому я бы первым делом взглянул на них. Это и отличная антивирусная защита, и защита компьютера от всех современных угроз.

На рис. 5.11 показан пример сети, защищенной через брандмауэр. Все запросы, которые поступают из Интернета или направляются туда, проходят через сетевой экран, который проверяет их по внутренним правилам. И если соответствие какому-нибудь правилу, разрешающему передачу, установлено, то пакет пропускается, иначе — просто удаляется.

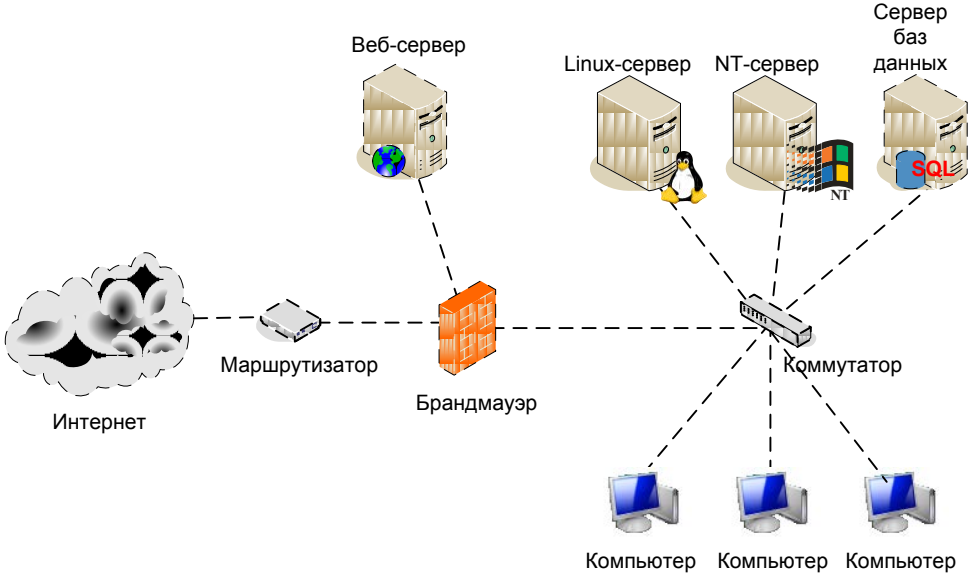


Рис. 5.11. Пример сети, защищенной через firewall от вторжения из Интернета

Вот какие могут быть правила:

- запрет на работу определенных протоколов. Например, можно блокировать использование 21 порта. Это значит, что из Интернета нельзя будет подключиться по протоколу FTP и закачать/скачать файлы, даже если на каком-либо из компьютеров сети, защищенной с помощью брандмауэра, запущен FTP-сервер. Единственный выход — запустить FTP-сервер на другом порту, который не запрещен сетевым экраном;
- запрет на определенные URL-адреса. В этом случае пользователи локальной сети не смогут зайти на некоторые сайты в Интернете, например, содержащие порнографию или нелегальное программное обеспечение;
- запрет на IP-адреса. На сетевом экране можно фильтровать желающих войти в контакт. Например, если фирма работает только с клиентами из США, то можно запретить входящие соединения из стран арабского и азиатского мира. Это только пример, ведь хакеры находятся не в этих странах, а большинство из них живет в Европе и США, поэтому такое ограничение не привнесет особой защиты;
- идентификация пользователя по паролю или любому другому средству типа Touch Memory, Smart Card или зашифрованная флешка.

В зависимости от сетевого экрана, вариантов правил может быть намного больше. Но уже сейчас видно, что он позволяет защищать локальную сеть не только от вторжения из Интернета, но и ограничить выход на определенные сайты, тем самым уменьшая вероятность нападения или заражения.

Но просто установить сетевой экран недостаточно, нужно правильно настроить программу и сформулировать эти правила. Для домашних компьютеров сетевые экраны конфигурируются практически автоматически, потому что здесь все достаточно просто, и основные усилия направлены на защиту от атак из Интернета и троянских программ, которые могут отправлять пароли в сеть. Чаще всего защитные комплексы для домашнего использования уже идут с предустановленными правилами, позволяющими вдохнуть полной грудью воздух свободы и безопасности.

Для домашнего пользователя сетевые экраны ставятся с правилом по умолчанию — запрещено все. Может быть сразу же разрешен доступ к обновлениям Windows или доступ к сайтам в Интернете через браузер. В случае если какая-то другая программа пытается установить соединение с Интернетом, то срабатывают защитные механизмы, отображающие на экране окно подтверждение, в котором пользователь должен явно разрешить такое соединение. Если пользователь сам запускал эту программу, то он подтвердит. Если вы ничего не запускали и не знаете программу, которая патается подключиться к сети, то это может быть вирус или троянская программа.

Сетевые экраны так же запрещают любые подключения к вашему Интернету из интрасети. Инициировать соединение должен клиент, а не сервер. Из-за этого могут возникнуть проблемы с некоторыми протоколами, например FTP, которые тре-

буют двухсторонних соединений. Но это единичные случаи, которые уже давно решены, и для FTP уже давно реализован пассивный режим, в котором все соединения инициируются клиентом.

Для корпоративных сетей ситуация намного сложнее, и уже нельзя доверяться автоматическим настройкам. Тут нужно следовать правилам безопасности, установленным в сети, и конфигурировать программу строго в соответствии с этими правилами. Дело в том, что в крупных сетях и компаниях сетевой экран находится на выделенном сервере, который соединяет локальную сеть с Интернетом. Этот сетевой экран просто не в состоянии вывести окно с подтверждением пользователю. Тут уже все правила конфигурируются администраторами.

Если в компании есть сетевой экран на выходе в Интернет, это не значит, что не нужно устанавливать дополнительную защиту на локальном компьютере и тем более отключать встроенные средства защиты ОС. Защита лишней не бывает, поэтому никогда не отключайте сетевой экран.

5.6.5. Сетевой экран — не панацея

Даже установив сетевой экран, вы не получаете полной защиты, потому что существуют варинаты обходы этой защиты. Самый банальный обход — использование подключения со стороны клиента к веб-серверу через IE. Браузер IE у бельшинства находится среди программ, которым система доверяет, и любой сетевой экран без дополнительных вопросов позволяет подключение к удаленным компьютерам на 80-й порт (используется для веб-серверов). Так как IE легко поддается управлению, любая троянская программа может обмениваться данными с управляющим центром посредством использования движка IE и HTTP-протокола.

Брандмауэр — это всего лишь замок на двери парадного входа. Злоумышленник никогда не воспользуется парадным входом, он будет проникать в систему через черный ход или полезет в окно. Например, на рис. 5.11 показана защищенная сеть, а ее главная дверь — это выход в Интернет через сетевой кабель. А если на какомнибудь клиентском компьютере стоит модем, то это уже черный ход, который не будет контролироваться сетевым экраном.

Я видел серверы, в которых доступ в сеть разрешен только с IP-адресов, определенных списком. Администраторы верят, что такое правило позволит защититься от хакеров. Это не так, потому что IP-адрес легко подделать.

Однажды я работал в фирме, где выход в Интернет контролировался по IP-адресу. У меня было ограничение на получение 100 Мбайт информации в месяц, а на соседнем компьютере был полный доступ. Чтобы не тратить свой трафик на получение больших файлов со своего IP-адреса, я только смотрел веб-страницы. Когда нужно было что-либо скачать, я выполнял следующие действия:

1. Дожидался, когда освободится нужный компьютер, например, когда хозяин уходил на обед.
2. Вытаскивал сетевой кабель на компьютере соседа, чтобы разорвать соединение.

3. Спокойно менял свой IP-адрес на соседский и быстро качал все, что требовалось, используя его безграничный трафик.
4. После скачивания возвращал IP-адрес и кабель на место.

Таким образом, я в течение месяца получал необходимую мне информацию.

Дальше стало еще проще. Я установил прокси-сервер на соседний компьютер и стал использовать его. После этого мы всем отделом заходили в Интернет через один IP-адрес, имеющий неограниченный трафик.

В современных сетевых экранах простая замена IP-адреса не позволит извне проникнуть в систему. Сейчас используются намного более сложные методы идентификации. С помощью подмены можно получить большие привилегии только в рамках сети, а не извне, да и то лишь при плохих настройках. Но хороший администратор даже внутри сети не допустит таких махинаций, потому что есть еще защита по MAC-адресу и пароли доступа.

Сетевые экраны могут работать на компьютере с ОС (программные) или на какомнибудь физическом устройстве (аппаратные). В любом случае это программа, а ее пишут люди, которым свойственно ошибаться. Как и ОС, так и программу сетевого экрана нужно регулярно обновлять и исправлять погрешности, которые есть всегда и везде.

Рассмотрим защиту по портам. Допустим, что у вас есть веб-сервер, который защищен сетевым экраном с разрешенным только 80 портом. А ему больше и не надо! Но это не значит, что нельзя будет использовать другие протоколы. Можно создать туннель, через который данные одного протокола передаются внутри другого. Так появилась знаменитая атака Loki, которая санкционирует передачу серверу команды на выполнение через ICMP-сообщения Echo Request (эхо-запрос) и Echo Reply (эхо-ответ), подобно команде `ping`.

Сетевой экран помогает защищать данные, но основным блюстителем порядка является администратор, который должен постоянно следить за безопасностью и выявлять атаки. Когда мы обсуждали вопросы защиты от вирусов *(см. разд. 4.1)*, я сказал, что новый его вид имеет шанс проникнуть практически в любую систему, потому что "вакцины" еще нет. Точно так же с атаками. Вновь разработанная атака сможет преодолеть сетевой экран, и компьютер ничего не заподозрит, потому что "заподозрить" его заставляют только заложенные в программу алгоритмы. Чтобы обработать нестандартную ситуацию, за системой должен наблюдать администратор, который будет реагировать на любые нештатные изменения основных параметров.

Для того чтобы пройти через сетевой экран, зачастую требуется пароль или предъявление какого-нибудь устройства типа Touch Memory, Smart Card и др. Если пароль не защищен, то все затраченные на сетевой экран деньги окажутся потерянными зря. Хакер может подсмотреть пароль или подслушать его с помощью анализатора пакетов (снифера) и предъявить подделанные параметры идентификации сетевому экрану. Таким образом было взломано немало систем.

Управление паролями должно быть четко определено. Вы должны контролировать каждую учетную запись. Например, если уволился сотрудник, у которого были

большие привилегии, то все сведения, определяющие его в ОС, необходимо тут же заблокировать и изменить все известные ему пароли.

Я всегда рекомендую, чтобы пароль с основными привилегиями на сетевой экран был известен только одному человеку, например начальнику информационного отдела, но никак не рядовому специалисту. Начальники меняются редко. Администраторы — достаточно часто, и после каждого их увольнения нужно не забыть поменять какой-нибудь пароль.

В качестве некоторой защиты от проблемы паролей уволенных сотрудников можно настроить политику безопасности так, чтобы учетные записи действовали только один месяц, после чего пароль должен меняться, иначе запись блокируется. Таким образом, уволенный и обиженный сотрудник сможет насолить бывшей компании максимально в течение месяца.

Именно поэтому описанная защита является неполной, ведь лазейка все равно остается, и нужен глаз да глаз. А если учесть, что обиженный на нечестное увольнение человек может сгоряча сразу полезть мстить, то защитой такое назвать очень тяжело.

5.6.6. Сетевой экран как панацея

Может сложиться впечатление, что брандмауэр — это пустое развлечение и трата денег. Это не так. Если он хорошо настроен, постоянно контролируется и обновляется, то сетевой экран может предотвратить большинство проблем.

Хороший экран имеет множество уровней проверки прав доступа, и нельзя использовать только один из них. В данном случае имеется в виду необходимость использования нескольких уровней, а не нескольких сетевых экранов. От количества экранов не всегда изменяется качество защиты, но лучше иметь все же два типа — один на входе в сеть и один на каждом клиентском компьютере.

Если вы ограничиваете доступ к Интернету исключительно по IP-адресу, то приготовьтесь оплачивать большой трафик. Но если при проверке прав доступа используется IP-адрес в сочетании с MAC-адресом и паролем, то такую систему взломать уже намного сложнее. Да, и MAC- и IP-адреса легко подделать, но можно для полной надежности подключить к системе защиты и порты на коммутаторе. В этом случае, даже если хакер будет знать пароль, то для его использования нужно сидеть именно за тем компьютером, за которым он закреплен.

Защита может и должна быть многоуровневой. Если у вас есть данные, которые нужно оградить от посторонних, то используйте максимальное количество уровней. Помните, что лишней защиты не бывает.

Представьте себе банк. У входа обязательно стоит секьюрити, который спасет от воров и мелких грабителей. Но если подъехать к такой организации на танке, то эта охрана не поможет.

Сетевой экран — это как охрана на дверях, защищает от мелких хакеров, которых подавляющее большинство. Но если вашей сетью займется профессионал, то он

может добиться успеха. Грубая сила иногда может позволить обойти экран, например, если хакер найдет ошибки переполнения стека или просто сможет произвести DoS-атаку.

Помимо охраны у входа, деньги в банке всегда хранятся в сейфе. Финансовые сбережения для банка — это как секретная информация для сервера, и они должны быть максимально защищены. Именно поэтому устанавливают сейфы со сложными механизмами защиты, и если не знать, как их обойти, вор потратит на вскрытие замка драгоценное время, и успеет приехать милиция.

В случае с сервером в роли сейфа может выступать шифрование, которое повышает гарантию сохранности данных. Даже если хакер проникнет на сервер, минуя сетевой экран, ему понадобится слишком много времени, чтобы расшифровать данные. Вы успеете заметить и вычислить злоумышленника. Ну а если взломщик скачал зашифрованные данные и пытается их расшифровать на своем компьютере, то с большой вероятностью можно утверждать, что информация раньше устареет, чем хакер сможет ее прочитать. Главное, чтобы алгоритм шифрования и ключ были максимально стойкими к подбору, особенно по словарю.

5.6.7. Виртуальная частная сеть

Одним из средств защиты является создание виртуальных частных сетей (VPN, Virtual Private Network). Допустим, что существует некая фирма с распределенной сетью филиалов, удаленных на большое расстояние, и для их соединения самым дешевым вариантом будет использование Интернета. Для того чтобы трафик не перехватили, применяется виртуальный канал, который шифруется и недоступен для хакера (рис. 5.12).

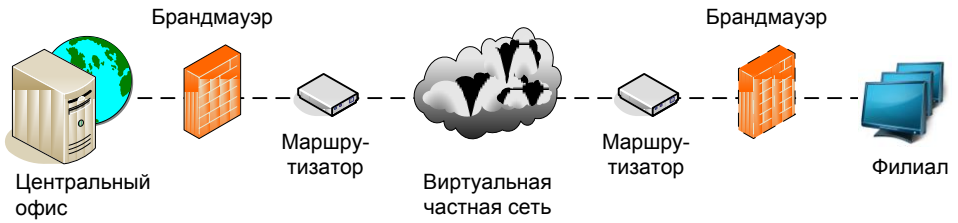


Рис. 5.12. Пример связи центрального офиса и филиала через VPN

Даже если кто-то перехватит трафик, проходящий по публичным сетям или каналам, этот трафик абсолютно бесполезный, потому что он зашифрован.

В настоящее время, благодаря большому количеству простых и удобных программ, построить такую сеть не составляет труда. На первый взгляд все безупречно. С обеих сторон стоят сетевые экраны, между ними — специальная связь, и проникнуть в систему невозможно. Но это так, пока не появится еще одна дверь. Допустим, что в филиале захотели получить доступ в Интернет для просмотра вебстраничек. Конечно же, этот трафик можно запустить через главный офис, но тогда любой запрос в Интернет должен будет идти через него, а не напрямую, что очень

дорого и накладно для канала, а потом уже из офиса к веб-серверу по другому каналу (оплачивается отдельно). Получается, что все запросы проходят по двум каналам, и за каждый мегабайт приходится платить дважды. К тому же сеть VPN имеет дополнительные расходы на шифрование простых веб-запросов и излишне нагружена.

Чтобы сэкономить деньги, большинство фирм кроме VPN для связи с офисом открывает отдельный канал для доступа в Интернет прямо из филиала, тем более, что там уже все равно, скорее всего, стоит сетевой экран (рис. 5.13).

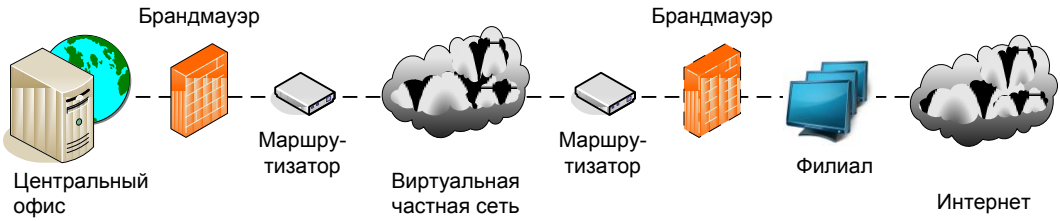


Рис. 5.13. Филиал с двумя выходами в Интернет

Все хорошо, но в главном офисе связи и защите всегда уделяют больше внимания, чем в филиалах, где в большинстве случаев нет своего администратора, а если даже и есть, то менее профессиональный и не такой опытный. Задача хакера — взломать филиал и войти в его сеть. Так как между филиалом и офисом установлены доверительные отношения, то хакер без проблем сможет из филиала получить доступ к главным серверам компании по VPN, и не надо будет взламывать шифрование.

Я работаю в Канаде, а большинство серверов, с которыми приходится работать, находятся в США. Не знаю почему, но многие любят использовать солнечные калифорнийские дейтацентры. Для того чтобы подключаться к дейтацентрам и оставлять мое соединение тайным, приходится использовать VPN.

5.6.8. Интернет — это зло

Когда я вел рубрику вопросов и ответов в журнале "Хакер", то однажды получил очень хороший вопрос: "Можно ли запустить ядерные ракеты США через Интернет?" Конечно же, это невозможно, но не потому, что компьютеры, управляющие пуском ракет, сильно защищены. Никакая система безопасности не может быть идеальной. Существует человеческий фактор: малейший неучтенный нюанс — и защита окажется взломанной хакером из какой-нибудь деревни.

Мы уже не раз слышали, как проникают на достаточно крупные сайты и серверы с великолепной системой защиты. А о скольких взломах умалчивают, чтобы не испортить имидж? Лично я никогда не доверю компьютеру через Интернет управлять даже краном на кухне. И такие страны, как США или Россия, не могут себе позволить подключить компьютеры, связанные с ядерным оружием, к Интернету, иначе войну сможет развязать какой-нибудь слишком умный хакер или не слишком добрый подросток :).

Стратегически важные данные должны храниться на компьютерах, не имеющих выхода в глобальную сеть. Однажды я проверял безопасность фирмы, занимающейся разработкой программного обеспечения. Руководители очень сильно заботились о сохранности исходных кодов, поэтому компьютеры программистов не имели дисководов, записывающих устройств или выхода в Интернет. Все машины были связаны в локальную сеть, и только одна из них имела флоппи-диск и записывающий CD-ROM для переноса данных на другие компьютеры. Таким образом, исходные коды крутились только в локальной сети, а утечка информации могла произойти лишь через единственный компьютер, и такая сеть легко контролировалась.

Если у вас есть информация, которую необходимо сохранить в тайне, то ее нужно изолировать от всемирной сети. После этих слов может показаться, что Интернет — это зло. Нет. Виноват тут не Интернет, а люди. Если пульт от ракетной установки поставить на улице, то какой-нибудь психически неуравновешенный человек когда-нибудь нажмет на нем опасную кнопку. Таких людей мало, и мир может прожить и 10 лет, и 20. Но все же, если кнопка доступна, то она когда-нибудь сработает. Интернет как улица. Он является виртуальным отражением нашей реальной жизни. В сети сейчас очень много людей. Когда-нибудь найдется человек, который по своей неопытности, случайности или глупости воспользуется оружием.

Люди не представляют себе угрозу, которую таят безобидные на первый взгляд вещи. Информация может нанести больший ущерб, чем атомная бомба, поэтому ее надо скрывать скрупулезнее, и при необходимости лучше не давать возможность воспользоваться.

В домашних сетях редко бывают ситуации, когда нужно так тщательно прятать информацию, а корпоративные случаи мы практически не рассматриваем. Но на данном аспекте я остановился, потому что это поможет вам в будущей работе или учебе.

Чаще всего взломы совершают неопытные хакеры в познавательных целях. Чтобы в домашних условиях изолировать себя от таких людей обычно достаточно просто спрятать компьютер. Выполните следующую команду:

```
net config server /hidden:yes
```

Теперь компьютер не будет виден в сетевом окружении. Но это не значит, что он недоступен. Зная IP-адрес, хакер может получить доступ напрямую, но в Интернете сетевого окружения нет, только прямая IP-адресация, ибо сеть в основном построена на данном протоколе.

А вот IP-адрес узнать не так уж и сложно. Достаточно просто проверить соединение со всеми адресами в локальной сети. Существует множество программ, которые позволяют сканировать диапазоны IP-адресов. В моей утилите CyD Network Utilities, которую я уже упоминал не раз, тоже есть такая возможность. Так что данный метод игры в прятки не сработает даже против начинающего взломщика.

5.6.9. Внутренний взлом

Очень сложно защититься от внутреннего взлома, т. е. человека, который заведомо имеет хоть какой-то доступ к ресурсам. К таким людям можно отнести сотрудников компании или ваших соседей, родителей, родственников.

Рассмотрим пример с родителями. Они могут знать пароль на ваш компьютер, потому что вы сами его дали. Но если вы поссоритесь с отцом из-за несданных экзаменов, то он может просто удалить все игры, чтобы вы больше уделяли времени учебе. Тут уж ничего не поделаешь, особенно, если отец не первый день работает за компьютером.

Я уже приводил пример с обиженным администратором фирмы. Такие люди знают все пароли и настройки безопасности, поэтому им не составит труда проникнуть в систему. От этого тоже никуда не деться. Нужно регулярно менять пароли, особенно после кадровых перестановок.

Некоторые люди страдают клептоманией или просто любят сделать другим что-то неприятное, поэтому специально похищают, удаляют или портят чужую информацию. Это, наверное, один из самых частых взломов, с которым мне приходилось встречаться. Например, один сотрудник допустил промашку. Чтобы скрыть все следы, он может подправить или стереть чужие данные.

5.7. Сканирование открытых ресурсов

Чтобы открывать файлы и папки на другом компьютере, у вас должен быть установлен клиент для той ОС, что установлена на нем. Например, если вы хотите видеть в сетевом окружении компьютеры на базе Windows, то необходимо, чтобы у вас был установлен **Клиент для сетей Microsoft** (Client for Microsoft Networks). Если вы хотите, чтобы ваши файлы и папки были доступны другим, то необходимо установить **Службу доступа к файлам и принтерам Microsoft** (File and Printer sharing for Microsoft Networks). Следовательно, если на чужом компьютере не установлена эта служба, то вы не увидите его файлы.

Эти службы устанавливаются в свойствах соединения. Выберите меню **Пуск | Панель управления | Центр управления сетями и общим доступом** (Start | Control Panel | Network and Sharing Center) и щелкните правой кнопкой по нужному соединению. В выпадающем меню необходимо выбрать пункт **Свойства** (Properties). В этом окне будет показан список всех установленных служб. Если у вас нет службы **Клиент для сетей Microsoft** (Client for Microsoft Networks), то вы не сможете произвести сканирование. Для установки нажмите кнопку **Установить** (Install). Если служба установлена, то необходимо убедиться, что напротив нее установлен флажок.

Теперь можно приступить к поиску компьютера в Интернете, где есть открытые папки. В этом нам помогут две программы:

- ipconfig — позволяет определить локальный IP-адрес;
- CyD NET Utils — умеет сканировать диапазон адресов на наличие открытых ресурсов. Эта же программа может определять IP-адрес.

Для начала с помощью командной строки запускаем программу ipconfig и определяем свой IP-адрес.

В результате вы увидите текст типа:

```
Windows IP Configuration
  Ethernet adapter Local Area Connection:
   Connection-specific DNS Suffix  . :
   IP-Address. . . . . . . . . . . . : 192.168.8.57
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.8.1
```

Если в компьютере установлено несколько сетевых карт, то может быть столько же IP-адресов. В данном случае только один адаптер (`Ethernet adapter Local Area Connection`) и адрес, соответственно, — 192.168.8.57.

У каждого интернет-провайдера свой диапазон IP-адресов, чаще всего он соответствует первым трем числам адреса. Они и обусловливают номер сети. Последнее число определяет номер компьютера. Конечно же, это не всегда справедливо, потому что в сочетании с IP-адресом используется номер, называемый *маской подсети*, позволяющий разбить сеть на более мелкие сегменты (узлы).

Маска определяет, сколько байт составлает адрес сети, а сколько — адрес узла (компьютера) внутри этой сети. Пусть, например, адрес компьютера — 192.168.8.57 и маска — 255.255.255.0. Первые три числа в маске 255, значит, первые три числа в адресе — это адрес сети. Последний ноль говорит, что последнее число в адресе — это адрес компьютера в сети. Еще пример: адрес — 192.168.8.57, маска — 255.255.0.0. По аналогии с предыдущим описанием 192.168 — это адрес сети, а 8.57 — адрес компьютера в этой сети. Провайдерам чаще всего достаются адреса, в которых можно устанавливать маску 255.255.255.0 или 255.255.0.0.

Адрес сети уникален, а внутри нее провайдер раздает адреса, как хочет (либо динамически, либо статически для выделенных линий). Например, у AOL может быть адрес сети 11.x.x.x (для такой сети маска 255.0.0.0), т. е. первое число 11 как раз указывает на адрес сети и этот адрес принадлежит AOL и только ей. Другая сеть не может иметь этот адрес. Остальные цифры AOL может раздавать компьютерам в своей сети, как хочет. У другого провайдера может быть адрес сети 192.168.x.x. (для такой сети маска 255.255.0.0). Здесь адрес сети — 192.168, и по этому адресу будет найдена сеть провайдера. Остальные числа описывают адреса компьютеров в сети провайдера.

Маска выбирается в зависимости от размера компании. Если это AOL, то для такой крупной компании понадобится большое количество адресов в сети и им будет выделена сеть класса C.x.x.x.

Тут нужно сделать еще одно замечание — первое число в адресе имеет определенное значение. По нему можно определить, какая максимальная маска может быть назначена данному адресу. Но это уже отдельная история, о которой можно прочитать в книгах по протоколу TCP/IP. Прочтите, это будет интересно.

Получается, что адрес сети — это как адрес дома, а адрес компьютера в сети — это как номер квартиры в этом доме. Что в адресе является адресом сети, а что адресом компьютера в сети определяется с помощью маски.

Компьютеры в сети провайдера (для данного примера) нумеруются от 192.168.8.1 до 192.168.8.254. Именно в этом диапазоне можно проводить сканирование. Запустите программу CyD NET Utils и выберите меню **Utils | Share scanner**. В появившемся окне введите в поле **From address** значение 192.168.8.1, а в поле **To address** — значение 192.168.8.57 (рис. 5.14). Нажмите кнопку **Scan** и ожидайте завершения сканирования. В строке состояния будет отображаться текущий адрес.

Если программа найдет открытый ресурс, то вы увидите его адрес, например **\\192.168.8.1\ftp**. Чтобы просмотреть его содержимое, достаточно ввести этот параметр в строке браузера или просто в окне **Computer** (Компьютер). На самом деле окно **Computer** (Компьютер) — это тоже Internet Explorer.

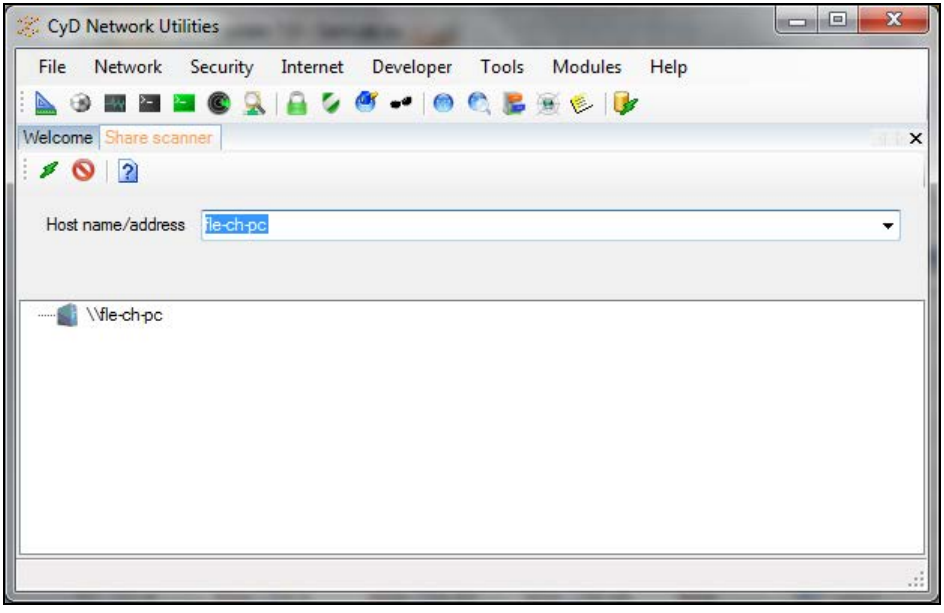


Рис. 5.14. Сканирование ресурсов с помощью CyD NET Utils

Преимущество программы CyD NET Utils в том, что перед попыткой просканировать адрес проверяется связь с помощью команды `ping`. Поиск открытых ресурсов в Windows происходит очень долго, и если адрес не существует, то нет смысла тратить усилия. Благодаря предварительной и быстрой команде `ping` можно быстро узнать, существует ли компьютер в сети и имеет ли смысл его сканировать.

С другой стороны, это обстоятельство можно расценивать, как недостаток. Сейчас очень многие сетевые экраны запрещают команду `ping`, поэтому программа может не просканировать существующий адрес. Но я не думаю, что стоит обращать внимание на данный факт.

5.8. Атаки хакеров

Невозможно дать определенные рецепты взломов. В каждом случае это творческий процесс, который зависит от конкретной системы и настроек ее безопасности. Чаще всего используются ошибки в программах, а каждый администратор может использовать различный софт.

Почему количество атак с каждым годом только увеличивается? Раньше вся информация об уязвимостях хранилась на закрытых BBS (Bulletin Board System, электронная доска объявлений) и была доступна только избранным. К этой категории относились и хакеры, совершавшие безнаказанные атаки, потому что уровень их просвещенности и опытности был достаточно высок.

В настоящее время сведения об уязвимостях стали достоянием общественности. Теперь взломом, в принципе, может заниматься кто угодно. Злоумышленники при этом могут преследовать одну из следующих целей.

- Хищение информации — вскрытие сервера для скачивания каких-либо данных, которые не должны быть доступны широкой общественности. Такие взломы чаще всего направляют против определенных компаний для кражи отчетности, исходных кодов программ, секретной документации и т. д. Как правило, такие взломы совершают профессиональные хакеры по заказу или для получения собственной выгоды.
- Нарушение целостности — изменение или уничтожение данных. Такие операции могут производиться против любых серверов в сетях Internet/Intranet. В качестве взломщиков могут выступать не только профессионалы, но и любители, или даже недовольные сотрудники фирм.
- Отказ в обслуживании — атака на сервер с целью сделать его недосягаемым для остальных участников сети. Такие действия присущи в основном любителям с одной только целью — навредить. Самое интересное, что такие атаки чаще происходят против каких-либо крупных компаний по идеологическим причинам. Например, несколько раз производились попытки навредить компании Microsoft. Нетрудно догадаться, что это делали ненавистники ОС Windows и Билла Гейтса в частности.
- Порабощение — получило распространение в последнее время. Например, для выполнения предыдущего пункта могут понадобиться большие ресурсы (мощный процессор и высокоскоростной доступ в сеть), которые отсутствуют в домашних компьютерах. Для этого захватывается какой-нибудь слабо защищенный сервер в Интернете, обладающий необходимыми техническими средствами, и используется в дальнейших взломах. Компьютеры и серверы, которые хакер использует в личных целях, называют рабами.

Атаки могут быть двух видов.

- Внутренние — хакер получил физический доступ к взламываемому компьютеру. Защитить системный блок сервера от злоумышленника не так уж и сложно, потому что можно преградить путь к серверу сейфом и поставить охрану. Вопрос в другом: это действительно нужно?

- Внешние — взлом через сеть. Именно этот вид атаки является самым интересным для защиты. Даже если для предотвращения удаленной атаки поставить замечательный "сейф" (firewall) и лучшую охрану для наблюдения (программы мониторинга и журналирования), безопасность не может быть гарантирована. Примерами этого являются нашумевшие взломы наиболее защищаемых серверов в сети (yahoo.com, microsoft.com, серверы NASA и т. д.).

Когда мы строим линию обороны, необходимо понимать, как хакеры атакуют компьютеры своих жертв. Только тогда можно предотвратить нежелательное вторжение и защитить систему. Давайте рассмотрим основные способы нападения, используемые хакером. При этом будем рассуждать так, как это делает взломщик.

Единственное, чего мы не будем касаться в этом разделе, — вопросов социальной инженерии *(см. разд. 5.3)*, которые могут использоваться для получения каких-либо данных, на любом этапе взлома.

5.8.1. Исследования

Допустим, что у вас на примете есть сервер, который нужно взломать или протестировать на защищенность от взлома. С чего нужно начинать? Что сделать в первую очередь? Сразу очень много вопросов и ни одного ответа.

Четкой последовательности действий нет. Взлом — это творческий процесс, а значит, и подходить к нему надо с этой точки зрения. Нет определенных правил, и нельзя все подвести под один шаблон. Зато есть несколько рекомендаций, которых желательно придерживаться.

Самое первое, с чего начинается взлом или тест ОС на уязвимость — сканирование портов. Для чего? А для того чтобы узнать, какие сервисы (в Linux это демоны) установлены в системе. Каждый открытый порт — это сервисная программа, установленная на сервере, к которой можно подключиться и выполнить определенные действия. Например, на 21 порту висит FTP-сервис. Если вы сможете к нему подключиться, то станет доступной возможность скачивания и закачивания на сервер файлов. Правда, для этого нужно обладать соответствующими правами.

Сначала нужно просканировать первые 1024 порта. Среди них очень много стандартных сервисов типа FTP, HTTP, Telnet и т. д. Каждый открытый порт — это дверь с замочком для входа на сервер. Чем больше таких дверей, тем больше вероятность, что какой-то засов не выдержит натиска и откроется. Именно поэтому я рекомендовал вам убрать из автозапуска все неиспользуемые сервисы *(см. разд. 4.6.2 и 4.6.3)*.

У хорошего администратора открыты только самые необходимые порты и не установлено ничего лишнего. Например, если это веб-сервер, не предоставляющий доступ к почте, то нет смысла держать почтовые сервисы. Должен быть открыт только порт 80, на котором как раз и работает веб-сервер.

Хороший сканер портов определяет не только номер открытого порта, но и показывает название установленного на нем сервиса (жаль, что не настоящее, а только имя возможного сервера). Так, для 80 порта будет показано "http". Желательно, чтобы

сканер умел сохранять результат своей работы в каком-нибудь файле и даже распечатывать. Если этой возможности нет, то придется переписать все вручную и положить на видное место. В дальнейшем вам пригодится каждая строчка этих записей.

После этого можно сканировать порты свыше 1024. Здесь стандартные сервисы встречаются редко. Зачем же тогда сканировать? А вдруг кто-то до вас уже побывал на этом месте и оставил открытую дверку или установил на сервер троян. Большинство троянских программ держат открытыми порты свыше 1024, поэтому если вы администратор и нашли открытый порт в этом диапазоне, необходимо сразу насторожиться. Ну а если вы взломщик, то нужно узнать имя троянской программы и найти для нее клиентскую часть, чтобы воспользоваться для управления чужой машиной. Хотя этот случай из ряда фантастики, его исключать нельзя. Фантастика иногда преавращается в реальность.

Помимо этого, на портах выше 1024 работает множество других программ, например, базы данных.

На этом взлом может закончиться, если вы нашли дверь и уже получили полный доступ к серверу. Однако такое происходит очень редко, и чаще всего нужно затратить намного больше усилий.

Теперь мы знаем, какие двери у сервера открыты. Но этого мало, потому что мы еще не ведаем, как их открыть.

Определение ОС

Сканирование — это всего лишь начальный этап, который дал вам информацию для размышления. Самое главное — узнать, какая именно установлена ОС. Желательно иметь сведения о версии, но это удается не всегда, да и на первых парах изучения системы можно обойтись без конкретизации.

Хотел бы посоветовать какую-то определенную программу, но не могу доверять никому кроме себя. В первом издании я рекомендовал Shadow Scan, который можно найти по адресу **http://www.safety-lab.com/en/products/securityscanner.htm**, но если честно, то я сам им давно не пользовался и не знаю, как работает его последняя версия. Раньше была очень удобная программа.

Кроме ОС желательно определять версии установленных сервисов. Это вам может очень сильно помочь. Допустим, вы узнали, что на компьютере установлен веб-сервер. Помимо этого известно, что используется операционная система Windows. Можно предположить, что веб-сервер именуется IIS, но эта гипотеза может не подтвердиться. Для Windows есть реализация сильнейшего сервера Apache. Могут быть установлены и другие веб-серверы, хотя самые популярные — именно эти два. А т. к. взлом различных серверов производится по-разному, то в первую очередь нас интересует, кто конкретно сидит на 80 порту.

Единственный недостаток Shadow Scan — именно при определении версии ОС некоторые релизы показывали синий экран. Но в последнем варианте эта ошибка, кажется, исправлена.

Как определяется тип ОС? Для этого есть несколько способов.

- *По реализации протокола TCP/IP.*

  В различных операционных системах по-разному организован стек протоколов. Программа может анализировать ответы сервера на запросы и давать заключение об установленной ОС. В основном этот вывод расплывчатый: Windows или Linux. Точную версию таким образом узнать невозможно, потому что, начиная с Windows 2000, реализация протокола практически не менялась, и отклики сервера будут одинаковыми. Даже если программа определила, что на сервере установлен Linux, то какой именно дистрибутив — вам никто не скажет, а ведь уязвимости в них разные. И поэтому такая информация — это только часть необходимых вам данных для взлома сервера.

- *По ответам разных сервисов.*

  Допустим, что на сервере жертвы есть анонимный доступ по FTP. Вам нужно всего лишь присоединиться к нему и посмотреть сообщение при входе в систему. По умолчанию в качестве приглашения используется надпись типа "Добро пожаловать на сервер FreeBSD4.0, версия FTP-клиента X.XXX". Если вы такое увидели, то еще рано радоваться, т. к. не известно, правда это или нет.

  Если надпись приглашения отражает действительность, то администратор — "чайник" со свистком, т. е. со стажем. Опытный администратор всегда изменяет приглашение, заданное по умолчанию. А вот хороший специалист может написать и ложное сообщение. Тогда на сервере с Windows NT 4.0 появится приглашение, например, в Linux. В этом случае злоумышленник безуспешно потратит очень много времени в попытках сломать Windows NT через дыры Linux. Поэтому не очень доверяйте надписям и старайтесь перепроверить любыми другими способами.

- *Социальная инженерия.*

  Если вы хотите взломать сервер хостинговой компании, то можно обратиться с письменным запросом об установленных у нее серверах в службу поддержки. Как правило, такая информация не скрывается, но бывают случаи откровенного вранья. Возможно, эти сведения будут лежать на главной странице сервера, но даже их следует проверить.

Чтобы вас не обманули, обязательно обращайте внимание на используемые на сервере сервисы, например в Linux не будут крутиться страницы, созданные по технологии ASP. Могут, но не будут. Такие вещи подделывают редко, хотя и это возможно. Достаточно немного постараться: использовать расширение asp для хранения PHP-сценариев и перенаправлять их интерпретатору PHP. Таким образом, хакер увидит, что на сервере работают файлы asp, но реально это будут PHP-сценарии.

Следовательно, задача защищающейся стороны — как можно сильнее запутать ситуацию. Большинство неопытных хакеров верит первым впечатлениям и потратит очень много времени на бесполезные попытки проникновения. Таким образом, вы сделаете взлом слишком дорогим занятием.

Задача хакера — распутать цепочки и четко определить систему, которую он взламывает. Без этого производить в дальнейшем какие-либо действия будет сложно, потому что хакер даже не будет знать, какие команды ему доступны после вторжения на чужую территорию, и какие исполняемые файлы можно подбрасывать на сервер.

Используем скрипты

Итак, теперь вы в курсе, какая на сервере установлена ОС, какие порты открыты и какие именно серверы висят на этих портах. Всю добытую информацию нужно записать в удобном для восприятия виде: в файле или хотя бы на бумаге. Главное, чтобы было комфортно работать.

Не ленитесь все собранные данные складывать в общую стопку. Помните, что даже компьютерные мозги иногда сбоят, а человеческие — делают это регулярно. Самое интересное, что чаще всего забывается наиболее необходимое. Ну а после взлома не забудьте уничтожить все записи, это может послужить доказательством содеянного в любом суде.

У вас есть достаточно информации для простейшего взлома с помощью дыр в ОС и сервисах, установленных на сервере. Просто посещайте регулярно **http://www.securityfocus.com/** или мой проект **http://www.securitylab.ru/**. Именно здесь нужно искать информацию о новых уязвимостях. Уже давно известно, что большая часть серверов (по разным источникам, от 70 до 90%) просто не латается или латается, но не вовремя. Поэтому проверяйте все найденные ошибки на жертве, возможно, что-то и сработает.

Очень рекомендую сайт **www.securitylab.ru**. Помимо того что там легко найти скрипты и программы для взлома, на нем так же можно пообщатся с интересными и умными людьми.

Я не знаю, как берут статистику о количестве нелатаемых серверов, но мне кажется, что она сильно завышена, чтобы пугать людей. Реально не латается не так уж и много серверов, и очень часто они просто не так интересны кому-то.

Если сервер в данный момент близок к совершенству, то придется ждать появления новых дыр и сплоитов (программ, позволяющих использовать уязвимость) к установленным на сервере сервисам. Как только увидите что-нибудь интересное, сразу качайте сплоит (или напишите свой) и воспользуйтесь им, пока администратор сервера не залатал очередную уязвимость.

Небольшое лирическое отступление. Я тут назвал диапазон нелатанных серверов — от 70 до 90%. Это средние данные, которые я видел в Интернете, но я не могу согласиться с таким количеством. Точные данные никто назвать не может, а большие цифры придуманы компаниями, предлагающими услуги по безопасности, дабы запугать пользователей и клиентов. На мой взгляд, реальные цифры в районе 20—30%, но и это очень много.

Автоматизация

Практически каждый день специалисты по безопасности находят в разных системах недочеты, откровенные дыры или даже пробоины в системе безопасности. Все

эти материалы выкладываются в отчетах BugTraq на разных серверах. Я уже не раз советовал посещать такие сайты, чтобы следить за новостями, и сейчас не отказываюсь от своих слов. Новинки действительно можно найти именно так, но ведь есть целый ворох старых уязвимостей, которые существовали, и еще не залатаны на сервере. Как же поступить с ними? Неужели придется качать все сплоиты и руками проверять каждую дыру? Ну, конечно же, нет. Существует громадное количество программ для автоматизации тестирования сервера на ошибки, и самые распространенные — SATAN, Internet Scanner, NetSonar, CyberCop Scanner.

Я не стану рекомендовать какую-нибудь определенную программу. Не существует такой утилиты, в которой была бы база абсолютно всех потенциальных уязвимостей. Поэтому скачивайте все, что попадется под руку, и тестируйте систему всеми доступными программами. Возможно, что-то вам и пригодится. Но обязательно обратите внимание на продукты компании Internet Security Systems (ISS, системы интернет-безопасности, доступные по адресу **http://www.iss.net/**). На данный момент, похоже, что эту компанию купила IBM, но кто будет владеть сканерами безопасности в будущем году, покажет время. Сканеры этой фирмы (Internet Scanner, Security Manager, System Scanner и Database Scanner) используют все три метода сканирования, о которых мы поговорим чуть позже. Сотрудники ISS работают в тесном контакте с Microsoft и постоянно обновляют базу данных уязвимостей. Но, несмотря на то, что продукты этой фирмы — лучшие, я советую использовать хотя бы еще один сканер другого производителя.

Компания Internet Security Systems разработала целый комплект утилит под общим названием SAFEsuite. В него входят не только компоненты проверки безопасности системы, но и модули выявления вторжения и оценки конфигурации основных серверных ОС.

Сканеры безопасности, как и антивирусы, защищают хорошо, но только от старых приемов. Любой новый метод взлома не будет обнаружен, пока вы не обновите программу, а точнее, базу данных уязвимостей. Поэтому я не рекомендую целиком и полностью полагаться на отчеты автоматизированного сканирования, а после работы программы самостоятельно проверить наличие последних уязвимостей, описанных в каком-либо бюллетене ошибок (BugTraq).

С помощью автоматизированного контроля очень хорошо производить первоначальную проверку, чтобы убедиться в отсутствии старых ляпсусов. Если ошибки найдены, то нужно обновить уязвимую программу, ОС или сервис или поискать в Интернете способ обезвреживания. Почти всегда вместе с описанием уязвимости дается вакцина, позволяющая залатать прореху в сервисе или ОС. Вакцину может предложить и программа сканирования, если в базе данных есть решение проблемы для данного случая.

Почему даже после лучшего и самого полного сканирования нельзя быть уверенным, что уязвимостей нет? Помимо новых ошибок в сервере надо принять во внимание еще и фактор конфигурации. На каждом сервере могут быть свои настройки, и при определенных условиях легко находимая вручную уязвимость может остаться незаметной для автоматического сканирования. На сканер надейся, а сам — не

плошай. Так что продолжайте тестировать систему на известные вам ошибки самостоятельно.

Каждый сканер использует свои способы и приемы, и если один из них не нашел ошибок, то другой может отыскать. Специалисты по безопасности любят приводить пример с квартирой. Допустим, что вы пришли к другу и позвонили в дверь, но никто не открыл. Это не значит, что дома никого нет, просто хозяин мог не услышать звонок, или звонок не работал. Но если позвонить по телефону, который лежит в этот момент возле хозяина, то он возьмет трубку. Может быть и обратная ситуация, когда вы названиваете по телефону, но его не слышно, а на звонок в дверь домочадцы отреагируют.

Так и при автоматическом сканировании: один сканер может позвонить по телефону, а другой — постучит в дверь. Они оба хороши, но в конкретных случаях при разных конфигурациях сканируемой машины могут быть получены различные результаты.

Существуют три метода автоматического определения уязвимости: сканирование, зондирование и имитация. В первом случае сканер собирает информацию о сервере, проверяет порты, чтобы узнать, какие установлены сервисы/демоны, и на основе их выдает отчет о потенциальных ошибках. Например, сканер может проверить сервер и увидеть на 21 порту работающую службу FTP. По строке приглашения (если она не была изменена), выдаваемой сервером при попытке подключения, можно определить его версию, которая сравнивается с базой данных. И если в базе есть уязвимость для данного сервера, то пользователю выдается соответствующее сообщение.

Сканирование — далеко не самый точный процесс, потому что автоматическое определение легко обмануть, да и уязвимости может не быть. Некоторые погрешности в сервисах проявляются только при определенных настройках, т. е. при установленных вами параметрах ошибка не обнаружится.

При зондировании сканер не обследует порты, а проверяет программы на наличие в них уязвимого кода. Этот процесс похож на работу антивируса, который просматривает все программы на наличие соответствующего кода. Ситуации похожие, но искомые объекты разные.

Метод хорош, но одна и та же ошибка может встречаться в нескольких программах. И если код в них разный, то сканер ее не обнаружит.

Во время имитации программа моделирует атаки из своей базы данных. Например, в FTP-сервере может возникнуть переполнение буфера при реализации определенной команды. Сканер не будет выявлять версию сервера, а попробует выполнить инструкцию. Конечно же, это приведет к зависанию, но вы точно будете знать о наличии или отсутствии ошибки на нем.

Имитация — самый долгий, но надежный способ. При этом программа пытается взломать систему программно. Если ей удалось взломать какой-либо сервис, то и у хакера это получится. Именно поэтому данный метод является самым точным и надежным. При установке нового FTP-сервера, который еще неизвестен сканерам, он будет опробован на уже известные ошибки других серверов. Очень часто про-

граммисты разных фирм допускают одни и те же ошибки, при этом методом сканирования анализатор может не найти подобную уязвимость только потому, что для данной версии нет записей в базе данных. А вот программная попытка взлома может дать результат.

Когда проверяете систему, обязательно отключайте сетевые экраны. Если блокирован доступ, то сканер не сможет протестировать нужный сервис. В этом случае анализатор сообщит, что ошибок нет, но реально они могут быть. Конечно же, это не критичные ошибки, если они под защитой сетевого экрана, но если хакер найдет потайной ход и обойдет сетевой экран, то уязвимость станет опасной.

Дайте сканеру все необходимые права и доступ к сканируемой системе. Например, некоторые считают, что наиболее эффективно удаленное сканирование выполняется тогда, когда по сети имитируется атака. Это правильно, но сколько времени понадобится на проверку стойкости паролей для учетных записей? Очень много! А сканирование реестра и файловой системы станет невозможным. Поэтому локальный контроль может дать более качественный результат.

При дистанционном сканировании только производится попытка прорваться в сеть. Такой анализ может указать на стойкость защиты от нападения извне. Но по статистике большинство взломов происходит изнутри, когда зарегистрированный пользователь поднимает свои права и тем самым получает доступ к запрещенной информации. Хакер тоже может иметь какую-нибудь учетную запись с минимальным статусом и воспользоваться уязвимостями для повышения прав доступа. Поэтому сканирование должно происходить и дистанционно для обнаружения потайных дверей, и локально для выявления ошибок в конфигурации, с помощью которых можно изменить привилегии.

Автоматические сканеры проверяют не только уязвимости ОС и ее сервисов, но и сложность пароля, и имена учетных записей. В анализаторах есть база наиболее часто используемых имен и паролей, и программа перебором проверяет их. Если удалось проникнуть в систему, то выдается сообщение о слишком простом пароле. Обязательно замените его, потому что хакер может использовать тот же метод, и легко узнает параметры учетной записи.

Анализаторы безопасности могут использовать как хакеры, так и администраторы. Но задачи у них разные. Одним нужно автоматическое выявление ошибок для последующего применения, а вторые используют его с целью закрытия уязвимости, причем желательно сделать это раньше, чем ту же уязвимость найдет и будет использовать хакер.

5.8.2. Взлом WWW-сервера

При взломе WWW-сервера есть свои особенности. Если на нем выполняются CGI/PHP или другие сценарии, то взлом проводится совершенно по-другому. Для начала нужно просканировать сервер на наличие уязвимых CGI-сценариев. Вы не поверите, но опять же, по исследованиям различных компаний, в Интернете работает большое количество "дырявых" скриптов. Это связано с тем, что при разработ-

ке сайтов изначально вносятся ошибки. Начинающие программисты очень редко проверяют входящие параметры в надежде, что пользователь не будет изменять код странички или адрес URL, где серверу передаются необходимые данные для выполнения каких-либо действий. В этой главе мы уже рассматривали, как можно накрутить счетчик с помощью изменения странички и подделки IP-адреса *(см. разд. 5.2)*. Это стало возможным потому, что программисты понадеялись на добросовестность посетителей. А зря.

Ошибку с параметрами имела одна из знаменитых систем управления сайтом — PHP-nuke. Это набор скриптов, позволяющих создать форум, чат, новостную ленту и управлять содержимым сайта. Все параметры в скриптах передаются через строку URL браузера, и просчет содержался в параметре ID. Разработчики предполагали, что в нем будет передаваться число, но не проверяли это. Хакер, знающий структуру базы данных (а это не сложно, потому что исходные коды PHP-nuke доступны), легко мог поместить SQL-запрос к базе данных сервера в параметр ID и получить пароли всех зарегистрированных на сайте пользователей. Конечно, пароли клиентов будут зашифрованы, но для расшифровки не надо много усилий, и это мы рассмотрим чуть позже.

Проблема усложняется тем, что некоторые языки (например, Perl) изначально не были предназначены для использования в Интернете. Из-за этого в них существуют опасные функции для манипулирования системой, и если программист неосторожно применил их в своих модулях, то злоумышленник может воспользоваться такой неосмотрительностью.

Потенциально опасные функции есть практически везде, только в разных пропорциях. Единственный более или менее защищенный язык — Java, но он очень сильно тормозит систему и требует много ресурсов, из-за чего его неохотно используют веб-мастера. Но даже этот язык в неуклюжих руках может превратиться в большие ворота для хакеров с надписью "Добро пожаловать!"

Но самая большая уязвимость — неграмотный программист. Из-за нехватки специалистов в этой области программированием стали заниматься все, кому не лень. Многие самоучки даже не пытаются задуматься о безопасности, а взломщикам это только на руку.

Итак, ваша первостепенная задача — запастись парочкой хороших CGI-сканеров. Какой лучше? Ответ однозначный — ВСЕ. Даже самый дрянной сканер может найти брешь, о которой неизвестно даже лучшему хакеру. А главное, что по закону подлости именно она окажется доступной на сервере. Помимо этого, не забываем заглядывать на сайты BugTraq за свежей информацией.

О взломе веб-серверов более подробно можно прочитать в книге "Web-сервер глазами хакера" [6], о которой я уже говорил.

Взлом WWW через поисковик

За последние 10 лет Интернет разросся до таких размеров, что найти в нем что-либо без хорошей поисковой системы стало невозможно. Первые системы просто индексировали страницы по их содержимому и потом использовали полученную

базу данных для поиска, который давал очень приблизительные результаты. Если ввести в качестве контекста слово "лук", то результатом будет огромное количество сайтов по пищевой промышленности и по стрельбе из лука. В большинстве языков есть слова, которые имеют несколько значений, и по ним поиск затруднителен.

Проблема не только в двусмысленности некоторых слов. Есть множество широко употребляемых выражений, по которым тоже сложно произвести точную выборку. В связи с этим поисковые системы стали развиваться, и теперь можно добавлять в запрос различные параметры. Одной из самых мощных является поисковая система Google (**http://www.google.com** или **http://www.google.ru**). В ней реализовано много возможностей, позволяющих сделать поиск более точным. Жаль, что большинство пользователей не освоило их, а вот взломщики изучили все функции и используют их в своих целях.

Один из самых простых способов взлома — найти с помощью поисковой системы закрытую веб-страницу. Некоторые сайты имеют засекреченные области, к которым доступ осуществляется по паролю. Сюда же относятся платные ресурсы, где защита основана на проверке пароля при входе, а не на защите каждой страницы и использовании SSL. В таких случаях Google проиндексирует запрещенные страницы, и их можно будет просмотреть через поиск. Для этого всего лишь надо четко знать, какая информация хранится в файле, и как можно точнее составить строку поиска.

Поиск индексированных секретов

С помощью Google можно найти достаточно важные данные, которые скрыты от пользователя, но по ошибке администратора стали доступными для индексирующей машины Google. Во время поиска нужно правильно задавать параметры. Например, можно ввести в строку поиска следующую команду:

```
Годовой отчет filetype:doc
```

или

```
Годовой отчет filetype:xls
```

И вы найдете все документы в формате Word или Excel, содержащие слова "Годовой отчет". Возможно, документов будет слишком много, поэтому запрос придется ограничить сильнее, но кто ищет, тот всегда найдет.

Поиск уязвимых сайтов

Допустим, вы узнали, что в какой-либо системе управления сайтом появилась уязвимость. Что это за система? Существует множество платных и бесплатных готовых программ, написанных на PHP, Perl и других языках и позволяющих создать сайт без особых усилий. Такие системы могут включать в себя готовые реализации форумов, гостевых книг, лент новостей и т. д. Например, phpbb или ikonboard, которые очень сильно распространены в Интернете — наиболее популярные исполнения форумов.

Если в какой-нибудь из таких специальных программ найдена критическая уязвимость, то все сайты в Интернете, использующие ее, подвергаются опасности. Большинство администраторов не подписано на новости и не обновляет свои скрипты, поэтому остается только найти нужный сайт и воспользоваться готовым решением для осуществления взлома.

Как найти сайты или форумы, которые содержат уязвимость? Очень просто. Чаще всего сценарий жертвы можно определить по URL. Например, когда вы просматриваете на сайте **http://www.sitename.ru/** раздел форума, использующего в качестве движка Invision Power Board (мощная и невидимая доска объявлений), то строка адреса содержит следующий код:

http://www.sitename.ru/index.php?showforum=4

Текст `index.php?showforum=` будет встречаться на любом сайте, использующем для форума Invision Power Board. Чтобы найти сайты, содержащие в URL данный текст, нужно выполнить в поисковой системе Google следующий запрос:

```
inurl:index.php?showforum
```

Могут быть и другие движки, которые используют этот текст. Чтобы отбросить их, нужно еще добавить поиск какого-нибудь фрагмента из страниц. Например, по умолчанию внизу каждой страницы форума есть подпись "Powered by Invision Power Board(U)". Конечно же, администратор волен изменить надпись, но в большинстве случаев ее не трогают. Именно такой текст можно добавить в строку поиска, и тогда результатом будут только страницы нужного нам форума. Попробуйте выполнить следующий запрос:

```
Powered by Invision Power Board(U) inurl:index.php?showforum
```

Вы увидите около 300 тысяч сайтов, реализованных на этом движке. Теперь, если появится уязвимость в Invision Power Board, то вы легко найдете жертву для испытания уязвимости. Далеко не все администраторы успеют ликвидировать ошибки, а некоторые вообще не будут их исправлять.

Попробуйте запустить поиск "inurl:admin/index.php", и вы найдете столько интересного, что аж дух захватывает. Такие ссылки очень часто используются для управления чем-либо на сайте. Опытные администраторы защищают их паролями, и, конечно, большинство из этих ссылок будут недоступны, но открытые могут позволить уничтожить сайт полностью.

5.8.3. Серп и молот

Там, где не удалось взломать сервер с помощью умения и знаний, всегда можно воспользоваться чисто русским методом "Серпа и молота". Это не значит, что серп нужно приставлять к горлу администратора, а молотком стучать по голове. Просто всегда остается в запасе тупой подбор паролей. Если уж перебор паролей не помог, то всегда остается метод горячего утюга на пузе администратора.

Давайте снова обратимся к статистике. Все исследовательские конторы пришли к одному и тому же выводу, что большинство начинающих выбирает в качестве па-

роля имена своих любимых собачек, кошечек, даты рождения или номера телефонов. Хорошо подобранный словарь может сломать практически любую систему, т. к. всегда найдутся неопытные пользователи с такими паролями. Самое страшное, если у этих "чайников" будут достаточно большие права. Именно поэтому я рекомендовал вам выбирать сложные пароли *(см. разд. 4.7.3)*.

Я сам страдаю подобной болезнью и очень часто в качестве пароля выбираю легкие слова. Например, для доступа к сайту **http://www.vr-online.ru/** долгое время использовалось название моей любимой футбольной команды. Если учесть, что в премьер-лиге таких команд всего 16, то, зная эту информацию, перебор даже вручную завершится за пять минут.

Сейчас я изменил пароль на название моей любимой компьютерной игры. Игр уже намного больше, поэтому даже эта информация не поможет вам быстро найти пароль к сайту, а значит, и к его админке.

Простые пароли я использую только там, где данные не связаны с критической для меня информацией или финансами. Доступ к банковским данным я защищаю сгенерированными паролями длиной не менее 12 символов, поэтому, тут можно даже не пытаться что-то подбирать.

Вы до сих пор еще не верите мне? Давайте вспомним знаменитейшего "червя Морриса", который пару десятков лет назад проникал в систему, взламывая ее по словарю. Собственный лексикон червя был достаточно маленьким и состоял менее чем из ста слов. Помимо этого, при переборе использовались термины из словаря, установленного в системе. Там их было тоже не так уж много. Но благодаря такому примитивному алгоритму червь смог поразить громаднейшее число компьютеров и серверов. Это был один из самых массовых взломов!!!

Да, случай давний, но средний профессионализм пользователей не растет, т. к. среди них много опытных, но достаточно и начинающих. А домохозяйки всегда будут использовать простые пароли, потому что им генерировать и запоминать что-то сложное не имеет никакого смысла.

Такой метод перебора очень часто используется для взлома почтовых ящиков, паролей FTP и др. Это достаточно долгий процесс, но если выбран действительно длинный и сложный пароль, то даже лучший словарь хакера не выручит.

Все мы слышали, что хакеры умеют воровать номера ICQ, перехватывая их на себя. В основном такое воровство происходит именно благодаря подбору. Программой ICQ пользуются люди разного образования и с разными навыками и далеко не все выбирают сложные пароли. Хакеры набирают в базу несколько номеров, и программа перебирает их по словарю. Какой-нибудь из номеров может сдаться и достаточно быстро.

Но даже если хакеру не удалось быстро найти ваш пароль в словаре, расслабляться не стоит. Он может воспользоваться полным подбором по всем символам. Это отнимет в несколько раз больше времени, но, в конце концов, принесет положительный результат, если пароль короткий. Чтобы этого не произошло, нужно установить какую-нибудь систему обнаружения атак. Хороший сетевой экран без проблем

выявляет попытки подбора и сигнализирует об этом. Убедитесь, что ваш сетевой экран содержит подобную функцию.

Но прежде чем приступать к подбору пароля, нужно хорошо отредактировать словари имен и паролей. Очень важно знать, какую систему вы взламываете. Именно для этого мы определяли версию ОС. Например, если это серверный вариант Windows, то желательно, чтобы среди логинов был "Администратор". Ну а если это UNIX-подобная система, то обязательно должен присутствовать "root", а все имена типа "Администратор" нужно убрать, потому что в UNIX-системе таких логинов не создают, особенно на русском языке.

Если перед нами ОС Windows, то желательно знать и локализацию. В русской версии "Администратор" пишется по-русски, а в английской это "Administrator".

Именно так чаще всего поступают хакеры. Наличие заведомо известного имени упрощает подбор, т. к. остается только найти пароль. Чтобы усложнить злоумышленнику задачу, необходимо изменить имена учетных записей. Если вы используете сложный и очень длинный пароль, то логин можно сделать попроще, потому что его лучше всего держать в голове, но переименовать в администраторскую учетную запись в любом случае не помешает.

Неплохо было бы включить в словарь любые имена и пароли, используемые по умолчанию для разных служб. Очень часто администраторы забывают или просто ленятся поменять пароли на сервисы, которые запущены, но не используются. Особенно этим грешат администраторы Windows, что связано с низким уровнем знаний специалистов, работающих с этой ОС. Нередко бензина в огонь подливают сами серверные программы, которые во время установки не требуют изменения пароля по умолчанию. В последнее время эта тенденция изменяется, и слава богу.

Например, я сталкивался с MS SQL Server 7.0, в котором включена встроенная учетная запись "sa", и при этом абсолютно без пароля. Наверное, поэтому Microsoft собирается убрать это имя своего сервера баз данных, а в SQL Server 2000 на каждом шагу предупреждает, что нужно указывать пароль. Если администратор не увидит таких откровенных предупреждений, то я бы его уволил первым паровозом.

Иногда сложные пароли могут сыграть злую шутку. Если случайно забыть или потерять листик с паролем, то в систему нельзя будет войти и самому. В этом случае приходится собственноручно взламывать систему перебором. Благо, что вы хоть приблизительно знаете свой пароль, и можно упросить задачу, сузив количество вариантов.

Для подбора пароля я опять могу посоветовать Shadow Scan или CyD NET Utils, в которую включен очень хороший генератор словарей и реализованы подборщики по всем основным протоколам для соответствующих сервисов.

5.8.4. Локальная сеть

Взлом в локальной сети может быть проще по многим причинам:

- компьютеры подключены по скоростному соединению от 10 Мбит/с и выше;
- есть возможность прослушивать трафик других компьютеров в сети;

- можно создавать подставные серверы;
- очень редко используются профессиональные сетевые экраны, потому что их ставят в основном перед выходом в Интернет, а персональные экраны далеки от идеала.

Рассмотрим различные варианты взломов, которые получили наибольшее распространение.

Прослушивание трафика

В локальной сети есть свои особенности. Соединения могут осуществляться различными способами. От выбранного типа топологии сети зависят используемый вид кабеля, разъем и используемое оборудование. При подключении по коаксиальному кабелю могут применяться две схемы: все компьютеры объединяются напрямую в одну общую шину (рис. 5.15) или кольцо. Во втором случае крайние компьютеры тоже соединены между собой (на рисунке показано пунктирной линией), и когда они обмениваются данными, все пакеты проходят через сетевую карту соседнего компьютера.

Рис. 5.15. Соединение по общей шине

Если используется такая топология, то весь трафик обязательно проходит через все компьютеры сети. Почему же вы его не видите? Просто ОС и сетевой адаптер сговорились и не показывают чужой трафик. Но если очень сильно захотеть, то, воспользовавшись программой-снифером, можно и просмотреть все данные, проходящие мимо сетевой карточки, даже если они предназначены не вам.

При подключении к Интернету с помощью снифера можно увидеть только свой трафик. Чтобы позаимствовать чужую информацию, нужно сначала взломать сервер провайдера, а туда уже поставить снифер и смотреть трафик всех клиентов. Это слишком сложно, поэтому способ через сниферы используют чаще всего в локальных сетях.

Соединение по коаксиальному кабелю встречается все реже, потому что оно ненадежно, позволяет передавать данные максимум на скорости 10 Мбит/с, сильно ограничено в длине и кабель неудобен в прокладке.

При объединении компьютеров через хаб (hub) или коммутатор (switch) используется топология "звезда" (рис. 5.16). В этом случае компьютеры с помощью витой пары получают в одну общую точку.

Но если в центре стоит устройство типа "хаб", то все пакеты, пришедшие с одного компьютера, копируются на все узлы, подключенные к этому хабу. В случае с ком-

мутатором пакеты будет видеть только получатель, потому что коммутатор имеет встроенные возможности маршрутизации, которые реализуются в основном на уровне MAC-адреса. В локальной сети, даже если вы отправляете данные на IP-адрес, используется физический адрес компьютера. При работе через Интернет всегда используется IP-адресация, и на этом уровне работают далеко не все коммутаторы. Для того чтобы пакеты проходили по правильному пути, нужны уже более интеллектуальные устройства — маршрутизаторы. Они также передают набор данных только на определенную машину или другому маршрутизатору, который знает, где находится компьютер получателя. Маршрутизаторы оперируют IP-адресами.

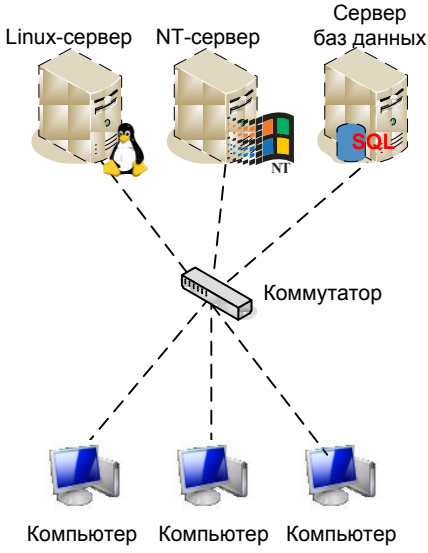


Рис. 5.16. Соединение через хаб или коммутатор

Таким образом, при использовании коммутаторов в локальной сети и из-за маршрутизации в Интернете прослушивание становится более сложным, и для выполнения этой задачи снифер должен находиться на самом коммутаторе или маршрутизаторе.

Работать с пакетами достаточно сложно, потому что в них содержится трудная для восприятия информация. Большой кусок данных разбивается на несколько пакетов, и вы будете видеть только отдельные ее части.

Сейчас в сети можно скачать громадное количество сниферов и дополнений к ним. Всевозможные версии "заточены" под разные нужды, и тут необходимо выбирать, исходя именно из этих соображений. Если вы ищете непосредственно пароли, то вам требуется снифер, который умеет выделять данные о регистрации из общего трафика сети. В принципе, это не так сложно, если учесть, что все пароли и любая информация пересылается в Интернет в открытом виде как текст, если не используется протокол SSL. Так уж получилось, что большинство интернет-протоколов текстовые и передают все данные в открытом виде.

Преимущество от использования сниферов при взломе в том, что они никак не влияют на атакуемую машину, и, значит, вычислить его очень сложно. В большинстве случаев даже невозможно узнать, что ваш трафик кем-то прослушивается в поисках паролей.

Однажды мне заказали определить протокол общения программы с устройством. Фирма заплатила большие деньги за аппаратуру, которая должна была снимать показания с выпускаемой продукции и передавать информацию в компьютер. Но поставлявшаяся в комплекте программа не подходила для нужд компании. Для написания собственных модулей требовались библиотеки, которые были доступны на сервере производителя, но не имели исходных кодов. Поэтому на их основе реализовать подходящую утилиту было невозможно. Для определения протокола мне требовалось решить именно эту задачу.

Связь обеспечивалась через простой сетевой интерфейс и протокол TCP/IP. Я подключил снифер и прослушал все пакеты, которыми обменивалось устройство со стандартной программой. Потом написал собственный простой пример, чтобы убедиться в работоспособности определенного мной протокола, и передал полученную информацию представителю фирмы. Компании это стоило лишних денег, а ведь не так уж и сложно было самостоятельно прослушать трафик.

Жаль, что сниферы не позволяют изменять пакеты. Мы можем только увидеть передаваемые другими компьютерами данные.

Подставной адрес

Мы уже говорили о том, что сетевые экраны разрешают или запрещают доступ пользователей на основе правил. Но блокировать абсолютно все обращения к любым портам не всегда удобно. Например, доступ к управляющим программам можно сохранить для определенного IP-адреса, с которого работает администратор. Любой, кто попытается с другого адреса войти в запрещенную область, будет остановлен сетевым экраном.

На первый взгляд, защита безупречна. Но существует такой метод атаки, как спуфинг, который подразумевает подделку IP-адреса авторизованного пользователя и вход в штурмуемый сервер. Старые сетевые экраны (да и дешевые современные) не могут определить фальшивый адрес в пакетах.

Фиктивный сервер

В локальной сети намного проще производить атаку через подставные серверы или сервисы. Например, одна из знаменитых атак через некорректные ARP-записи может быть воспроизведена именно в локальной сети.

Как мы уже знаем, когда вы обращаетесь к какому-либо компьютеру по IP-адресу, сначала определяется его MAC-адрес, а потом уже на него отсылается сообщение. Как определить MAC-адрес, когда нам неизвестно, какой сетевой интерфейс установлен, а мы знаем только IP? Для этого используется протокол ARP (Address Resolution Protocol, протокол разрешения адресов), который рассылает широкове-

щательный запрос всем компьютерам сети и выясняет, где находится экземпляр с указанным IP-адресом. В этом пакете заполнен только IP-адрес, а вместо искомого MAC-адреса указано значение FFFFFFFFFFFFh. Если в сети есть компьютер с запрошенным IP, то в ответном пакете будет указан MAC-адрес. В противном случае ответ может прислать маршрутизатор, который сообщит свой MAC-адрес. Тогда компьютер будет обмениваться данными с ним, а тот уже в свою очередь будет пересылать пакеты дальше в сеть или другому маршрутизатору, пока они не достигнут получателя. Работа ARP-протокола происходит незаметно для пользователя.

А что если ответит не тот компьютер, а другой, с иным IP-адресом? Ведь в локальной сети передача осуществляется по MAC-адресу, поэтому пакет получит тот компьютер, который откликнется, вне зависимости от его IP. Получается, что задача хакера — вычислить ARP-запрос и ответить на него вместо реального адресата. Таким образом можно перехватить чужое соединение.

Допустим, что компьютер запросил соединение с сервером. Если мы ответим на него и сэмулируем запрос на ввод параметров для входа в сервер, то пароль будет перехвачен. Сложность такого метода в том, что вручную его реализовать практически невозможно. Для этого нужно писать соответствующую программу, а тут без знания программирования и сетевых протоколов не обойтись.

Есть еще один нюанс, о котором стоит упомянуть. После того как компьютер определил какой-либо физический адрес, то соответствие MAC и IP сохраняется в локальном кэше. У вас есть возможность управлять этим кэшем с помощью утилиты arp, встроенной в ОС. Она запускается из командной строки и не совсем удобна. Более подходящей я считаю уже не раз описанную мною CyD NET Utils. Запустите эту программу и выберите меню **Manage | IP ARP**. Перед вами появится окно, в котором можно просматривать текущее содержимое таблицы ARP-записей, добавлять и удалять их.

Когда вы вручную добавляете запись ARP, то она становится статической и может быть удалена из системы только вручную. Если запись была создана автоматически, то она считается динамической и через определенное время удаляется системой.

С таким же успехом можно подменять DNS-запросы. Если ARP-протокол предназначен для преобразования IP-адреса в MAC, то DNS сопоставляет символьные имена и IP-адреса. Задача та же самая — использовать параметры компьютера, который будет перехватывать DNS-запросы, и подделывать ответ. Таким способом было проведено уже несколько широкомасштабных и знаменитых атак в Интернете.

Основная цель, которую может преследовать хакер — перенаправление трафика на себя для выявления пароля или переадресации пакетов на другой сервер. Если переправить весь трафик какого-либо DNS-сервера, например, на **http://www.yahoo.com/**, то даже мощный веб-сервер Yahoo не выдержит такого количества запросов и может зависнуть или просто перестать откликаться. Но это уже из серии атак DoS, о которых мы поговорим позже *(см. разд. 5.8.6)*.

5.8.5. Троян

Использование троянских программ — самый глупый и ненадежный в отношении администраторов сетей способ, но для простых пользователей подойдет, потому что им проще подбросить серверную часть программы. Хотя среди администраторов встречаются непрофессионалы, но на такие шутки уже мало кто попадается. Но кто сказал, что в сети существуют только они? Есть еще куча простых пользователей с большими привилегиями и доверчивой душой. Вот именно их и надо троянить.

Троянская программа состоит из двух частей — клиента и сервера. Сервер нужно подбросить на компьютер жертвы и заставить жертву запустить файл. Чаще всего троянская программа после первого запуска прописывается в автозагрузку и стартует вместе с ОС, и при этом незаметна в системе. После этого вы подключаетесь к серверной части с помощью клиента и выполняете заложенные в программу действия, например, перезагрузка компьютера, воровство паролей и т. д.

Как забрасывать троянскую программу? Самый распространенный способ — почтовый ящик. Просто даете исполняемому файлу серверной части какое-нибудь привлекательное имя и отправляете сообщение жертве. В тексте письма должны быть мягкие, но заманчивые призывы запустить прикрепленный файл. Это то же самое, что и распространение вирусов, письма с которыми мы видим каждый день в своих ящиках *(см. разд. 4.7.1)*. Если пользователь запустит серверную часть, то считайте, что вы стали царем на его компьютере. Теперь вам будет доступно все, что может для вас сделать боевой конь.

Какое дать имя, чтобы заинтересовать пользователя? Очень просто, и мы об этом говорили при рассмотрении безопасности системы *(см. разд. 4.1.2)*. Windows очень часто не показывает расширения всех зарегистрированных в системе файлов. Если вы назовете файл Anna_Kurnikova.jpg.exe, то ОС спрячет последнее расширение (exe), и любой пользователь подумает, что видит картинку. Для большей надежности лучше присвоить такое имя: Anna_Kurnikova.jpg .exe, где я для наглядности обозначил знаком " " пробел. В этом случае, даже если расширение не прячется по умолчанию, его все равно видно не будет, особенно если вы не поскупитесь на пробелы.

Мне дважды приходилось забрасывать друзьям трояна через почтовый ящик, и оба раза процесс прошел удачно. Первый раз это произошло на спор, когда мой друг сказал, что я не смогу заразить его компьютер таким способом. Второй раз я создал троянскую программу, с помощью которой собирался подшутить над моим знакомым. Для этого я использовал очень интересный и эффективный метод. Мы уже говорили о том, что нельзя открывать никакие файлы, прикрепленные к письму (особенно от незнакомых людей). Большинство опытных пользователей уже давно следуют этому правилу.

Итак, чтобы пользователь запустил нужную программу, следует заставить его самого скачать и запустить необходимый исполняемый файл. Я отправил письмо, в котором прорекламировал бесплатную программу, которую можно скачать с за-

ранее созданного мною сайта. Главное — выбрать ее имя, чтобы оно заинтересовало пользователя. Например, если жертва любит рисовать на компьютере, то можно предложить скачать новый графический эффект.

Письмо должно выглядеть, как спам. Сколько бы не говорили, но все мы читаем или хотя бы заглядываем в такие сообщения. Если сразу заинтересовать жертву, то она обязательно выполнит вашу просьбу. Возможно, первое письмо попадет в Корзину, но хотя бы в третий раз оно будет прочитано, и вы добьетесь нужного результата. Более трех попыток можно не делать, потому что или у жертвы стоит почтовый фильтр, или вы его не заинтересовали. Нужно придумывать новую программу и сочинять другое письмо.

Чтобы жертва ничего не заподозрила, сайт должен выглядеть как можно профессиональнее, содержать описание возможностей скачиваемой программы и снимки экранов. Вся эта информация берется с реального сайта какой-нибудь не очень знаменитой фирмы или программиста-одиночки.

Оба моих товарища попались на эту удочку, и при этом они очень хорошо знакомы со всеми методами проникновения вирусов в систему. Конечно же, при отправке серверной части я использовал анонимное письмо, чтобы меня не вычислили. Таким образом, я позаботился, чтобы файл запустили, и скрыл источник происхождения троянской программы.

Данный метод очень скучен, т. к. требует много времени и сил на подготовку, создание сайта, размещение на нем серверной части трояна.

Если троянская программа направлена на воровство паролей, то после заражения она может незаметно для пользователя выслать письмо с файлом паролей на определенный электронный адрес. Профессионалы легко находят такие адреса (с помощью отладки приложения), но на этом все останавливается. Профессиональные хакеры не глупы и для троянских программ регистрируют почтовые адреса на бесплатных сервисах, при этом указывается ложная информация о владельце. Злоумышленник заводит почтовый ящик или проверяет его на предмет писем с паролями только через анонимный прокси-сервер, и узнать реальный IP-адрес человека становится очень сложно.

Трояны получили большое распространение из-за того, что вычислить автора при соблюдении простых правил анонимности непросто. При этом использование самих программ стало примитивным занятием. Сейчас даже не надо быть программистом, чтобы создать собственную программу, достаточно воспользоваться любым конструктором, которых в Интернете предостаточно. Самым знаменитым стал Back Orifice, благодаря которому было произведено очень большое количество взломов.

Серверная часть трояна Back Orifice устанавливается на компьютер жертвы и позволяет хакеру выполнять следующие действия:

- осуществлять доступ к жесткому диску удаленного компьютера;
- редактировать реестр;
- запускать программы на чужом компьютере;

- ❒ отслеживать введенные пароли;
- ❒ копировать содержимое экрана;
- ❒ управлять процессами, в том числе и перезагрузкой.

Но самое страшное в этой программе — возможность перед сборкой исполняемого файла добавлять расширения (Plug-in), которых в Интернете предостаточно.

Опасность, которую таят в себе троянские программы, подтверждается и тем, что большинство антивирусных программ стало сканировать не только на наличие вирусов, но и троянов. Например, антивирусные программы идентифицируют Back Orifice, как вирус Win32.BO.

5.8.6. Denial of Service

Самая глупая атака, которую могли придумать хакеры — это отказ от обслуживания (DoS, Denial of Service). Заключается она в том, чтобы заставить сервер не отвечать на запросы. Как это можно сделать? Очень часто такого результата добиваются с помощью зацикливания работы. Например, если сервер не проверяет корректность входящих пакетов, то хакер может сделать такой запрос, который будет обрабатываться вечно, а на работу с остальными соединениями не хватит процессорного времени, тогда клиенты получат отказ от обслуживания.

Атака DoS может производиться двумя способами: через ошибку в программе или перегрузку канала или вычислительной мощности атакуемой машины.

Первый способ требует знания об уязвимости на сервере и, конечно же, наличия этих уязвимостей. Рассмотрим, как происходит отказ от обслуживания через переполнение буфера (это чаще всего используемая ошибка). Допустим, что вы должны передать на сервер строку "HELLO". Для этого в серверной части выделяется память для хранения 5 символов. Структура программы может выглядеть примерно следующим образом:

```
Код программы
Буфер для хранения 5 символов
Код программы
```

Предположим, пользователь отправит не пять, а сто символов. Если при приеме информации программа не проверит размер блока, то при записи данных в буфер они выйдут за его пределы и запишутся поверх кода. Это значит, что программа будет запорчена и не сможет выполнять каких-либо действий, и, скорее всего, произойдет зависание или даже синий экран. В результате сервер не будет отвечать на запросы клиента, т. е. совершится классическая атака Denial of Service через переполнение буфера.

Таким образом, компьютер не взломали, и информация осталась нетронутой, но сервер перестал быть доступным по сети. В локальной сети такую атаку вообще несложно произвести. Для этого достаточно свой IP-адрес поменять на адрес атакуемой машины, и произойдет конфликт. В лучшем случае недоступной станет только штурмуемая машина, а в худшем — обе машины не смогут работать.

Для перегрузки ресурсов атакуемой машины вообще не надо ничего знать, потому что это война, в которой побеждает тот, кто сильнее. Ресурсы любого компьютера ограничены. Например, веб-сервер для связи с клиентами может организовывать только определенное количество виртуальных каналов. Если их создать больше, то сервер становится недоступным. Для совершения такой акции достаточно написать программу на любом языке программирования, бесконечно открывающую соединения. Рано или поздно предел будет превышен, и сервер не сможет работать с клиентами.

Если нет программных ограничений на ресурсы, то сервер будет обрабатывать столько подключений, сколько сможет. В таком случае атака может производиться на канал связи или на сервер. Выбор цели зависит от того, что слабее. Например, если на канале в 100 Мбит стоит компьютер с процессором Pentium 100 МГц, то намного проще убить машину, чем перегрузить данными канал связи. Ну а если это достаточно мощный сервер, который может выполнять миллионы запросов в секунду, но находится на канале в 64 Кбит, то легче загрузить канал бессмысленными запросами.

Как происходит загрузка канала? Допустим, что вы находитесь в чате, и кто-то вам нагрубил. Вы узнаете его IP-адрес и выясняется, что обидчик работает на простом dial-up-соединении через модем в 56 Кбит/с. Даже если у вас такое же соединение, можно без проблем перегрузить канал обидчику. Для этого направляем на его IP-адрес бесконечное количество ping-запросов с большим размером пакета. Компьютер жертвы должен будет отвечать на них. Если пакетов много, то мощности канала хватит только на то, чтобы принимать и отвечать на эхо-запросы, и обидчик уже не сможет нормально работать в сети. Если у вас канал такой же, то и ваше соединение будет занято исключительно приемом-отсылкой больших пакетов. Это того стоит? Если да, то можете приступать.

Для реализации атаки DoS с помощью ping-запросов воспользуемся утилитой CyD NET Utils. Запустите программу и выберите меню **Utils | Ping server**. В появившемся окне перейдите на вкладку **Options** (рис. 5.17). В поле **Number of packets** (Количество пакетов) введите очень большое значение (несколько тысяч). Установите 1 в поле **Time Out** (Время ожидания ответа). В этом случае программа не станет дожидаться ответа, а каждую секунду будет направлять ping-пакет. В поле **Size of packets** (Размер пакета) также установите большое значение, например 10 000, чтобы одним пакетом отправлялось много данных. Теперь можно запускать операцию ping на нужный IP-адрес.

Таким образом, мы можем загрузить канал жертвы, но при условии, что наш канал равен или больше, чем у атакуемого компьютера. Если у вас скорость соединения медленнее, то удастся загрузить только часть канала, равную пропускной способности вашего соединения. Остальная часть останется свободной, и жертва сможет использовать ее. С другой стороны, связь будет заниженной, и хотя бы чего-то мы добьемся.

В случае атаки на сервер и его процессор наш канал может быть намного слабее, главное — правильно определить слабое звено. Допустим, что сервер предоставляет услугу скачивания и хранения файлов. Чтобы перегрузить канал такого сервера,

нужно запросить одновременное скачивание нескольких очень больших файлов. Скорость связи резко упадет, и сервер может даже перестать отвечать на запросы остальных клиентов, при этом загрузка процессора сервера может быть далека от максимальной.

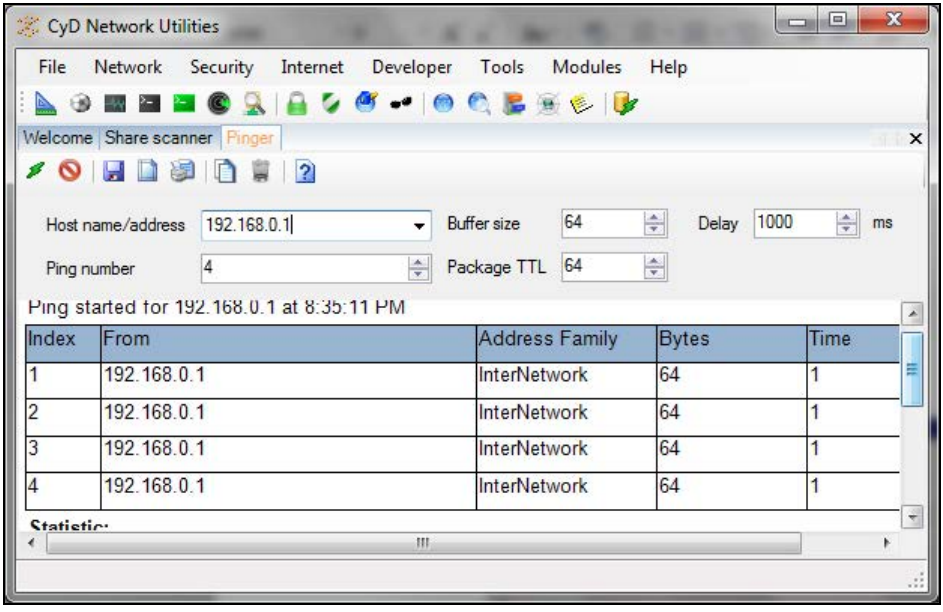


Рис. 5.17. Настройка отправки ping-пакетов

Для загрузки процессора тоже не требуется слишком большой канал. Нужно только подобрать запрос, который будет выполняться очень долго. Допустим, что вы решили произвести атаку на сервер, позволяющий переводить на другой язык указанные страницы любого сайта. Находим веб-страницу с большим количеством текста (например, книгу или документацию RFC — Request for Comments — рабочее предложение) и посылаем множество запросов на ее перевод. Мало того, что объем большой и для скачивания серверу нужно использовать свой канал, так еще и перевод — достаточно трудоемкий процесс. Достаточно в течение одной секунды отправить 100 запросов на перевод громадной книги, чтобы сервер перегрузился. А если сервер написан "с умом" и на нем используется блокировка многократного перевода одного и того же текста, то нужно подыскать несколько больших книг. Однако такой трюк пройдет, только если сервер не имеет ограничение на размер переводимого документа.

Атака отказа от обслуживания отражается достаточно просто. Серверное программное обеспечение должно контролировать и ограничивать количество запросов с одного IP-адреса. Но это все теоретически, и такие проверки оградят только от начинающих хакеров. Опытному взломщику не составит труда подделать IP-адрес и засыпать сервер пакетами, в которых в качестве отправителя указан поддельный адрес.

Для сервера еще хуже, если взлом идет по TCP/IP, потому что этот протокол требует установки соединения. Если хакер пошлет очень большое количество запросов на открытие соединения с разными IP-адресами, то сервер разошлет на эти адреса подтверждения и будет дожидаться дальнейших действий. Но т. к. реально с этих адресов не было запроса, то и остановка будет бессмысленной. Таким образом, заполнив буфер очереди на входящие соединения, сервер становится недоступным до подключения несуществующих компьютеров (тайм-аут, т. е. время, которое сервер ожидает ответа до того, как "решит", что больше можно не ждать, для этой операции может составлять до 5 секунд). За это время хакер может забросать буфер новыми запросами и продлить бессмысленное ожидание сервера.

Distributed Denial Of Service

С помощью DoS достаточно сложно вывести из обслуживания такие домены, как **http://www.microsoft.com/** или **http://www.yahoo.com/**, потому что их обслуживают достаточно широкие каналы и сверхмощные серверы. Захватить же такие ресурсы в одиночку просто невозможно. Но как показывает практика, хакеры находят выходы из любых ситуаций. Для получения такой мощности используются распределенные атаки DoS (Distributed Denial of Service).

Мало кто из пользователей добровольно отдаст мощность своего компьютера для проведения распределенной атаки на крупные серверы. Чтобы решить эту проблему, хакеры пишут вирусы или трояны, которые без разрешения ничего не подозревающих пользователей занимаются захватом и зомбируют их компьютеры. Так, вирус Mydoom C искал в сети компьютеры, зараженные вирусами Mydoom версий A и B, и использовал их для атаки на серверы корпорации Microsoft. Благо этот вирус не смог захватить достаточного количества машин, и мощности не хватило для проведения полноценного налета. Администрация Microsoft утверждала, что серверы работали в штатном режиме, но некоторые все же смогли заметить замедление в работе и задержки в получении ответов на запросы.

От распределенной атаки защититься очень сложно, потому что множество реально работающих компьютеров шлют свои запросы на один сервер. В этом случае трудно определить, что это идут ложные запросы с целью вывести систему из рабочего состояния.

5.8.7. Взлом паролей

Когда взломщик пытается проникнуть в систему, то он чаще всего использует один из следующих способов:

- если на атакуемом сервере уже есть аккаунт (путь и гостевой), попытаться поднять его права;
- получить учетную запись конкретного пользователя;
- добыть файл паролей и воспользоваться чужими учетными записями.

Даже если взломщик повышает свои права в системе, он все равно стремится обрести доступ к файлу с паролями, потому что это позволит добраться до учетной

записи root (для UNIX-систем) и получить полные права на систему. Но пароли зашифрованы, и в лучшем случае можно будет увидеть хэш-суммы, которые являются результатом необратимого шифрования пароля.

Когда администратор заводит нового пользователя в системе, то его пароль чаще всего шифруется с помощью алгоритма MD5, т. е. не подлежит дешифровке. В результате получается хэш-сумма, которая и сохраняется в файле паролей. Когда пользователь вводит пароль, то он также шифруется, и результат сравнивается с хэш-суммой, хранящейся в файле. Если значения совпали, то пароль введен верно.

Так как обратное преобразование невозможно, то, вроде бы, и подобрать пароль для хэш-суммы нельзя. Но это только на первый взгляд. Для подбора существует много программ, например, John the Ripper (**http://www.openwall.com/john/**) или PasswordsPro (**http://www.insidepro.com/**).

В NT-системах пароли также шифруются необратимым образом, но хранятся в базе данных SAM, и для их взлома нужна уже другая утилита — SAMInside (**http://www.insidepro.com/**). Главное окно программы можно увидеть на рис. 5.18.

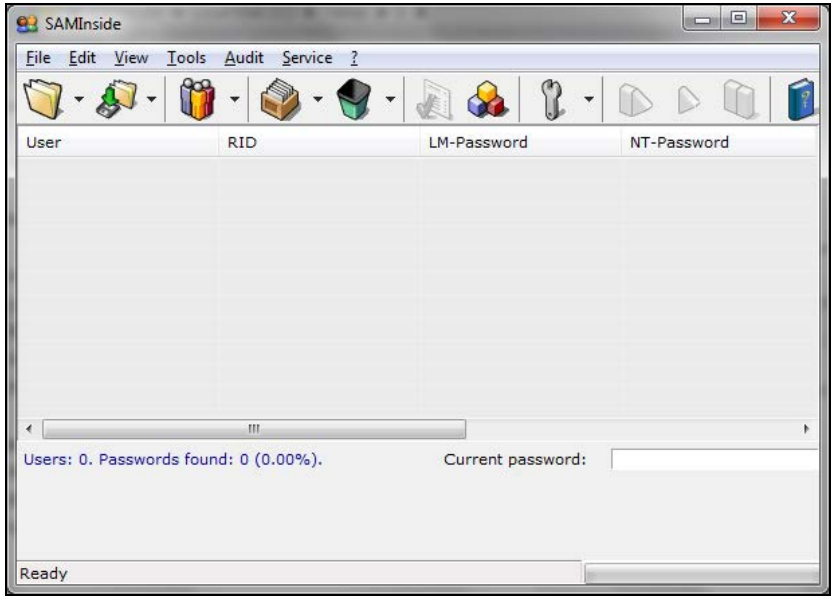


Рис. 5.18. Программа SAMInside взламывает пароли NT-систем

Почему эти утилиты так свободно лежат в Интернете, когда они позволяют злоумышленнику воровать пароли? Любая программа может иметь как положительные, так и отрицательные стороны. Что делать, если вы забыли пароль администратора или администратор уволился и не сказал вам его? Переустанавливать систему? Это долго и может грозить потерей данных. Намного проще снять жесткий диск и подключить к другому компьютеру (или просто загрузиться с дискеты, умеющей читать вашу файловую систему), потом взять файл паролей и восстановить утерянную информацию.

Конкретный пользователь

Для получения прав определенного пользователя взломщики чаще всего используют:

- методы социальной инженерии — тривиальный и не требующий много времени, но при этом ненадежный способ;
- троянские программы — просты в использовании, но применение может не принести результата, если не удастся заразить компьютер жертвы;
- подбор пароля — сложнее всех в реализации и может занять у взломщика годы, и в этом случае тоже не даст результата.

При использовании методов социальной инженерии нужно знать контактную информацию лица, учетную запись которого нужно получить. Если это e-mail, то на него отправляется сообщение, в котором каким-либо ненавязчивым способом предлагается показать свой пароль. Это может быть письмо от администрации сервера с просьбой сообщить свои данные для проверки, ссылка на подставной сайт, где нужно ввести личную информацию и т. д.

Для троянской программы тоже нужен почтовый адрес, на который высылается письмо с серверной частью трояна или ссылка с призывом скачать исполняемый файл самостоятельно. Вероятность проникновения зависит от профессионализма жертвы (умение распознавать письма со зловредным кодом) и ваших способностей заинтересовать жертву в запуске нужного файла.

Подбор пароля будет самым быстрым, если он простой и легко находится по словарю. А может оказаться самым долгим, если использованы все рекомендации по формированию пароля. Это только в кино хакеры за пять минут взламывают пароли Пентагона, а в жизни весь процесс отнимает, как минимум, часы, а то и дни, или даже месяцы терпеливого и кропотливого труда.

Когда хакер пытается проникнуть в систему, то он может использовать все доступные методы одновременно. Какой-нибудь даст результат быстрее других.

И все же, есть еще один вариант, который мы не рассматривали, хотя косвенно затрагивали эту тему. Каждый сервис имеет права определенной учетной записи, и если выполнять команды от его имени, то и привилегии будут теми же, что у аккаунта, под которым он работает.

Большинство администраторов устанавливает всем сервисам максимальные права, чтобы не разбираться в тонкостях настройки. Если разрешить работу службы при входе в систему, например, под гостевой учетной записью, то сервис может перестать функционировать. Некоторым серверным программам нужен доступ к реестру или системным каталогам, и если это запретить, то сервис просто не запустится, а найти причину бывает сложно, если нет подробной документации по политике безопасности программы. С другой стороны, большинству сервисов просто не нужны большие полномочия.

Когда хакер стремится получить прерогативу администратора, то он может задаться целью найти уязвимость сервиса, который обладает нужными правами. А затем с его помощью попытаться пробиться дальше на сервер.

Чтобы не давать хакеру лишних лазеек, ограничьте права сервисов. В этом случае, даже если злоумышленник нашел какую-либо уязвимость, проникнуть в систему будет сложно.

Например, для FTP-сервера можно создать учетную запись, у которой будет доступ только к определенным папкам, которые и так открыты по сети для клиентов этого сервиса. Но системный каталог для FTP-сервера чаще всего не требуется. Если же ваш сервер использует реестр и что-то пишет в систему, откажитесь от его использования, потому что его безопасность далека от идеала. Доступ к системным каталогам абсолютно не нужен большинству сервисов или, по крайней мере, должен быть не нужен, но программисты лезут в него.

Если вы программист и разрабатываете свои серверные продукты, то не трогайте системные области без особой надобности. Работайте только в одной папке, где пользователь установит программу. Если избегать обращения к опасным ресурсам, то можно минимизировать возможность через ваш сервер попасть в систему. А это уже означает, что ваша программа будет реже появляться в списках дырявых сервисов, что улучшит ваше положение на рынке.

Конечно же, для программистов можно дать очень много рекомендаций, но мы рассматриваем компьютер с точки зрения пользователя, поэтому не будем уходить в сторону.

5.8.8. Взлом не зависит от ОС

Некоторые спорят, что ломают чаще: Windows или Linux? Вопрос не совсем верный, потому что крушат то, что надо. Если хакеру нужно проникнуть на сервер банка, то он будет ломать его вне зависимости от установленной на нем операционной системы. Будь это UNIX или Windows, ничто не остановит злоумышленника в проведении своих действий, кроме правильной политики безопасности и грамотного администратора.

Результат взлома также не зависит от ОС, потому что проникнуть можно в обе системы примерно с равной вероятностью. Я бы сказал, что результат в большей степени зависит от квалификации обеих сторон — злоумышленника и администратора. Взлом — это война, похожая на троянскую. Хакеры атакуют крепость в виде ОС, ищут недочеты и уязвимости, а администратор старается настроить свою систему, обеспечивая максимальную защиту. Ошибка одного из них принесет победу сопернику.

Безопасность зависит от степени подготовленности администратора. При управлении Windows для выполнения основных задач не требуется высочайшей квалификации, поэтому среди администраторов Windows больше специалистов среднего уровня. В UNIX нужно больше знаний, но и администрировать намного сложнее, поэтому даже квалифицированные специалисты иногда допускают грубые ошибки. Получается, что ОС Windows чаще всего сочетает простоту настройки и неопытность администрирования, а UNIX-система совмещает сложность конфигурирования и высокий профессионализм, который не всегда спасает в тяжелых ситуациях.

Как мы уже знаем, взлом происходит не только самой ОС, но и сервисов, установленных на ней. А тут уже производитель операционной системы может быть ни при чем. Например, для Windows в качестве веб-сервера может использоваться Apache, к разработке которого фирма Microsoft не имела никакого отношения, поэтому нельзя обвинять производителей ОС во всех бедах.

Почему в наше время так много взломов? Просто Интернет разрабатывался как свободная сеть, и в то время о хулиганах даже не думали. В протоколе TCP/IP, который является основным транспортом, отсутствует полноценная защита (аутентификация, проверка пользователя и т. д.). Именно из-за этого происходит большинство взломов.

В новой версии протокола IPv6 уже встроены все необходимые средства для обеспечения конфиденциальности, проверка подлинности, целостности данных и т. д. Протокол разработан уже несколько лет назад, но его внедрение происходит слишком долго, и когда это произойдет, сказать сложно. Но мы надеемся, что к моменту полноценной эксплуатации (коммерческого использования) возможности безопасности, заложенные в протокол, не устареют.

5.8.9. Резюме

Этот обзор хакерских атак не претендует на полноту, но я постарался дать все начальные сведения. В то же время я воздержался от конкретных рецептов, потому что это может быть воспринято, как призыв к действию, а я не ставлю своей целью увеличить количество хакеров. Моя задача — показать, как хакер видит и использует компьютер. Это поможет вам больше узнать о своем противнике и сделать собственную жизнь безопаснее.

В основном мы рассматривали теорию. Для реализации на практике всего вышесказанного нужны специализированные программы, и для определенных задач их придется писать самостоятельно. А это уже из серии программирования глазами хакера.

Почему хакеры очень часто легко добиваются цели? Для этого есть несколько причин:

- открытость сетевого трафика, выражающаяся в том, что по умолчанию пакеты, передаваемые по сети, не шифруются и легко могут быть прочитаны;
- наличие ошибок в ОС и программном обеспечении, используемом на сервере, а главное — несвоевременное их обновление;
- сложность организации защиты между разнородными сетями;
- ошибки конфигурирования ОС, серверных программ и средств защиты;
- экономия на специалистах безопасности и системах обеспечения безопасности. Это самое страшное. Только специалист, имеющий многолетний опыт, может защитить систему от вторжения. Многие доверяются своим знаниям или просто конфигурируют системы с целью обучения. Но приобретать навыки надо на тестовых технических средствах, а рабочие серверы и компьютеры должны поддерживаться только специалистами.

5.9. Как скрываются хакеры

Естественное желание хакера — остаться незамеченным, и в основу любого действия положены принципы анонимности, которые мы рассматривали *(см. разд. 5.4 и 5.5)*. Злоумышленники маскируют свой реальный IP-адрес большими цепочками прокси-серверов, а наиболее опытные — привлекают компьютеры рабов (серверы, взломанные в Интернете с целью дальнейшего использования), устанавливая VPN. Такие взломщики находят компьютер-раб, к которому, как правило, имеют полный доступ, и могут уничтожить на нем всю компрометирующую информацию (журналы безопасности).

Что происходит, когда взломщики проникают в систему? Все зависит от преследуемой цели. Если это разрушение, то сокрытию следов отводится не самая важная роль. Если же цель заключается в незаметном присутствии и использовании чужого мощного сервера — это совсем другое дело.

5.9.1. На долгий срок

Если хакер стремится захватить систему на длительный срок, то он создает потайную дверь, через которую можно будет в любой момент незаметно войти и выполнять необходимые действия. Каждый раз использовать уязвимость слишком накладно и заметно. Лучше иметь что-то более завуалированное.

Проникнув в систему, хакеры чаще всего открывают на каком-нибудь порту Shell (оболочку, которая позволяет выполнять в системе команды) или забрасывают троянскую программу. Администраторы, к сожалению, очень редко проверяют открытые порты в своих системах, особенно с номерами более 10 000, потому что это не очень интересное занятие.

В случае с Windows большинство троянских и backdoor-программ определяются с помощью антивируса. Достаточно просто поставить такой антивирус и уже можно более менее спать спокойно. Для Linux антивирусы, вроде бы, есть (что-то выпускал, кажется, Касперский), но их почему-то не ставят. Я не видел ни одного линуксоида, который поставил бы на свой сервер антивирус.

Оригинальным решением является поднятие прав отдельной учетной записи. Администраторы опять же не следят за уже существующими записями и быстро реагируют только на добавление новых. Например, если гостевой записи разрешить чтение/запись системного каталога, то большинство администраторов заметят такие изменения не сразу, а некоторые вообще никогда не увидят.

Расширение прав для гостевой записи я привел только в качестве примера. Если у вас будет выбор, то отдайте предпочтение чему-нибудь более незаметному (например, аккаунту рядового бухгалтера или экономиста). Гостевая учетная запись редактируется достаточно часто и находится под бóльшим присмотром, чем записи рядовых сотрудников сети.

Чтобы хакер остался незаметным, он может попытстья чистить журналы. Раньше это было серьезной проблемой, и даже появились решения, которые позволяли

дублировать записи журнала на удаленном сервере. Каждая запись сохранялась не только в локальном файле, но и удаленно. Даже если хакер получал доступ к локальному компьютеру и чистил лог-файлы, данные на удаленной машине позволяли восстановить картину взлома.

Чистка журнала — это основа, которая позволяет хакеру остаться незамеченным. Как бы злоумышленник не прятал свой IP-адрес, его смогут найти (или хотя бы будут искать), если станет известно, что в систему кто-то проник. Если администратор не заметит, что его сервер взломали, то никто и не будет заниматься поисками злоумышленника. А если заметит, то начнется розыск, но при очищенном журнале вероятность положительного результата падает до 0, потому что главный источник определения активности хакера уничтожен. Именно поэтому злоумышленники стараются затереть все следы своего присутствия в системе.

Кратковременные вторжения мало кто заметит, поэтому не стоит забивать себе голову лишними проблемами, а лучше позаботиться о скрытии своего IP-адреса. Без этого параметра журнал транзакций не сильно поможет администратору и спецслужбам, а в случае редких и непродолжительных вторжений найти вторгающегося очень сложно.

Чем мне нравится журналирование Windows, так это тем, что здесь после очистки в журнале появляется запись, в которой показано, кто производил очистку. По этой записи можно сразу определить, какую учетную запись захватил хакер. Или с вашим компьютером поиграл шутник-коллега. В любом случае очистка журнала Windows должна настораживать.

5.9.2. Коротко и ясно

Если целью хакера было кратковременное вторжение для выполнения определенных действий (например, удаление или воровство файлов), то, выполнив нужные операции, он по возможности уничтожает все следы своего пребывания (чистит журналы безопасности) и навсегда выходит из системы. Такие хакеры наиболее опасны, потому что если им не удается замести следы, то они могут очистить или отформатировать весь диск. Как говорится, после меня хоть потоп.

На многих серверах стоят системы зеркалирования журналов. Тогда информация об активности сервера и пользователях попадает не только в системный, но и резервный журнал, который может быть хорошо спрятан. В таких случаях хакеры в панике могут испортить весь диск, но это бесполезно. Резервная копия журнала чаще всего защищена, и если не уничтожить ее, то мошенника смогут найти по записям в этом журнале. Первым делом нужно очистить именно резервную копию, а потом уже основной журнал.

Некоторые взломщики, которые преследуют только цель уничтожения, не обращают внимания на системы журналирования, а перед выходом из системы просто уничтожают информацию. Благо, что таких хакеров не много. Большинство понимает, что хороший администратор сделает все необходимое, чтобы найти злоумышленника, и лучше остаться незамеченным, чем проявить себя неосмотрительными действиями.

Чем меньше хакер находится в системе, тем сложнее его потом найти. При длительном пребывании злоумышленник вольно или невольно оставляет много следов, даже если просто просматривает содержимое сервера и ничего не изменяет.

5.9.3. Скрываться бесполезно

Если вы съели в магазине конфетку, то вас, скорее всего, не будут разыскивать. Тратить деньги налогоплательщиков на поиск мелкого жулика — просто сумасшествие. Но если вы украли чертежи секретной военной установки, то, поверьте мне, правительство задействует все возможные ресурсы на то, чтобы найти вас.

Достаточно посмотреть на сайт WikiLeaks, владелец которого вроде бы и не ломал ничего, но выкладывал секретные документы. И тут же против него придумали дело про каких-то шведских девушек и моментально арестовали. В момент написания этих строк владелец проета WikiLeaks вроде бы находится на свободе, но что-то его секретные материалы уже не так шумят или он перестал их выкладывать.

Точно так же и со взломом. Простую замену главной страницы сервера маленькой компании оставят без внимания. Но если это было воровство денег из банка или вторжение в военные/правительственные сети, то вас обязательно будут искать всеми возможными способами и, скорее всего, найдут. До сих пор находили даже очень профессиональных хакеров.

Некоторые хакеры считают, что, зашифровав жесткий диск, они обезопасят себя, и правоохранительные органы не смогут найти доказательств. Это заблуждение. Допустим, что вы закрыли украденные вещи в квартире за семью замками. Можно считать, что вы в безопасности? Конечно же, нет. Получив разрешение на обыск, сотрудники полиции могут потребовать ключи или взломают замки. Любые усилия воспрепятствовать будут расценены, как попытки помешать следствию, и сделают только хуже.

Компьютер тоже может быть подвергнут обыску, и мешать этому бесполезно. Даже если злоумышленник будет утверждать, что ключ к шифру утерян, правительство может задействовать большие ресурсы для подбора пароля. Хакер усугубит свою вину и получит дополнительное наказание, если в компьютере окажутся нужные доказательства. Всем известно, что помощь следствию уменьшает срок, а любые помехи как минимум оставляют его неизменным, а в худшем — увеличивают.

Если вы нарушаете закон, находясь в России, то сталкиваетесь именно с российскими правоохранительными органами. Мне только один раз приходилось общаться с ними в качестве подозреваемого, и все закончилось для меня удачно, ибо не был виновен. Но если посмотреть телевизор и послушать что пишут, то если быть виновным, то наша полиция может выбить любые признания.

Даже если вы нарушаете закон за пределами России и взламываете серверы НАТО, общаться все равно придется со своими родными служителями порядка, потому что Интерпол не имеет никакой силы за пределами своей юрисдикции. Они могут только попросить полицию найти и доказать.

Если вы идете на нарушение закона, то лучше проконсультироваться у профессионального юриста, а я всего лишь программист, который совсем немного знаком с законом.

5.10. Произошло вторжение

Самое страшное для любого администратора или пользователя компьютера — увидеть, что в систему проник злоумышленник. Что делать в этом случае?

Руководители крупных компаний, проинформированные техническими специалистами о вторжении, пытаются скрыть эту информацию и не предпринимают никаких усилий с целью выявления злоумышленника, а администраторы просто стараются избавиться от непрошенного гостя.

Многие администраторы первым делом отключают сеанс злоумышленника, и только потом выясняют, как он проник в систему. Это неправильно, потому что по истечении времени вы не узнаете путь проникновения. Вероятнее всего, удастся определить учетную запись, которую он использовал, и максимум, что можно сделать, — поменять ее пароль.

А что если хакер получил доступ к учетной записи через ошибку в скрипте? В этом случае ему достаточно повторить те же действия, получить новый пароль и использовать его, пока администратор снова не увидит вторжение.

Лучший вариант, если сервер выполняет только одно определенное действие. Например, веб-сервер установлен на отдельной машине, а почтовый — на другой. В этом случае легко локализовать "чувствительное" место:

- уязвимость в ОС или сервисе — проверьте все последние отчеты об ошибках BugTraq и убедитесь, что у вас установлены все обновления;
- пароль пользователя — определите наличие незащищенного пароля пользователя, который мог подобрать хакер;
- прослушивание — поищите программу-снифер, если взлом произошел локально, возможно, пароль был получен с ее помощью;
- уязвимость в конфигурации — вы неправильно настроили систему или сервис, благодаря чему оказались доступными запрещенные ресурсы или пользователь смог повысить свои права.

Это наиболее распространенные ошибки, хотя мы уже знаем, что существуют и более изощренные и сложные методы взлома, но они производятся только профессионалами, а их во всем мире не так уж и много.

Самый простой вариант — локальный взлом (внутри сети). Достаточно доложить об инциденте начальству, и после наказания виновного подобные случаи не повторятся. Люди всегда страдают любопытством, поэтому этот порок надо как-то сдерживать.

Если взлом был произведен извне, то вы обязательно должны сначала узнать IP-адрес обидчика, а затем ограничить его права в системе. Если он работает через

простой аккаунт (учетная запись не принадлежит администратору), повысив привилегии, то вы должны установить уровень доступа в нужное состояние, чтобы хакер не натворил бед. Теперь можно и поиграть с ним.

Если хакер не испугался того, что его права были понижены, и попытается вернуть себе утраченное, то вы сможете увидеть, как это происходит. Для этого отслеживайте любые действия хакера по его IP-адресу и замеченной вами учетной записи. Ваша задача — определить лазейку, через которую он проникает в систему, и закрыть к ней доступ.

Если вы увидели, что на сервер началась атака отказа от обслуживания с помощью переполнения ресурсов, вы должны запретить прием лавины пакетов с узлов, с которых замечен интенсивный трафик. Благо, сетевые экраны сейчас есть в любой ОС. В UNIX-системах (таких, как Linux или FreeBSD) сетевые экраны достаточно мощные и позволяют защититься от кого угодно. В Windows эта утилита появилась недавно и только расширяет свои функциональные возможности.

Если сетевого экрана все же нет, то придется только смиренно наблюдать, как сервер переваривает всю входящую информацию. Если нагрузка приблизится к 90%, то я бы прервал на несколько минут соединение, чтобы переждать атаку. Если сервер зависнет, то на перезагрузку и восстановление работы может понадобиться намного больше времени. Если же отключение от сети невозможно из-за необходимости постоянной связи, то в этом случае можно только посочувствовать, потому что при такой нагрузке работа канала не может быть стабильной. Нужно было устанавливать сетевой экран, а в момент атаки это делать уже поздно.

От прослушивания трафика может помочь только шифрование. Если ваши серверные программы позволяют его использовать, то этот режим необходимо настроить заранее. Не стоит пытаться прятать траффик в туннели или пытаться запутать кого-то; это, скорее всего, не сработает. Лучше воспользоваться шифрованием. Да, оно кушает немного ресурсов компьютера, но работает надежно.

От атак типа "подставной DNS-сервер" или "ARP-запрос" администратор вообще ничего сделать не сможет. Тут уже поможет только разработчик программы DNS-сервера, которую вы используете, и обновление системы, или же полное отключение уязвимых сервисов.

Некоторые атаки могут производиться через отдельные просчеты в программе, например, через сценарии JavaScript. В этом случае их следует немедленно отключить и дождаться обновления браузера. Не дожидайтесь, когда хакер воспользуется ошибкой программистов и проникнет в ваш компьютер.

Но самое страшное для администратора — это атака с целью уничтожения (при отсутствии копий). Я на своем домашнем компьютере ежемесячно делаю резервные копии основных каталогов, где хранятся мои исходные коды, документы, почта и т. д. Таким образом, если сломается жесткий диск или все удалит вирус/хакер, то максимум, что я потеряю, — это месяц работы.

Некоторые администраторы вообще не задумываются о такой проблеме. Я работал в одной производственной фирме, так там регулярно создавалась резервная копия

только контроллера домена, а на файловом, почтовом, веб-сервере и сервере базы данных делали резервную копию, когда вспоминали. А это происходило раз в месяц или даже реже. С таким отношением администраторы могли лишиться всей информации, накопленной в течение многих лет, и принести бюджету своей фирмы многомиллионные убытки. А ведь потеря базы данных может привести даже к банкротству предприятия.

Защита от нападения — это война с хакерами, и побеждает тот, кто быстрее реагирует на изменение ситуации. Враг не спит, поэтому всегда нужно следить за безопасностью своей системы. Атаки хакеров чаще всего проводятся массово в момент появления новой уязвимости. Это подтверждает тот факт, что 90% хакеров — молодые ребята, которые используют чужие методы. Как только кто-то найдет новый способ, большая армия ламохакеров бежит его испытывать. Некоторые делают это со злым умыслом, но большинство все же просто ограничивается шалостью. Но и озорство может оказаться смертельным для компании, если будет украдена или уничтожена очень важная информация.

Если вы администрируете сервер, то в вашем арсенале должны быть все необходимые программы для выявления удаленных атак. Для домашнего компьютера такой программой может служить сетевой экран, но для сервера нужно принять дополнительные меры по мониторингу системы. Чем раньше вы заметите вторжение, тем меньше будет нежелательных последствий от взлома компьютера.

5.10.1. Резервирование и восстановление

Никто не застрахован от вторжения. Вы должны быть готовы ко всему и четко спланировать ваши действия, потому что только так можно максимально быстро отреагировать в критической ситуации. Для этого вы должны заранее на тестовой системе отработать различные варианты вторжения. Вам необходимо на практике (и в совершенстве) овладеть следующими навыками:

- ❒ восстановление работоспособности ОС, включая воссоздание всех конфигурационных файлов. Если хакер оставил потайной ход, то, вернув все конфигурационные файлы, можно восстановить систему в состояние на момент взлома, и тогда потайная дверь закроется сама по себе;
- ❒ восстановление баз данных и всех рабочих файлов. Атаки хакеров нередко направлены на уничтожение именно такой информации. Если утраченные файлы достаточно скопировать из резервной копии на исходное место, то для восстановления базы данных нужны дополнительные знания.

Для реализации этих двух пунктов нужно четко следовать такой политике резервного копирования, которая позволяла бы быстро производить восстановление с минимальными потерями. Существуют три основные стратегии:

1. Если какие-то файлы изменяются редко и незначительно, то можно делать резервные копии с большими промежутками времени. Если последние изменения и будут утеряны, то за счет небольшого их объема ручное восстановление не потребует много времени.

2. Если данные модифицируются часто, но незначительно, тогда можно сохранять только эти изменения.
3. Если данные изменяются часто и существенно, то выгоднее сохранять полную их копию.

Кроме этого, резервные копии необходимо делать и после каждого значительного/важного изменения данных или конфигурации системы.

Резервное копирование рабочих файлов должно производиться ежедневно, и не на локальный диск компьютера, а на съемные носители типа CD-R/RW, DVD, сменные диски или внешние дисководы.

Если вы делаете ежедневные копии на перезаписываемые носители, то сохраняйте их в течение месяца. Только после этого можно стирать данные и записывать на их место новые. Ежемесячные копии лучше делать для постоянного хранения. В этом случае вы всегда сможете посмотреть конфигурационные файлы, которые были в системе на определенный период времени, и откатить систему в случае неудачной настройки.

Резервное копирование позволяет защититься не только от вторжения, но и от нарушений в работе системы, поломок носителей информации (жесткие диски) и т. д. Не менее часто встречающаяся ситуация — неверные действия операторов или ошибки в программах, которые также могут привести к потере информации. Когда восстановить удаленную (искаженную) информацию не удается, положение может спасти только резервная копия.

Резервирование можно автоматизировать, чтобы оно происходило в определенное время. Это удобно, но не дает гарантии целостности данных. Однажды меня попросили восстановить систему после сбоя. На сервере в конце каждого рабочего дня запускалось автоматическое резервное копирование в один и тот же файл в сетевой папке. Это значит, что в любой момент можно было откатиться на сутки назад. Ошибка, которая привела к утере данных, произошла за 12 минут до автоматической процедуры, а заметили ее только через 15 минут. В этот момент уже началось очередное резервирование, и старая копия уничтожилась, а новая — уже стала содержать испорченные данные. Таким образом, неправильно настроенная автоматика сработала во вред. Вероятность возникновения такого случая минимальна, и я просто поражен, что смог увидеть подобное, но данный случай подтвердил, что возможно все. Лучше готовиться к худшему сценарию, чем встретиться с ним и быть не готовым.

Если вы являетесь администратором сервера, то отработайте все возможные механизмы восстановления данных заранее. У вас должна быть тестовая система для изучения всех нюансов восстановления данных после аварийных ситуаций различного масштаба и степени сложности.

Модели резервирования и восстановления могут различаться в зависимости от используемых программ или сервера баз данных. Следует внимательно ознакомиться с возможностями программного обеспечения, и после этого выбрать оптимальную для вас схему. Мы же рассмотрели только основы, потому что более конкретная информация выходит за рамки данной книги.

ПРИЛОЖЕНИЕ 1

Полезные программы

- **CyD Careful Observer** (**russia.cydsoft.com/**) — программа следит за соединением с указанными компьютерами и, если соединение разорвалось, выполняет указанное действие: выдает звук, отправляет e-mail, запускает программу или перезагружает компьютер.
- **CyD NET Utils** (**www.cydsoft.com/russia/**) — отличный, быстрый и удобный набор сетевых утилит для любого хакера и администратора. Позволяет проверять связь с удаленными компьютерами (ping), сканировать открытые порты (запущенные сервисы), сканировать открытые ресурсы и т. д.
- **John the Ripper** (**http://www.openwall.com/john/**) — программа подбора паролей для UNIX-систем.
- **Internet Scanner** (**http://www.iss.net/**) — один из лучших сканеров безопасности. Входит в комплект утилит IBM Internet Security System (система безопасности Интернета от фирмы IBM), который включает в себя множество программ по тестированию безопасности и выявлению вторжения.
- **Password Pro** (**http://www.insidepro.com/**) — программа подбора паролей для UNIX-систем.
- **Postman** (**http://www.cydsoft.com/russia/**) — программа для рассылки сообщений со встроенным сервером SMTP, что позволяет отправлять письма с поддельным e-mail-адресом.
- **PWLinside** (**http://www.insidepro.com/**) — программа подбора паролей для Windows 9*x*, ссылку для ее скачивания можно найти на форуме указанного сайта.
- **SAMinside** (**http://www.insidepro.com/**) — программа подбора паролей для Windows NT и систем, базирующихся на этой ОС.
- **SockChain** (**http://www.ufasoft.com/socks/**) — позволяет строить цепочки из proxy- и Socks-серверов, обеспечивая анонимность при работе в сети.

ПРИЛОЖЕНИЕ 2

Полезные ссылки

- **http://www.flenov.info/** — мой персональный блог.
- **http://www.cert.org/ —** хороший сервер, на котором есть раздел с описанием уязвимостей. Информация иногда поступает с задержкой, но очень хорошо описана.
- **http://www.securityfocus.com/** — еще один сайт с описанием уязвимостей.
- **http://www.2600.com/** — самый знаменитый журнал для хакеров.
- **http://www.defcon.org/ —** самая любимая тусовка для хакеров.

ПРИЛОЖЕНИЕ 3

Термины

- **ASP** — язык сценариев от корпорации Microsoft, который работает на платформе Windows.
- **CGI** — Common Getaway Interface или интерфейс, с помощью которого разрабатываются программы для веб-серверов на таких языках как Perl, C, Delphi и др.
- **Cookies** — технология, которая позволяет веб-сайтам сохранять какую-либо информацию на жестком диске пользователя.
- **DNS** — протокол определения IP-адреса компьютера по его доменному имени.
- **Firewall** — сетевой экран, который позволяет защищать компьютер или целую сеть от вторжения. Основой этой защиты является фильтрация пакетов на основе определенных правил.
- **FTP** — протокол передачи файлов по сети.
- **Hub** (концентратор) — устройство, с помощью которого компьютеры объединяются в сеть кабелем типа "витая пара". При этом все пакеты, приходящие на один порт, тиражируются на все порты устройства, т. е. пересылаются всем компьютерам, подключенным к устройству.
- **IP-адрес** — адрес устройства или компьютера в сети размером в 32 бита. В ближайшее время намечается переход на новую версию протокола IP, который имеет большую длину адреса, и, следовательно, можно использовать в сети намного больше устройств.
- **MAC address** (Media Access Control address) — это 48-разрядное число, которое присваивается каждому сетевому адаптеру производителем.
- **PHP** — язык сценариев для веб-страниц. Этот язык в последнее время набирает все большую популярность, потому что его реализация есть для всех основных платформ, и при этом язык достаточно прост и удобен.
- **RFC** (Request For Comments) — документы, описывающие рекомендации для реализации различных технологий. Например, в RFC описана реализация протокола SMTP, и при реализации данного протокола в своих программах желатель-

но следовать этим рекомендациям. Следование рекомендациям не является обязательным, но желательно.

- **Switch** (коммутатор) — устройство, с помощью которого компьютеры объединяются в сеть кабелем типа "витая пара". При этом пакеты, приходящие на один порт, отправляются только на тот порт, где подключен компьютер-получатель. Таким образом, усложняется прослушивание чужого трафика.
- **Анонимный доступ** — доступ к серверу, который не требует авторизации. В случае с FTP для этого надо указать в качестве имени слово Anonymous, а вместо пароля — свой e-mail. При таком имени пароль не проверяется, поэтому можно указывать любой почтовый адрес, главное, чтобы был похож на правду. С таким доступом чаще всего права ограничены, и вы сможете только просматривать открытую информацию. Изменять и удалять файлы, чаще всего, запрещено, и никаких важных данных вы не увидите.
- **Дейтаграмма** — пакет данных, который отправляется в сеть. Для его отправки не требуется устанавливать соединение и отправитель не получает подтверждения об удачной доставке данных.
- **Демон** — серверная программа, которая работает в фоновом режиме и предназначена для выполнения каких-либо действий. Этот термин применяется в *NIX-средах. Названия таких программ, в основном, отличаются тем, что в конце имени стоит буква "d". Например, демон веб-сервера — это программа, которая загружена в памяти и ждет подключения на 80-й порт (по умолчанию; порт может быть изменен). Как только клиент подсоединился, демон начинает принимать запросы и отвечать на них. Демоны бывают не только сетевыми: к сетевым, например, невозможно отнести демон печати.
- **Контрольная сумма** — число, которое рассчитывается по определенному алгоритму и по которому можно определить целостность данных: если расчет по имеющимся данным дает неверную контрольную сумму, то данные неточны.
- **Порт** — каждая сетевая программа при старте открывает для себя какой-то свободный порт. Некоторые порты зарезервированы, например 21-й порт используется для протокола FTP, 80-й — для протокола HTTP и т. д. Допустим, что на сервере запущены два сервиса: FTP и Web. Это значит, что на сервере работают две программы, к которым можно подключатся по сети. Если вы хотите присоединиться к FTP-серверу, вы посылаете запрос по адресу XXX.XXX.XXX.XXX на порт 21. Сервер получает такой запрос и по номеру порта определяет, что запрос относится именно к FTP-, а не к Web-серверу. Так что сетевые порты — это нечто виртуальное, что увидеть невозможно. Но если бы не было портов, то компьютер не смог бы определить, для кого именно пришел сетевой запрос.
- **Службы** — это то же самое, что и *демоны*, но эта терминология принята в Windows.
- **Сплоит** — программа, которая умеет пользоваться какой-нибудь уязвимостью. Если он написан под *NIX, то может поставляться в исходных кодах. В этом случае перед использованием потребуется компиляция.

- **Троянская программа** — программа, которая незаметно сидит в системе жертвы и позволяет управлять его компьютером. Такие программы чаще всего состоят из двух частей — клиента и сервера. Сервер забрасывается на компьютер жертвы и запускается. Теперь с помощью клиента можно подключатся к серверу и заставлять сервер выполнять определенные действия. Бывают троянские программы, состоящие только из сервера. В этом случае, когда жертва запускает такой файл, сервер выполняет определенные действия (например, пересылает все найденные пароли в Интернет) и может после этого самоуничтожаться.

ПРИЛОЖЕНИЕ 4

Описание электронного архива

По ссылке **ftp://85.249.45.166/9785977507905.zip** можно скачать электронный архив с материалами к главам книги. Эта ссылка доступна также со страницы книги на сайте **www.bhv.ru**.

Содержимое архива представлено в табл. П4.1.

Таблица П4.1

Папки	Описание
\Chapter1	Файлы, которые помогут украсить Windows и Internet Explorer
\Chapter2	Файлы, использованные в материалах *главы 2*
\Chapter3	Файлы для *главы 3*
\Chapter4	Программа CyD Archiver XP, позволяющая сделать архивы недоступными
\Chapter5	Файлы, использованные в материалах *главы 5*
\Doc	Статьи, полезные для ознакомления
\Soft	Демонстрационные программы от CyD Software Labs. Большинство из них использовались для подготовки материала книги

Список литературы

1. Фленов М. Е. Программирование на C++ глазами хакера. — СПб.: БХВ-Петербург, 2004. 330 с.
2. Фленов М. Е. Программирование в Delphi глазами хакера. — СПб.: БХВ-Петербург, 2003. 380 с.
3. **http://www.vr-online.ru/** — сайт для программистов и администраторов.
4. **http://www.flenov.net/** — новостной сайт с информацией об уязвимостях.
5. **http://www.xakep.ru/** — сайт журнала "Хакер". На сайте вы можете найти статьи о хакерах и о смежных вопросах, а также статьи автора книги.
6. Фленов М. Е. Web-сервер глазами хакера. — СПб.: БХВ-Петербург, 2009. 300 с.
7. Фленов М. Е. PHP глазами хакера. — СПб.: БХВ-Петербург, 2010.

Предметный указатель

З

И

К

Л

М

Н

О

П

С

Т

У

Ф

Х

Ч

Ш

Я

КОМПЬЮТЕР ГЛАЗАМИ ХАКЕРА

Новый взгляд и новые возможности в третьем издании мирового бестселлера, популярного в России, Европе, США и Канаде

3-е издание

Компьютер, операционная система Windows и Интернет во многом определяют облик и темп нашей современной жизни. Эти «три кита» рассмотрены в книге с точки зрения хакера. Вы узнаете про тюнинг (оптимизацию и ускорение), что позволит вам получить от компьютера максимум возможностей. В книге рассматриваются вопросы взлома и защиты ОС Windows и Интернета, а также веселые розыгрыши друзей и коллег с помощью компьютера.

Большая часть книги посвящена рассмотрению атак хакеров: начиная со сбора информации об атакуемой системе до непосредственного взлома. На практике рассматриваются примеры накручивания счетчиков на интернет-сайтах и взлом простых вариантов защиты программ Shareware. Отдельная глава посвящена советам хакеров, которые позволят вам во время путешествия в Интернете не «заразиться» троянской программой или не попасть на удочку сетевых мошенников, манипулирующих поведением людей, используя методики социальной инженерии.

Прочитав книгу, вы не станете хакером, но сможете сделать интерфейс Windows более удобными и привлекательным, компьютер — надежнее и быстрее, а работу в сети — более безопасной.

Флёнов Михаил, профессиональный программист. Работал в журнале «Хакер», в котором несколько лет вел рубрики «Hack-FAQ» и «Кодинг» для программистов, печатался в журналах «Игромания» и «Chip-Россия». Автор бестселлеров «Библия Delphi», «Программирование в Delphi глазами хакера», «Программирование на C++ глазами хакера», «Web-сервер глазами хакера» и др. Некоторые книги переведены на иностранные языки и популярны в США, Канаде, Польше и других странах.

Каждый «чайник» рано или поздно становится пользователем. Пользователь — продвинутым пользователем. Продвинутый пользователь учится, читает книги, ковыряет программы, изучает протоколы, ломает, портит, программирует, создает. Он совершенствует свои знания. Обычно для этого ему приходится прочесть немало книг, статей, до некоторых вещей дойти методом проб, ошибок и переустановок программ. Эта книга, несмотря на название, не сделает тебя хакером. Никто не сделает тебя хакером кроме тебя самого :), но вот заменить множество книг и «опытов» на пути от «чайника» к продвинутому пользователю она сможет. Читай ее и радуйся, что сегодня ты избавился от лишней переустановки системы, нудного чтения некоторых мануалов и порчи оборудования.

А. Лозовский, выпускающий редактор журнала «ИТСпец» и рубрики «Кодинг» в журнале «Хакер»

Программы, описанные в книге, а также используемые файлы и дополнительные статьи можно скачать по ссылке ftp://85.249.45.166/9785977507905.zip, а также со страницы книги на сайте www.bhv.ru.

ISBN 978-5-9775-0790-5

БХВ-ПЕТЕРБУРГ
190005, Санкт-Петербург,
Измайловский пр., 29
E-mail: mail@bhv.ru
Internet: www.bhv.ru
Тел.: (812) 251-42-44
Факс: (812) 320-01-79