

Антивирус Касперского 2013

KASPERSKY **lab**

Руководство пользователя

ВЕРСИЯ ПРОГРАММЫ: 13.0

ИСТОЧНИКИ ИНФОРМАЦИИ О ПРОГРАММЕ

Этот раздел содержит описание источников информации о программе и сведения о веб-сайтах, которые вы можете использовать, чтобы обсудить работу программы.

Вы можете выбрать наиболее удобный источник информации в зависимости от важности и срочности вопроса.

В ЭТОМ РАЗДЕЛЕ

Источники информации для самостоятельного поиска.....	9
Обсуждение программ «Лаборатории Касперского» на форуме.....	10
Обращение в Департамент продаж	10
Обращение в Отдел локализации и разработки технической документации.....	10

ИСТОЧНИКИ ИНФОРМАЦИИ ДЛЯ САМОСТОЯТЕЛЬНОГО ПОИСКА

Вы можете использовать следующие источники для самостоятельного поиска информации о программе:

- страница на веб-сайте «Лаборатории Касперского»;
- страница на веб-сайте Службы технической поддержки (База знаний);
- электронная справка;
- документация.

Если вы не нашли решения возникшей проблемы самостоятельно, рекомендуем вам обратиться в Службу технической поддержки «Лаборатории Касперского» (см. раздел «Техническая поддержка по телефону» на стр. [58](#)).

Для использования источников информации на веб-сайте «Лаборатории Касперского» необходимо подключение к интернету.

Страница на веб-сайте «Лаборатории Касперского»

Веб-сайт «Лаборатории Касперского» содержит отдельную страницу для каждой программы.

На странице (http://www.kaspersky.ru/kaspersky_anti-virus) вы можете получить общую информацию о программе, ее возможностях и особенностях работы.

Страница <http://www.kaspersky.ru> содержит ссылку на интернет-магазин. В нем вы можете приобрести программу или продлить право пользования программой.

Страница на веб-сайте Службы технической поддержки (База знаний)

База знаний – раздел веб-сайта Службы технической поддержки, содержащий рекомендации по работе с программами «Лаборатории Касперского». База знаний состоит из справочных статей, сгруппированных по темам.

На странице программы в Базе знаний (<http://support.kaspersky.ru/kav2013>) вы найдете статьи, которые содержат полезную информацию, рекомендации и ответы на часто задаваемые вопросы о приобретении, установке и использовании программы.

Статьи могут отвечать на вопросы, которые относятся не только к Антивирусу Касперского, но и к другим программам «Лаборатории Касперского», а также могут содержать новости Службы технической поддержки.

Электронная справка

В состав электронной справки программы входят файлы справки.

Контекстная справка содержит сведения о каждом окне программы: перечень и описание параметров и список решаемых задач.

Полная справка содержит подробную информацию о том, как управлять защитой, настраивать параметры программы и решать основные задачи пользователя.

Документация

Руководство пользователя программы содержит информацию об установке, активации, настройке параметров программы, а также сведения о работе с программой. В документе приведено описание интерфейса программы, предложены способы решения типовых задач пользователя при работе с программой.

ОБСУЖДЕНИЕ ПРОГРАММ «ЛАБОРАТОРИИ КАСПЕРСКОГО» НА ФОРУМЕ

Если ваш вопрос не требует срочного ответа, вы можете обсудить его со специалистами «Лаборатории Касперского» и другими пользователями на нашем форуме (<http://forum.kaspersky.com>).

На форуме вы можете просматривать опубликованные темы, добавлять свои комментарии, создавать новые темы для обсуждения.

ОБРАЩЕНИЕ В ДЕПАРТАМЕНТ ПРОДАЖ

Если у вас возникли вопросы по выбору, приобретению или продлению срока использования программы, вы можете связаться с нашими специалистами из Департамента продаж одним из следующих способов:

- Позвонив по телефонам нашего центрального офиса в Москве (<http://www.kaspersky.ru/contacts>).
- Отправив письмо с вопросом по электронному адресу sales@kaspersky.com.

Обслуживание осуществляется на русском и английском языках.

ОБРАЩЕНИЕ В ОТДЕЛ ЛОКАЛИЗАЦИИ И РАЗРАБОТКИ ТЕХНИЧЕСКОЙ ДОКУМЕНТАЦИИ

Для обращения в Группу разработки документации требуется отправить письмо по адресу docfeedback@kaspersky.com. В качестве темы письма нужно указать «Kaspersky Help Feedback: Антивирус Касперского».

Почтовый Антивирус

Почтовый Антивирус проверяет входящие и исходящие почтовые сообщения на вашем компьютере. Письмо будет доступно адресату только в том случае, если оно не содержит опасных объектов.

Веб-Антивирус

Веб-Антивирус перехватывает и блокирует выполнение скриптов, расположенных на веб-сайтах, если эти скрипты представляют угрозу безопасности компьютера. Веб-Антивирус также контролирует весь веб-трафик и блокирует доступ к опасным веб-сайтам.

IM-Антивирус

IM-Антивирус обеспечивает безопасность работы с интернет-пейджерами. Компонент защищает информацию, поступающую на ваш компьютер по протоколам интернет-пейджеров. IM-Антивирус обеспечивает безопасную работу со многими программами, предназначенными для быстрого обмена сообщениями.

Мониторинг сети

Мониторинг сети предназначен для наблюдения за сетевой активностью в реальном времени.

Анти-Фишинг

Анти-Фишинг позволяет проверять веб-адреса на принадлежность к списку фишинговых веб-адресов. Этот компонент встроен в Веб-Антивирус и IM-Антивирус.

Анти-Баннер

Анти-Баннер блокирует рекламные баннеры, размещенные на веб-сайтах и в интерфейсах программ.

СЕРВИС ДЛЯ ПОЛЬЗОВАТЕЛЕЙ

Приобретая лицензию на использование программы, в течение срока действия лицензии вы можете получать следующие услуги:

- обновление баз и предоставление новых версий программы;
- консультации по телефону и электронной почте по вопросам, связанным с установкой, настройкой и использованием программы;
- оповещение о выходе новых программ «Лаборатории Касперского», а также информацию о появлении новых вирусов и вирусных эпидемиях. Для использования этой услуги требуется подписаться на рассылку новостей ЗАО «Лаборатория Касперского» на веб-сайте Службы технической поддержки.

Консультации по работе операционных систем, стороннего программного обеспечения и технологиям не проводятся.

АППАРАТНЫЕ И ПРОГРАММНЫЕ ТРЕБОВАНИЯ

Для функционирования Kaspersky Internet Security и Антивируса Касперского компьютер должен удовлетворять следующим требованиям:

Общие требования:

- 480 МБ свободного места на жестком диске (в том числе 380 МБ на системном диске).
- CD- / DVD-ROM (для установки Антивируса Касперского с дистрибутивного CD-диска).

УСТАНОВКА И УДАЛЕНИЕ ПРОГРАММЫ

Этот раздел содержит пошаговые инструкции по установке и удалению программы.

В ЭТОМ РАЗДЕЛЕ

Стандартная процедура установки	15
Обновление предыдущей версии Антивируса Касперского.....	18
Нетиповые сценарии установки	21
Удаление программы	21

СТАНДАРТНАЯ ПРОЦЕДУРА УСТАНОВКИ

Антивирус Касперского устанавливается на компьютер в интерактивном режиме с помощью мастера установки.

Мастер состоит из последовательности окон (шагов), переключение между которыми осуществляется нажатием на кнопки **Назад** и **Далее**. Работа мастера завершается нажатием на кнопку **Завершить**. Для прекращения работы мастера на любом этапе установки следует закрыть окно мастера.

Если программа будет использована для защиты более чем одного компьютера (максимально допустимое количество компьютеров зависит от условий вашей лицензии), то процедура установки будет одинаковой на всех компьютерах.

➔ *Чтобы установить Антивирус Касперского на ваш компьютер,*

на CD-диске с продуктом запустите файл дистрибутива (файл с расширением exe).

Для установки Антивируса Касперского вы также можете использовать дистрибутив, полученный через интернет. При этом для некоторых языков локализации мастер установки отображает несколько дополнительных шагов установки.

В ЭТОМ РАЗДЕЛЕ

Шаг 1. Поиск более новой версии программы	16
Шаг 2. Начало установки программы.....	16
Шаг 3. Просмотр Лицензионного соглашения	16
Шаг 4. Положение об использовании Kaspersky Security Network.....	16
Шаг 5. Установка	17
Шаг 6. Завершение установки	17
Шаг 7. Активация программы	17
Шаг 8. Регистрация пользователя	18
Шаг 9. Завершение активации.....	18

ШАГ 1. ПОИСК БОЛЕЕ НОВОЙ ВЕРСИИ ПРОГРАММЫ

Перед началом установки мастер проверяет наличие более актуальной версии Антивируса Касперского на серверах обновлений «Лаборатории Касперского».

Если мастер установки не обнаружит на серверах обновлений более актуальную версию программы, он запустит установку текущей версии.

Если мастер обнаружит на серверах обновлений более актуальную версию Антивируса Касперского, он предложит вам загрузить и установить ее на ваш компьютер. Рекомендуется устанавливать новую версию программы, так как в новые версии вносятся улучшения, позволяющие более эффективно защищать ваш компьютер. Если вы откажетесь от установки новой версии, мастер запустит установку текущей версии программы. Если вы согласитесь установить новую версию программы, мастер установки скопирует файлы дистрибутива на ваш компьютер и запустит установку новой версии. Дальнейшее описание установки новой версии программы смотрите в документации к ней.

ШАГ 2. НАЧАЛО УСТАНОВКИ ПРОГРАММЫ

На этом этапе мастер установки предлагает вам установить программу.

Для продолжения установки нажмите на кнопку **Установить**.

В зависимости от типа установки и языка локализации на этом этапе мастер установки может предлагать вам ознакомиться с Лицензионным соглашением, которое заключается между вами и «Лабораторией Касперского», а также принять участие в программе Kaspersky Security Network.

ШАГ 3. ПРОСМОТР ЛИЦЕНЗИОННОГО СОГЛАШЕНИЯ

Этот шаг мастера установки отображается для некоторых языков локализации при установке Антивируса Касперского с дистрибутива, полученного через интернет.

На этом этапе мастер установки предлагает вам ознакомиться с Лицензионным соглашением, которое заключается между вами и «Лабораторией Касперского».

Внимательно прочитайте Лицензионное соглашение и, если вы согласны со всеми его пунктами, нажмите на кнопку **Принять**. Установка программы на ваш компьютер будет продолжена.

Если Лицензионное соглашение не принято, установка программы не производится.

ШАГ 4. ПОЛОЖЕНИЕ ОБ ИСПОЛЬЗОВАНИИ KASPERSKY SECURITY NETWORK

Этот шаг мастера установки отображается для некоторых языков локализации при установке Антивируса Касперского с дистрибутива, полученного через интернет.

На этом этапе мастер установки предлагает вам принять участие в программе Kaspersky Security Network. Участие в программе предусматривает отправку в ЗАО «Лаборатория Касперского» информации о новых угрозах, обнаруженных на вашем компьютере, о запускаемых программах и о загружаемых подписанных программах, а также информации о системе. При этом сбор, обработка и хранение ваших персональных данных не производятся.

Ознакомьтесь с положением об использовании Kaspersky Security Network. Если вы согласны со всеми его пунктами, в окне мастера установите флажок **Я хочу участвовать в программе Kaspersky Security Network (KSN)**.

Нажмите на кнопку **Далее**, чтобы продолжить установку программы.

ШАГ 5. УСТАНОВКА

Установка программы занимает некоторое время. Дождитесь ее завершения.

По завершении установки мастер автоматически переходит к следующему шагу.

Во время установки Антивирус Касперского производит ряд проверок. В результате этих проверок могут быть обнаружены следующие проблемы:

- **Несоответствие операционной системы программным требованиям.** Во время установки мастер проверяет соблюдение следующих условий:
 - соответствие операционной системы и пакетов обновлений (Service Pack) программным требованиям;
 - наличие необходимых программ;
 - наличие необходимого для установки свободного места на диске.

Если какое-либо из перечисленных условий не выполнено, на экран будет выведено соответствующее уведомление.

- **Наличие на компьютере несовместимых программ.** При обнаружении несовместимых программ их список будет выведен на экран, и вам будет предложено удалить их. Программы, которые Антивирус Касперского не может удалить автоматически, необходимо удалить вручную. Во время удаления несовместимых программ потребуется перезагрузка системы, после чего установка Антивируса Касперского продолжится автоматически.
- **Наличие на компьютере вредоносных приложений.** При обнаружении на компьютере вредоносных приложений, препятствующих установке антивирусных программ, мастер установки предложит загрузить специальное средство для устранения заражения – *утилиту Kaspersky Virus Removal Tool*.

Если вы согласитесь установить утилиту, мастер установки загрузит ее с серверов «Лаборатории Касперского», после чего автоматически запустится установка утилиты. Если мастер не сможет загрузить утилиту, он предложит вам загрузить ее самостоятельно, перейдя по предлагаемой ссылке.

ШАГ 6. ЗАВЕРШЕНИЕ УСТАНОВКИ

На этом этапе мастер информирует вас о завершении установки программы. Чтобы начать работу с Антивируса Касперского немедленно, убедитесь, что флажок **Запустить Антивирус Касперского 2013** установлен, и нажмите на кнопку **Готово**.

В некоторых случаях для завершения установки может потребоваться перезагрузка операционной системы. Если флажок **Запустить Антивирус Касперского 2013** установлен, после перезагрузки программа будет запущена автоматически.

Если перед завершением работы мастера вы сняли флажок **Запустить Антивирус Касперского 2013**, программу нужно будет запустить вручную.

ШАГ 7. АКТИВАЦИЯ ПРОГРАММЫ

На этом этапе мастер установки предлагает вам активировать программу.

Активация – это процедура введения в действие полнофункциональной версии программы на определенный срок.

Если вы приобрели лицензию на использование Антивирус Касперского и загрузили программу через интернет-магазин, активация программы может быть выполнена автоматически в процессе установки.

Вам предлагаются следующие варианты активации Антивируса Касперского:

- **Активировать коммерческую версию.** Выберите этот вариант и введите код активации (см. раздел «О коде активации» на стр. [24](#)), если вы приобрели коммерческую версию программы.

Если в поле ввода вы укажете код активации Kaspersky Internet Security, по завершении активации запустится процедура переключения на Kaspersky Internet Security.

- **Активировать пробную версию.** Выберите этот вариант активации, если вы хотите установить пробную версию программы перед принятием решения о покупке коммерческой версии. Вы сможете использовать программу в режиме полной функциональности в течение срока действия, ограниченного условиями пробной лицензии. По истечении срока действия лицензии возможность повторной активации пробной версии будет недоступна.

Для активации программы необходимо подключение к интернету.

ШАГ 8. РЕГИСТРАЦИЯ ПОЛЬЗОВАТЕЛЯ

Этот шаг доступен только при активации коммерческой версии программы. При активации пробной версии шаг пропускается.

Зарегистрированные пользователи получают возможность отправлять запросы в Службу технической поддержки и Вирусную Лабораторию через Личный кабинет на веб-сайте «Лаборатории Касперского», возможность удобного управления кодами активации, а также оперативную информацию о новых продуктах и специальных предложениях.

Если вы согласны зарегистрироваться, для отправки своих регистрационных данных в «Лабораторию Касперского» укажите их в соответствующих полях и нажмите на кнопку **Далее**.

В некоторых случаях регистрация пользователя необходима для использования программы.

ШАГ 9. ЗАВЕРШЕНИЕ АКТИВАЦИИ

Мастер информирует вас об успешном завершении активации Антивируса Касперского. Кроме того, в окне приводится информация о действующей лицензии: тип (коммерческая или пробная), дата окончания срока действия лицензии, а также количество компьютеров, на которые эта лицензия распространяется.

В случае подписки вместо даты окончания срока действия лицензии приводится информация о статусе подписки.

Нажмите на кнопку **Завершить**, чтобы завершить работу мастера.

ОБНОВЛЕНИЕ ПРЕДЫДУЩЕЙ ВЕРСИИ АНТИВИРУСА КАСПЕРСКОГО

Если на вашем компьютере уже установлен Антивирус Касперского 2011 или 2012, вам нужно обновить программу до версии Антивирус Касперского 2013. При наличии действующей лицензии на использование Антивирус Касперского 2011 или 2012 вам не понадобится активировать программу: мастер установки автоматически получит информацию о лицензии на использование Антивирус Касперского 2011 или 2012 и применит ее в процессе установки.

Антивирус Касперского устанавливается на компьютер в интерактивном режиме с помощью мастера установки.

Мастер состоит из последовательности окон (шагов), переключение между которыми осуществляется нажатием на кнопки **Назад** и **Далее**. Работа мастера завершается нажатием на кнопку **Завершить**. Для прекращения работы мастера на любом этапе установки следует закрыть окно мастера.

Если программа будет использована для защиты более чем одного компьютера (максимально допустимое количество компьютеров зависит от условий вашей лицензии), то процедура установки будет одинаковой на всех компьютерах.

➔ Чтобы установить Антивирус Касперского на ваш компьютер,

на CD-диске с продуктом запустите файл дистрибутива (файл с расширением exe).

Для установки Антивируса Касперского вы также можете использовать дистрибутив, полученный через интернет. При этом для некоторых языков локализации мастер установки отображает несколько дополнительных шагов установки.

В ЭТОМ РАЗДЕЛЕ

Шаг 1. Поиск более новой версии программы	19
Шаг 2. Начало установки программы.....	19
Шаг 3. Просмотр Лицензионного соглашения	20
Шаг 4. Положение об использовании Kaspersky Security Network.....	20
Шаг 5. Установка	20
Шаг 6. Завершение установки	21

ШАГ 1. ПОИСК БОЛЕЕ НОВОЙ ВЕРСИИ ПРОГРАММЫ

Перед началом установки мастер проверяет наличие более актуальной версии Антивируса Касперского на серверах обновлений «Лаборатории Касперского».

Если мастер установки не обнаружит на серверах обновлений более актуальную версию программы, он запустит установку текущей версии.

Если мастер обнаружит на серверах обновлений более актуальную версию Антивируса Касперского, он предложит вам загрузить и установить ее на ваш компьютер. Рекомендуется устанавливать новую версию программы, так как в новые версии вносятся улучшения, позволяющие более эффективно защищать ваш компьютер. Если вы откажетесь от установки новой версии, мастер запустит установку текущей версии программы. Если вы согласитесь установить новую версию программы, мастер установки скопирует файлы дистрибутива на ваш компьютер и запустит установку новой версии. Дальнейшее описание установки новой версии программы смотрите в документации к ней.

ШАГ 2. НАЧАЛО УСТАНОВКИ ПРОГРАММЫ

На этом этапе мастер установки предлагает вам установить программу.

Для продолжения установки нажмите на кнопку **Установить**.

В зависимости от типа установки и языка локализации на этом этапе мастер установки может предлагать вам ознакомиться с Лицензионным соглашением, которое заключается между вами и «Лабораторией Касперского», а также принять участие в программе Kaspersky Security Network.

ШАГ 3. ПРОСМОТР ЛИЦЕНЗИОННОГО СОГЛАШЕНИЯ

Этот шаг мастера установки отображается для некоторых языков локализации при установке Антивируса Касперского с дистрибутива, полученного через интернет.

На этом этапе мастер установки предлагает вам ознакомиться с Лицензионным соглашением, которое заключается между вами и «Лабораторией Касперского».

Внимательно прочитайте Лицензионное соглашение и, если вы согласны со всеми его пунктами, нажмите на кнопку **Принять**. Установка программы на ваш компьютер будет продолжена.

Если Лицензионное соглашение не принято, установка программы не производится.

ШАГ 4. ПОЛОЖЕНИЕ ОБ ИСПОЛЬЗОВАНИИ KASPERSKY SECURITY NETWORK

Этот шаг мастера установки отображается для некоторых языков локализации при установке Антивируса Касперского с дистрибутива, полученного через интернет.

На этом этапе мастер установки предлагает вам принять участие в программе Kaspersky Security Network. Участие в программе предусматривает отправку в ЗАО «Лаборатория Касперского» информации о новых угрозах, обнаруженных на вашем компьютере, о запускаемых программах и о загружаемых подписанных программах, а также информации о системе. При этом сбор, обработка и хранение ваших персональных данных не производятся.

Ознакомьтесь с положением об использовании Kaspersky Security Network. Если вы согласны со всеми его пунктами, в окне мастера установите флажок **Я хочу участвовать в программе Kaspersky Security Network (KSN)**.

Нажмите на кнопку **Далее**, чтобы продолжить установку программы.

ШАГ 5. УСТАНОВКА

Установка программы занимает некоторое время. Дождитесь ее завершения.

По завершении установки мастер автоматически переходит к следующему шагу.

Во время установки Антивирус Касперского производит ряд проверок. В результате этих проверок могут быть обнаружены следующие проблемы:

- **Несоответствие операционной системы программным требованиям.** Во время установки мастер проверяет соблюдение следующих условий:
 - соответствие операционной системы и пакетов обновлений (Service Pack) программным требованиям;
 - наличие необходимых программ;
 - наличие необходимого для установки свободного места на диске.

Если какое-либо из перечисленных условий не выполнено, на экран будет выведено соответствующее уведомление.

- **Наличие на компьютере несовместимых программ.** При обнаружении несовместимых программ их список будет выведен на экран, и вам будет предложено удалить их. Программы, которые Антивирус Касперского не может удалить автоматически, необходимо удалить вручную. Во время удаления несовместимых программ потребуется перезагрузка системы, после чего установка Антивируса Касперского продолжится автоматически.

- **Наличие на компьютере вредоносных приложений.** При обнаружении на компьютере вредоносных приложений, препятствующих установке антивирусных программ, мастер установки предложит загрузить специальное средство для устранения заражения – *утилиту Kaspersky Virus Removal Tool*.

Если вы согласитесь установить утилиту, мастер установки загрузит ее с серверов «Лаборатории Касперского», после чего автоматически запустится установка утилиты. Если мастер не сможет загрузить утилиту, он предложит вам загрузить ее самостоятельно, перейдя по предлагаемой ссылке.

ШАГ 6. ЗАВЕРШЕНИЕ УСТАНОВКИ

Это окно мастера информирует вас о завершении установки программы.

По завершении установки необходимо перезагрузить операционную систему.

Если флажок **Запустить Антивирус Касперского** установлен, после перезагрузки программа будет запущена автоматически.

Если перед завершением работы мастера вы сняли флажок **Запустить Антивирус Касперского**, программу нужно запустить вручную.

НЕТИПОВЫЕ СЦЕНАРИИ УСТАНОВКИ

В этом разделе описаны сценарии установки программы, которые отличаются от стандартной установки или обновления с предыдущей версии.

Установка Антивируса Касперского с активацией с помощью кода активации Kaspersky Internet Security

Если в процессе установки Антивируса Касперского на шаге Активация программы вы введете код активации Kaspersky Internet Security, то будет запущен мастер миграции, в результате работы которого на ваш компьютер будет установлен Kaspersky Internet Security.

Если в процессе установки Антивируса Касперского на шаге Активация программы вы выберете вариант **Активировать позже**, а затем активируете установленную программу с помощью кода активации Kaspersky Internet Security, то также будет запущен мастер миграции, в результате работы которого Антивирус Касперского переключится на Kaspersky Internet Security.

Установка Антивируса Касперского 2013 поверх Kaspersky Internet Security 2011 или 2012

Если вы запустите установку Антивируса Касперского 2013 на компьютере, на котором уже установлен Kaspersky Internet Security 2011 или 2012 с действующей лицензией, то мастер установки, обнаружив это, предложит вам выбрать вариант дальнейших действий:

- Продолжить использовать Kaspersky Internet Security по действующей лицензии. В этом случае будет запущен мастер миграции, в результате работы которого на ваш компьютер будет установлен Kaspersky Internet Security 2013. Вы сможете пользоваться Kaspersky Internet Security 2013 в течение срока действия лицензии на использование Kaspersky Internet Security 2011 или 2012.
- Продолжить установку Антивируса Касперского 2013. В этом случае процедура установки будет продолжена согласно стандартному сценарию, начиная с шага Активация программы.

УДАЛЕНИЕ ПРОГРАММЫ

В результате удаления Антивируса Касперского компьютер и ваши личные данные окажутся незащищенными!

Удаление Антивируса Касперского выполняется с помощью мастера установки.

➔ Чтобы запустить мастер,

в меню **Пуск** выберите пункт **Программы** → **Антивирус Касперского 2013** → **Удалить Антивирус Касперского 2013**.

В ЭТОМ РАЗДЕЛЕ

Шаг 1. Сохранение данных для повторного использования	22
Шаг 2. Подтверждение удаления программы	22
Шаг 3. Удаление программы. Завершение удаления	22

ШАГ 1. СОХРАНЕНИЕ ДАННЫХ ДЛЯ ПОВТОРНОГО ИСПОЛЬЗОВАНИЯ

На этом шаге вы можете указать, какие используемые программой данные вы хотите сохранить для дальнейшего использования при повторной установке программы (например, при установке более новой версии).

По умолчанию программа предлагает сохранить информацию об активации.

➔ Чтобы сохранить данные для повторного использования, выполните следующие действия:

1. Установите флажки напротив тех данных, которые нужно сохранить:

- **Информация о лицензии** – данные, позволяющие в дальнейшем не активировать устанавливаемую программу, а использовать ее по уже действующей лицензии, если срок действия лицензии не истечет к моменту установки.
- **Объекты карантина** – файлы, проверенные программой и помещенные на карантин.

При удалении Антивируса Касперского с компьютера файлы на карантине будут недоступны. Для работы с этими файлами нужно установить Антивирус Касперского.

- **Параметры работы программы** – значения параметров работы программы, установленные во время ее настройки.
- **Данные iChecker** – файлы, содержащие информацию об объектах, уже проверенных с помощью технологии iChecker .

ШАГ 2. ПОДТВЕРЖДЕНИЕ УДАЛЕНИЯ ПРОГРАММЫ

Поскольку удаление программы ставит под угрозу защиту компьютера и ваших личных данных, требуется подтвердить свое намерение удалить программу. Для этого нажмите на кнопку **Удалить**.

ШАГ 3. УДАЛЕНИЕ ПРОГРАММЫ. ЗАВЕРШЕНИЕ УДАЛЕНИЯ

На этом шаге мастер удаляет программу с вашего компьютера. Дождитесь завершения процесса удаления.

В процессе удаления требуется перезагрузка операционной системы. Если вы откажетесь от немедленной перезагрузки, завершение процедуры удаления будет отложено до того момента, когда операционная система будет перезагружена или компьютер будет выключен и включен.

ЛИЦЕНЗИРОВАНИЕ ПРОГРАММЫ

Этот раздел содержит информацию об основных понятиях, связанных с активацией программы. Из этого раздела вы узнаете о назначении Лицензионного соглашения, типах лицензии, способах активации программы, а также о продлении срока действия лицензии.

В ЭТОМ РАЗДЕЛЕ

О Лицензионном соглашении	23
О лицензии.....	23
О коде активации.....	24
О предоставлении данных.....	24

О ЛИЦЕНЗИОННОМ СОГЛАШЕНИИ

Лицензионное соглашение – это юридическое соглашение между вами и ЗАО «Лаборатория Касперского», в котором указано, на каких условиях вы можете использовать программу.

Внимательно ознакомьтесь с условиями Лицензионного соглашения перед началом работы с программой.

Считается, что вы принимаете условия Лицензионного соглашения, подтверждая свое согласие с текстом Лицензионного соглашения при установке программы. Если вы не согласны с условиями Лицензионного соглашения, вы должны прервать установку программы или не использовать программу.

О ЛИЦЕНЗИИ

Лицензия – это ограниченное по времени право на использование программы, предоставляемое вам на основе Лицензионного соглашения. С лицензией связан уникальный код активации вашего экземпляра Антивируса Касперского.

Лицензия включает в себя право на получение следующих видов услуг:

- Использование программы на одном или нескольких устройствах.

Количество устройств, на которых вы можете использовать программу, определяется условиями Лицензионного соглашения.

- Обращение в Службу технической поддержки «Лаборатории Касперского».
- Получение прочих услуг, предоставляемых вам «Лабораторией Касперского» или ее партнерами в течение срока действия лицензии (см. раздел «Сервис для пользователей» на стр. [13](#)).

Объем предоставляемых услуг и срок использования программы зависят от типа лицензии, по которой была активирована программа.

Предусмотрены следующие типы лицензий:

- *Пробная* – бесплатная лицензия, предназначенная для ознакомления с программой.

Пробная лицензия обычно имеет небольшой срок действия. По истечении срока действия пробной лицензии Антивирус Касперского прекращает выполнять все свои функции. Для продолжения использования программы требуется приобрести коммерческую лицензию.

- *Коммерческая* – платная лицензия, предоставляемая при приобретении программы.

По истечении срока действия коммерческой лицензии программа продолжает работу, но с ограниченной функциональностью (например, недоступно обновление и использование сервиса Kaspersky Security Network). Вы по-прежнему можете использовать все компоненты программы и выполнять проверку на вирусы и другие программы, представляющие угрозу, но только на основе баз, установленных до даты окончания срока действия лицензии. Для продолжения использования Антивируса Касперского в режиме полной функциональности требуется продлить срок действия коммерческой лицензии.

Рекомендуется продлевать срок действия лицензии не позднее даты его окончания, чтобы обеспечить максимальную защиту от всех угроз компьютерной безопасности.

О КОДЕ АКТИВАЦИИ

Код активации – это код, который вы получаете, приобретая коммерческую лицензию на использование Антивируса Касперского. Этот код необходим для активации программы.

Код активации представляет собой уникальную последовательность из двадцати латинских букв и цифр в формате xxxxx-xxxxx-xxxxx-xxxxx.

В зависимости от способа приобретения программы возможны следующие варианты получения кода активации:

- Если вы приобрели коробочную версию Антивируса Касперского, код активации указан в документации или на коробке, в которой находится установочный компакт-диск.
- Если вы приобрели Антивирус Касперского в интернет-магазине, код активации высылается по адресу электронной почты, указанному вами при заказе.

Отсчет срока действия лицензии начинается с даты активации программы. Если вы приобрели лицензию, допускающую использование Антивируса Касперского на нескольких устройствах, то отсчет срока действия лицензии начинается с даты первого применения кода активации.

Если код активации был потерян или случайно удален после активации программы, то для его восстановления требуется отправить запрос в Службу технической поддержки «Лаборатории Касперского» из Личного кабинета (см. раздел «Получение технической поддержки через Личный кабинет» на стр. [59](#)).

О ПРЕДОСТАВЛЕНИИ ДАННЫХ

Для повышения уровня оперативной защиты, принимая условия Лицензионного соглашения, вы соглашаетесь в автоматическом режиме предоставлять «Лаборатории Касперского» следующую информацию:

- информацию о контрольных суммах обрабатываемых файлов (MD5);
- информацию для определения репутации URL;
- статистику использования продуктовых уведомлений;
- статистические данные для защиты от спама;
- данные об активации и используемой версии Антивируса Касперского;

- информацию о типах обнаруженных угроз;
- информацию об используемых цифровых сертификатах и информацию, необходимую для проверки их подлинности.

Если компьютер оборудован модулем TPM (Trusted Platform Module), то вы также соглашаетесь предоставлять «Лаборатории Касперского» отчет TPM о загрузке операционной системы компьютера и информацию, необходимую для проверки подлинности отчета. При возникновении ошибки установки Антивируса Касперского вы соглашаетесь в автоматическом режиме предоставить «Лаборатории Касперского» информацию о коде ошибки, используемом дистрибутиве и компьютере.

При участии в программе Kaspersky Security Network (см. раздел «Участие в Kaspersky Security Network (KSN)» на стр. 54) в «Лабораторию Касперского» автоматически передается следующая информация, полученная в результате работы Антивируса Касперского на компьютере:

- информация об установленном аппаратном и программном обеспечении;
- информация о состоянии антивирусной защиты компьютера, а также обо всех потенциально вредоносных объектах и действиях и принятых решений относительно этих объектов и действий;
- информация о загружаемых и запускаемых программах;
- информация об ошибках и использовании пользовательского интерфейса Антивируса Касперского;
- информация о версии используемых баз программы;
- статистика обновлений и соединений с серверами «Лаборатории Касперского».

Также для дополнительной проверки в «Лабораторию Касперского» могут отправляться файлы (или их части), в отношении которых существует риск использования их злоумышленником для нанесения вреда компьютеру или данным.

Полученная информация защищается «Лабораторией Касперского» в соответствии с установленными законом требованиями. «Лаборатория Касперского» использует полученную информацию только в виде общей статистики. Данные общей статистики формируются автоматически из исходной полученной информации и не содержат персональных данных и иной конфиденциальной информации. Исходная полученная информация хранится в зашифрованном виде и уничтожается по мере накопления (два раза в год). Данные общей статистики хранятся бессрочно.

РЕШЕНИЕ ТИПОВЫХ ЗАДАЧ

Этот раздел содержит пошаговые инструкции для выполнения основных задач пользователя, которые решает программа.

В ЭТОМ РАЗДЕЛЕ

Активация программы	27
Приобретение лицензии и продление срока ее действия.....	28
Работа с уведомлениями программы	28
Анализ состояния защиты компьютера и устранение проблем безопасности	29
Обновление баз и модулей программы.....	30
Проверка важных областей компьютера на вирусы	30
Полная проверка компьютера на вирусы	30
Проверка на вирусы файла, папки, диска или другого объекта	31
Проверка возможно зараженных объектов	32
Восстановление удаленного или вылеченного программой объекта	32
Восстановление операционной системы после заражения.....	33
Проверка почты и фильтрация вложений в почтовых сообщениях	35
Проверка компьютера на уязвимости	36
Проверка репутации программы	36
Защита личных данных от кражи	37
Определение безопасности веб-сайта	44
Использование Игрового профиля для работы в полноэкранном режиме.....	45
Создание и использование диска аварийного восстановления	45
Защита доступа к параметрам Антивируса Касперского с помощью пароля.....	48
Приостановка и возобновление защиты компьютера	49
Просмотр отчета о работе программы	50
Восстановление стандартных параметров работы программы.....	50
Импорт параметров программы в Антивирус Касперского, установленный на другом компьютере	52
Использование Kaspersky Gadget	53
Участие в Kaspersky Security Network (KSN)	54
Переход с Антивируса Касперского к использованию Kaspersky Internet Security	55

АКТИВАЦИЯ ПРОГРАММЫ

Для того, чтобы пользоваться функциями программы и связанными с программой дополнительными услугами, нужно активировать программу.

Если вы не активировали программу во время установки, вы можете сделать это позже. О необходимости активировать программу вам будут напоминать уведомления Антивируса Касперского, появляющиеся в области уведомлений панели задач. Активация Антивируса Касперского выполняется с помощью мастера активации.

➤ *Чтобы запустить мастер активации Антивируса Касперского, выполните одно из следующих действий:*

- Перейдите по ссылке **Активировать** в окне уведомления Антивируса Касперского, появляющегося в области уведомлений панели задач.
- Перейдите по ссылке **Введите код активации**, расположенной в нижней части главного окна программы. В открывшемся окне **Лицензирование** нажмите на кнопку **Активировать программу**.

Во время работы мастера активации программы требуется указать ряд параметров.

Шаг 1. Ввод кода активации

Введите код активации (см. раздел «О коде активации» на стр. 24) в соответствующее поле и нажмите на кнопку **Далее**.

Шаг 2. Запрос на активацию

При успешном выполнении запроса на активацию мастер автоматически переходит к следующему шагу.

Шаг 3. Ввод регистрационных данных

Зарегистрированные пользователи получают следующие возможности:

- отправлять запросы в Службу технической поддержки и Вирусную Лабораторию через Личный кабинет на веб-сайте «Лаборатории Касперского»;
- управлять кодами активации;
- получать информацию о новых продуктах и специальных предложениях «Лаборатории Касперского».

Укажите ваши данные для регистрации, затем нажмите на кнопку **Далее**.

Шаг 4. Активация

Если активация программы прошла успешно, мастер автоматически переходит к следующему окну.

Шаг 5. Завершение работы мастера

В этом окне мастера отображается информация о результатах активации.

Нажмите на кнопку **Завершить**, чтобы завершить работу мастера.

ПРИБРЕТЕНИЕ ЛИЦЕНЗИИ И ПРОДЛЕНИЕ СРОКА ЕЕ ДЕЙСТВИЯ

Если вы установили Антивирус Касперского, не имея лицензии, вы можете приобрести лицензию после установки программы. При приобретении лицензии вы получите код активации, с помощью которого нужно активировать программу (см. раздел «Активация программы» на стр. [27](#)).

Когда срок действия лицензии подходит к концу, вы можете его продлить. Для этого вы можете добавить в программу резервный код активации, не дожидаясь истечения срока действия лицензии. По истечении срока действия лицензии Антивирус Касперского будет автоматически активирован с помощью резервного кода активации.

➔ *Чтобы приобрести лицензию, выполните следующие действия:*

1. Откройте главное окно программы.
2. По ссылке **Введите код активации / Лицензирование**, расположенной в нижней части главного окна, откройте окно **Лицензирование**.
3. В открывшемся окне нажмите на кнопку **Купить код активации**.

Откроется веб-страница интернет-магазина, где вы можете приобрести лицензию.

➔ *Чтобы добавить резервный код активации, выполните следующие действия:*

1. Откройте главное окно программы.
2. По ссылке **Введите код активации / Лицензирование**, расположенной в нижней части главного окна, откройте окно **Лицензирование**.
3. В открывшемся окне нажмите на кнопку **Ввести код активации**.

Откроется окно мастера активации программы.

4. Введите код активации в соответствующие поля и нажмите на кнопку **Далее**.

Антивирус Касперского отправит данные на сервер активации для проверки. Если проверка завершится успешно, мастер активации автоматически перейдет на следующий шаг.

5. По завершении работы мастера нажмите на кнопку **Завершить**.

РАБОТА С УВЕДОМЛЕНИЯМИ ПРОГРАММЫ

Уведомления программы, появляющиеся в области уведомлений панели задач, информируют о событиях, происходящих в процессе работы программы и требующих вашего внимания. В зависимости от степени важности события уведомления могут быть следующих типов:

- *Критические* – информируют о событиях, имеющих первостепенную важность для обеспечения безопасности компьютера (например, об обнаружении вредоносного объекта или опасной активности в системе). Окна критических уведомлений и всплывающих сообщений – красные.
- *Важные* – информируют о событиях, потенциально важных для обеспечения безопасности компьютера (например, об обнаружении возможно зараженного объекта или подозрительной активности в системе). Окна важных уведомлений и всплывающих сообщений – желтые.
- *Информационные* – информируют о событиях, не имеющих первостепенной важности для обеспечения безопасности компьютера. Окна информационных уведомлений и всплывающих сообщений – зеленые.

При появлении на экране уведомления следует выбрать один из предложенных в уведомлении вариантов действия. Оптимальный вариант – тот, который рекомендован экспертами «Лаборатории Касперского» по умолчанию.

АНАЛИЗ СОСТОЯНИЯ ЗАЩИТЫ КОМПЬЮТЕРА И УСТРАНЕНИЕ ПРОБЛЕМ БЕЗОПАСНОСТИ

О появлении проблем в защите компьютера сигнализирует индикатор, расположенный в левой части главного окна программы (см. рис. ниже). Индикатор представляет собой изображение монитора, которое меняет цвет в зависимости от состояния защиты компьютера: зеленый цвет означает, что компьютер защищен, желтый цвет свидетельствует о наличии проблем в защите, красный – о серьезной угрозе безопасности компьютера. Проблемы и угрозы безопасности рекомендуется немедленно устранять.



Рисунок 1. Индикатор состояния защиты

Нажав на индикатор в главном окне программы, вы можете открыть окно **Проблемы безопасности** (см. рис. ниже), в котором приведена подробная информация о состоянии защиты компьютера и предложены варианты действий для устранения проблем и угроз.

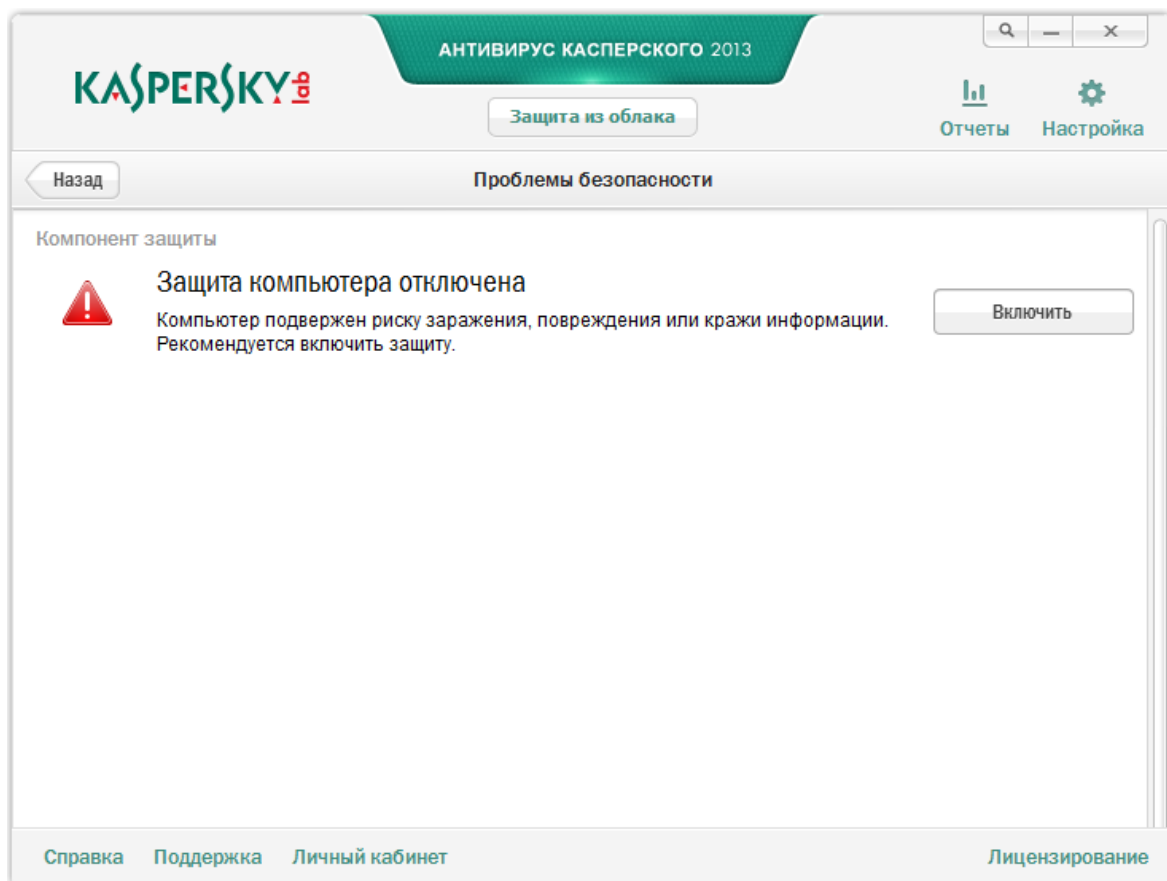


Рисунок 2. Окно **Проблемы безопасности**

Проблемы в защите сгруппированы по категориям, к которым они относятся. Для каждой проблемы приведены действия, которые вы можете предпринять, чтобы решить проблему.

ОБНОВЛЕНИЕ БАЗ И МОДУЛЕЙ ПРОГРАММЫ

По умолчанию Антивирус Касперского автоматически проверяет наличие обновлений на серверах обновлений «Лаборатории Касперского». Если на сервере содержится набор последних обновлений, Антивирус Касперского загружает и устанавливает их в фоновом режиме. Вы можете в любой момент запустить обновление Антивируса Касперского вручную из главного окна программы или из контекстного меню значка программы в области уведомлений панели задач.

Для загрузки обновлений с серверов «Лаборатории Касперского» требуется соединение с интернетом.

➤ *Чтобы запустить обновление из контекстного меню значка программы в области уведомлений панели задач,*

в контекстном меню значка программы выберите пункт **Обновление**.

➤ *Чтобы запустить обновление из главного окна программы, выполните следующие действия:*


1. Откройте главное окно программы и в нижней части окна выберите раздел **Обновление**.
2. В открывшемся окне **Обновление** нажмите на кнопку **Обновить**.

ПРОВЕРКА ВАЖНЫХ ОБЛАСТЕЙ КОМПЬЮТЕРА НА ВИРУСЫ

Под проверкой важных областей подразумевается проверка следующих объектов:

- объектов, которые загружаются при запуске операционной системы;
- системной памяти;
- загрузочных секторов диска.

➤ *Чтобы запустить проверку из главного окна программы, выполните следующие действия:*

1. Откройте главное окно программы и в нижней части окна выберите раздел **Проверка**.
2. В открывшемся окне **Проверка** в блоке **Проверка важных областей** нажмите на кнопку .

ПОЛНАЯ ПРОВЕРКА КОМПЬЮТЕРА НА ВИРУСЫ

Во время полной проверки по умолчанию Антивирус Касперского проверяет следующие объекты:

- системную память;
- объекты, которые загружаются при старте операционной системы;
- резервное хранилище системы;
- жесткие и съемные диски.

Рекомендуется выполнить полную проверку сразу после установки Антивируса Касперского на компьютер.

➔ Чтобы запустить полную проверку из главного окна программы, выполните следующие действия:

1. Откройте главное окно программы и в нижней части окна выберите раздел **Проверка**.

2. В открывшемся окне **Проверка** в блоке **Полная проверка** нажмите на кнопку



ПРОВЕРКА НА ВИРУСЫ ФАЙЛА, ПАПКИ, ДИСКА ИЛИ ДРУГОГО ОБЪЕКТА

Проверить на вирусы отдельный объект вы можете следующими способами:

- из контекстного меню объекта;
- из главного окна программы;
- с помощью гаджета (см. раздел «Использование Kaspersky Gadget» на стр. 53) Антивируса Касперского (только для операционных систем Microsoft Windows Vista и Microsoft Windows 7).

➔ Чтобы запустить проверку на вирусы из контекстного меню объекта, выполните следующие действия:

1. Откройте окно Проводника Microsoft Windows и перейдите в папку с объектом, который нужно проверить.
2. По правой клавише мыши откройте контекстное меню объекта (см. рисунок ниже) и выберите пункт **Проверить на вирусы**.

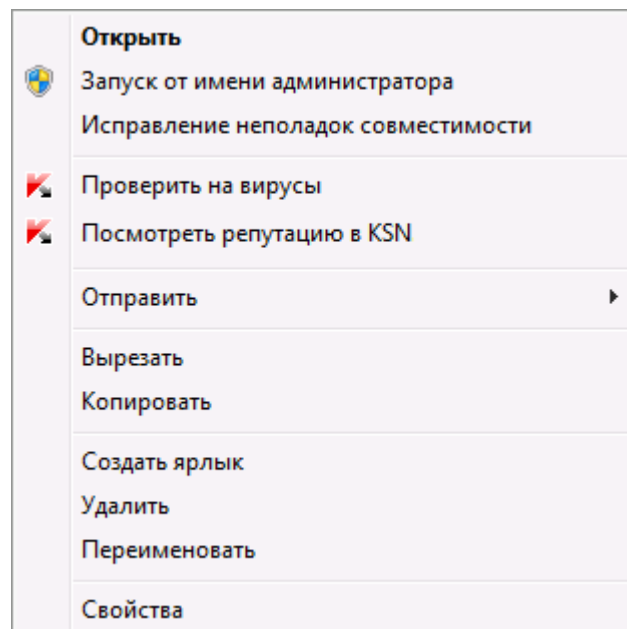


Рисунок 3. Контекстное меню объекта в Microsoft Windows

➤ *Чтобы запустить проверку объекта на вирусы из главного окна программы, выполните следующие действия:*

1. Откройте главное окно программы и в нижней части окна выберите раздел **Проверка**.
2. По ссылке **Укажите**, расположенной в нижней правой части окна, откройте окно **Выборочная проверка** и установите флажки напротив папок и дисков, которые нужно проверить.

Если в окне отсутствует объект, который требуется проверить, выполните следующие действия:

- a. Нажмите на кнопку **Добавить**.
- b. В открывшемся окне **Выбор объекта для проверки** выберите объект для проверки.

➤ *Чтобы проверить объект на вирусы с помощью гаджета,*

перетащите объект проверки на гаджет.

ПРОВЕРКА ВОЗМОЖНО ЗАРАЖЕННЫХ ОБЪЕКТОВ

Если вы подозреваете, что объект может быть заражен, проверьте его с помощью Антивируса Касперского (см. раздел «Проверка на вирусы файла, папки, диска или другого объекта» на стр. [31](#)).

Если после проверки программа сообщит, что объект не заражен, но вы подозреваете обратное, вы можете отправить объект в *Вирусную лабораторию*. Специалисты Вирусной лаборатории проверят объект и, если он действительно заражен вирусом, внесут описание нового вируса в базы, которые будут загружены программой во время обновления (см. раздел «Обновление баз и модулей программы» на стр. [30](#)).

➤ *Чтобы отправить файл в Вирусную лабораторию, выполните следующие действия:*

1. Перейдите на страницу отправки запроса в Вирусную лабораторию (<http://support.kaspersky.ru/virlab/helpdesk.html>).
2. Следуйте инструкциям, приведенным на странице, чтобы отправить запрос.

ВОССТАНОВЛЕНИЕ УДАЛЕННОГО ИЛИ ВЫЛЕЧЕННОГО ПРОГРАММОЙ ОБЪЕКТА

«Лаборатория Касперского» не рекомендует восстанавливать удаленные и вылеченные объекты, поскольку они могут представлять угрозу для вашего компьютера.

Для восстановления удаленного или вылеченного объекта используется его резервная копия, созданная программой в ходе проверки объекта.

➤ *Чтобы восстановить удаленный или вылеченный программой файл, выполните следующие действия:*

1. Откройте главное окно программы.
2. В нижней части окна выберите раздел **Карантин**.

3. В открывшемся окне **Карантин** выберите нужный файл в списке и нажмите на кнопку **Восстановить** (см. рис. ниже).

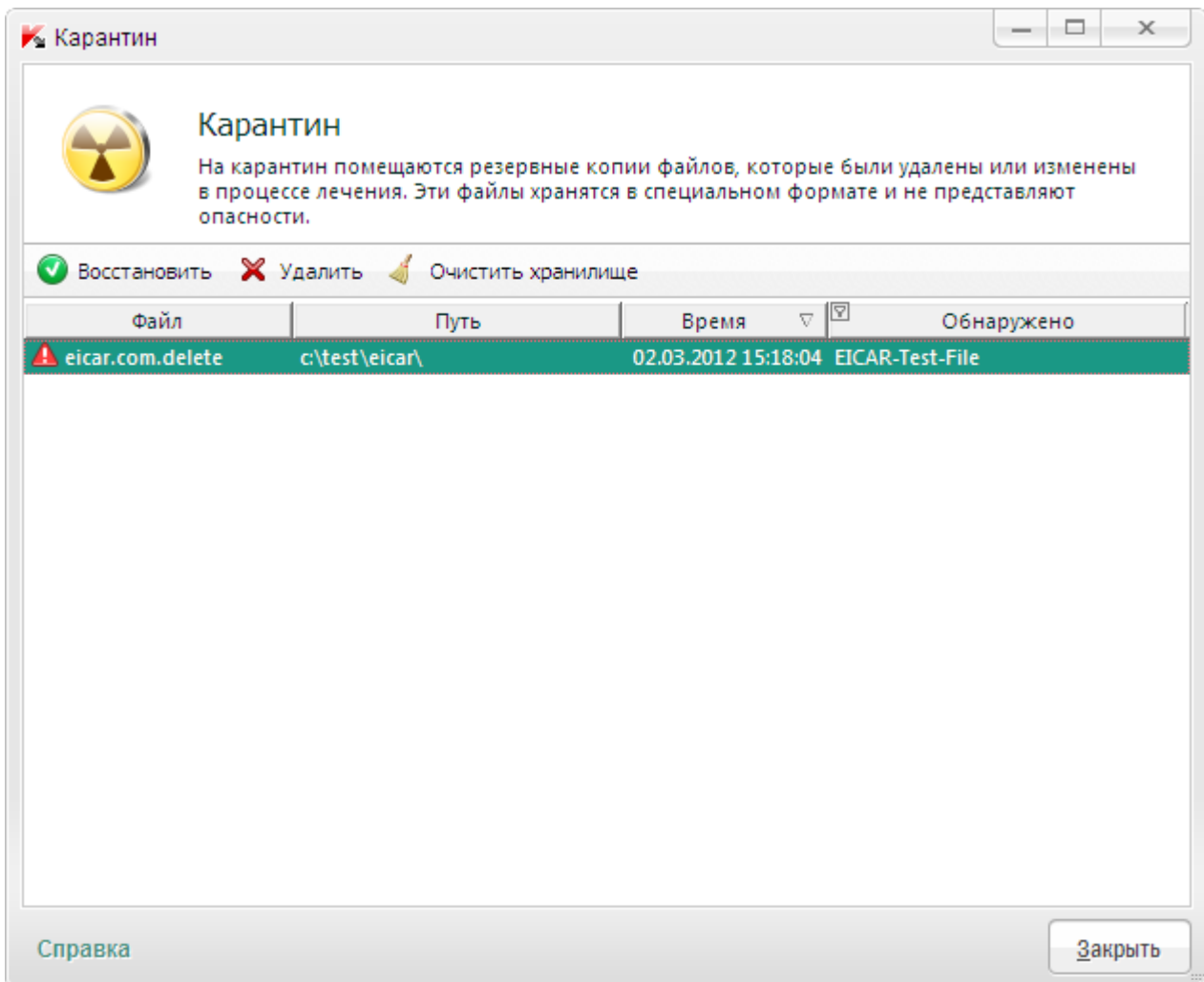


Рисунок 4. Окно **Карантин**

ВОССТАНОВЛЕНИЕ ОПЕРАЦИОННОЙ СИСТЕМЫ ПОСЛЕ ЗАРАЖЕНИЯ

Если вы подозреваете, что операционная система вашего компьютера была повреждена или изменена в результате действий вредоносных программ или системного сбоя, используйте *мастер восстановления после заражения*, устраняющий следы пребывания в системе вредоносных объектов. Специалисты «Лаборатории Касперского» рекомендуют также запускать мастер после лечения компьютера, чтобы убедиться, что все возникшие угрозы и повреждения устранены.

В ходе работы мастер проверяет наличие в системе каких-либо изменений, к числу которых могут относиться блокировка доступа к сетевому окружению, изменение расширений файлов известных форматов, блокировка панели управления и тому подобное. Причины появления таких повреждений различны. Это могут быть активность вредоносных программ, неправильная настройка системы, системные сбои или применение неправильно работающих программ – оптимизаторов системы.

После исследования мастер анализирует собранную информацию с целью выявления в системе повреждений, которые требуют немедленного вмешательства. По результатам исследования составляется список действий, которые следует выполнить, чтобы устранить повреждения. Мастер группирует действия по категориям с учетом серьезности обнаруженных проблем.

➡ Чтобы запустить мастер восстановления после заражения, выполните следующие действия:

1. Откройте главное окно программы.
2. В нижней части окна выберите раздел **Инструменты**.
3. В открывшемся окне в блоке **Восстановление после заражения** нажмите на кнопку **Выполнить**.

Откроется окно мастера восстановления после заражения.

Мастер состоит из последовательности окон (шагов), переключение между которыми осуществляется нажатием на кнопки **Назад** и **Далее**. Работа мастера завершается нажатием на кнопку **Завершить**. Для прекращения работы мастера на любом этапе следует нажать на кнопку **Отмена**.

Рассмотрим подробнее шаги мастера.

Шаг 1. Запуск восстановления системы

Убедитесь, что в окне мастера выбран вариант **Выполнить поиск проблем, связанных с активностью вредоносного ПО**, и нажмите на кнопку **Далее**.

Шаг 2. Поиск проблем

Мастер выполняет поиск проблем и возможных повреждений, которые следует исправить. По завершении поиска мастер автоматически переходит к следующему шагу.

Шаг 3. Выбор действий для устранения проблем

Все найденные на предыдущем шаге повреждения группируются с точки зрения опасности, которую они представляют. Для каждой группы повреждений специалисты «Лаборатории Касперского» предлагают набор действий, выполнение которых поможет устранить повреждения. Всего выделено три группы действий:

- *Настоятельно рекомендуемые действия* помогут избавиться от повреждений, представляющих серьезную проблему. Рекомендуем вам выполнить все действия этой группы.
- *Рекомендуемые действия* направлены на устранение повреждений, которые могут представлять потенциальную опасность. Действия этой группы также рекомендуется выполнять.
- *Дополнительные действия* предназначены для устранения неопасных в данный момент повреждений системы, которые в дальнейшем могут поставить безопасность компьютера под угрозу.

Для просмотра действий, включенных в группу, нажмите на значок **+**, расположенный слева от названия группы.

Чтобы мастер выполнил какое-либо действие, установите флажок слева от названия действия. По умолчанию выполняются все рекомендуемые и настоятельно рекомендуемые действия. Если вы не хотите выполнять какое-либо действие, снимите флажок рядом с ним.

Настоятельно не рекомендуется снимать флажки, установленные по умолчанию, поскольку в результате этого действия безопасность вашего компьютера останется под угрозой.

Сформировав набор действий для выполнения мастером, нажмите на кнопку **Далее**.

Шаг 4. Устранение проблем

Мастер выполняет действия, выбранные на предыдущем шаге. Устранение проблем может занять некоторое время. По завершении устранения проблем мастер автоматически перейдет к следующему шагу.

Шаг 5. Завершение работы мастера

Нажмите на кнопку **Завершить**, чтобы завершить работу мастера.

ПРОВЕРКА ПОЧТЫ И ФИЛЬТРАЦИЯ ВЛОЖЕНИЙ В ПОЧТОВЫХ СООБЩЕНИЯХ

Антивирус Касперского позволяет проверять сообщения электронной почты на наличие в них опасных объектов с помощью Почтового Антивируса. Почтовый Антивирус запускается при старте операционной системы, постоянно находится в оперативной памяти компьютера и проверяет почтовые сообщения, получаемые или отправляемые по протоколам POP3, SMTP, IMAP, MAPI и NNTP (в том числе через защищенные соединения (SSL) по протоколам POP3, SMTP и IMAP).

По умолчанию Почтовый Антивирус проверяет как входящие, так и исходящие сообщения. При необходимости вы можете включить проверку только входящих сообщений.

➤ *Чтобы проверять только входящие сообщения, выполните следующие действия:*

1. Откройте главное окно программы.
2. В верхней части окна перейдите по ссылке **Настройка**.
3. В левой части окна выберите в разделе **Центр защиты** компонент **Почтовый Антивирус**.
4. В правой части окна нажмите на кнопку **Настройка**.

Откроется окно **Почтовый Антивирус**.

5. В открывшемся окне на закладке **Общие** в блоке **Область защиты** выберите вариант **Только входящие сообщения**.

Если угрозы в почтовом сообщении не обнаружены или зараженные объекты были успешно вылечены, почтовое сообщение становится доступным для работы. Если зараженный объект вылечить не удалось, Почтовый Антивирус переименовывает или удаляет объект из сообщения и помещает в тему сообщения уведомление о том, что оно обработано Антивирусом Касперского. В случае удаления объекта Антивирус Касперского создает его резервную копию и помещает на карантин (см. раздел «Восстановление удаленного или вылеченного программой объекта» на стр. [32](#)).

Вредоносные программы могут распространяться в виде вложений в почтовые сообщения. Вы можете включить фильтрацию вложений в почтовых сообщениях. Фильтрация позволяет автоматически переименовывать или удалять вложенные файлы указанных вами типов.

➤ *Чтобы включить фильтрацию вложений в почтовых сообщениях, выполните следующие действия:*

1. Откройте главное окно программы.
2. В верхней части окна перейдите по ссылке **Настройка**.
3. В левой части окна выберите в разделе **Центр защиты** компонент **Почтовый Антивирус**.
4. В правой части окна нажмите на кнопку **Настройка**.

Откроется окно **Почтовый Антивирус**.

5. В открывшемся окне на закладке **Фильтр вложений** выберите режим фильтрации вложений (**Переименовывать вложения указанных типов** или **Удалять вложения указанных типов**).
6. В списке типов файлов (расширений) выберите типы вложений, которые нужно фильтровать.
Если вы хотите добавить маску нового типа файлов, выполните следующие действия:
 - a. По ссылке **Добавить** в нижней части окна откройте окно **Маска имени файла**.
 - b. В открывшемся окне введите нужную маску типа файлов.
7. В окне **Настройка** нажмите на кнопку **Применить**.

ПРОВЕРКА КОМПЬЮТЕРА НА УЯЗВИМОСТИ

Уязвимости – это незащищенные места программного кода, которые злоумышленники могут использовать в своих целях: например, копировать данные, используемые программами с незащищенным кодом. Проверка вашего компьютера на наличие потенциальных уязвимостей позволяет найти такие «слабые места» в защите компьютера. Найденные уязвимости рекомендуется устранить.

➔ Чтобы запустить поиск уязвимостей из главного окна программы, выполните следующие действия:

1. Откройте главное окно программы и в нижней части окна выберите раздел **Проверка**.

2. В открывшемся окне **Проверка** в блоке **Поиск уязвимостей** нажмите на кнопку  .

ПРОВЕРКА РЕПУТАЦИИ ПРОГРАММЫ

Антивирус Касперского позволяет проверять репутацию программ у пользователей во всем мире. В состав репутации программы входят следующие показатели:

- название производителя;
- информация о цифровой подписи (доступно при наличии цифровой подписи);
- информация о группе, в которую программа помещена большинством пользователей Kaspersky Security Network;
- количество пользователей Kaspersky Security Network, использующих программу (доступно, если программа отнесена к группе Доверенные в базе Kaspersky Security Network);
- время, когда программа стала известна в Kaspersky Security Network;
- страны, в которых программа наиболее распространена.

Проверка репутации программ доступна, если вы согласились участвовать в Kaspersky Security Network.

- ➔ Чтобы узнать репутацию программы,

откройте контекстное меню исполняемого файла программы и выберите пункт **Посмотреть репутацию в KSN** (см. рис. ниже).

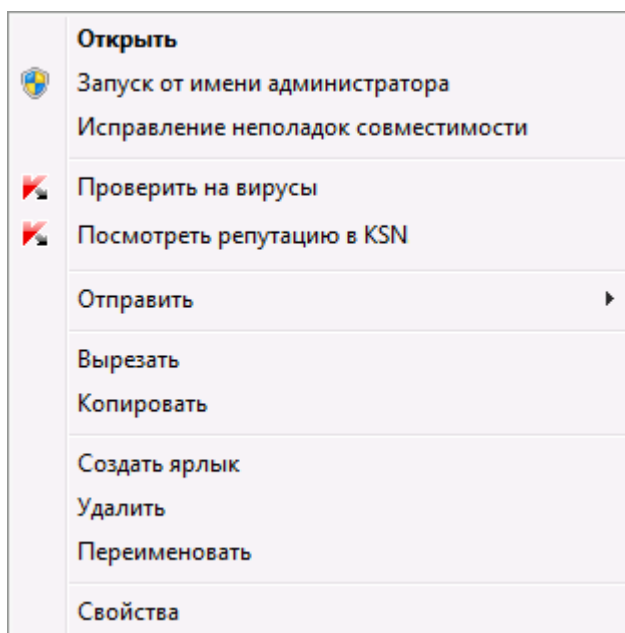


Рисунок 5. Контекстное меню объекта в Microsoft Windows

Откроется окно со сведениями о репутации программы в KSN.

СМ. ТАКЖЕ

Участие в Kaspersky Security Network (KSN) [54](#)

ЗАЩИТА ЛИЧНЫХ ДАННЫХ ОТ КРАЖИ

С помощью Антивируса Касперского вы можете защитить от кражи свои личные данные:

- пароли, имена пользователя и другие регистрационные данные;
- номера счетов и кредитных карт.

В состав Антивируса Касперского входят компоненты и инструменты, позволяющие защитить ваши личные данные от кражи злоумышленниками, использующими такие методы как фишинг и перехват данных, вводимых с клавиатуры.

Для защиты от фишинга предназначен Анти-Фишинг, включенный в состав компонентов Веб-Антивирус и IM-Антивирус.

Для защиты от перехвата данных с клавиатуры предназначены виртуальная клавиатура и защита ввода данных с аппаратной клавиатуры.

Для удаления информации о действиях пользователя на компьютере предназначен мастер устранения следов активности.

В ЭТОМ РАЗДЕЛЕ

Защита от фишинга.....	38
Виртуальная клавиатура.....	39
Защита ввода данных с аппаратной клавиатуры	41
Устранение следов активности	42

ЗАЩИТА ОТ ФИШИНГА

Для защиты от фишинга предназначен Анти-Фишинг, включенный в состав компонентов Веб-Антивирус и IM-Антивирус. Включите эти компоненты, чтобы обеспечить максимально эффективную защиту от фишинга.

Вы можете настроить дополнительные параметры защиты от фишинга при работе компонентов Веб-Антивирус и IM-Антивирус.

➤ *Чтобы настроить защиту от фишинга при работе Веб-Антивируса, выполните следующие действия:*

1. Откройте главное окно программы.
2. В верхней части окна перейдите по ссылке **Настройка**.
3. В открывшемся окне **Настройка** в разделе **Центр защиты** выберите подраздел **Веб-Антивирус** и нажмите на кнопку **Настройка**.

Откроется окно **Веб-Антивирус**.

4. В открывшемся окне на закладке **Общие** в блоке **Проверка ссылок** установите флажок **Проверять веб-страницы на наличие фишинга**.
5. Если вы хотите, чтобы Анти-Фишинг использовал эвристический анализ при проверке веб-страниц, нажмите на кнопку **Дополнительно**.

Откроется окно **Настройка Анти-Фишинга**.

6. В открывшемся окне установите флажок **Использовать эвристический анализ для проверки веб-страниц на наличие фишинга** и задайте уровень детализации проверки.
7. В окне **Настройка** нажмите на кнопку **Применить**.

➤ *Чтобы настроить защиту от фишинга при работе IM-Антивируса, выполните следующие действия:*

1. Откройте главное окно программы.
2. В верхней части окна перейдите по ссылке **Настройка**.
3. В открывшемся окне **Настройка** в разделе **Центр защиты** выберите подраздел **IM-Антивирус**.
4. В правой части окна в блоке **Методы проверки** установите флажок **Проверять ссылки по базе фишинговых веб-адресов**.
5. В окне **Настройка** нажмите на кнопку **Применить**.

ВИРТУАЛЬНАЯ КЛАВИАТУРА

При работе в интернете часто возникают ситуации, когда необходимо указать персональные данные, а также имя пользователя и пароль. Это происходит, например, при регистрации на веб-сайтах, совершении покупок в интернет-магазинах, использовании интернет-банкинга.

В таких случаях существует опасность перехвата персональной информации с помощью аппаратных перехватчиков или клавиатурных перехватчиков – программ, регистрирующих нажатие клавиш.

Виртуальная клавиатура позволяет избежать перехвата данных, вводимых с клавиатуры.

Виртуальная клавиатура защищает от перехвата персональной информации только при работе с интернет-браузерами Microsoft Internet Explorer, Mozilla™ Firefox™ и Google Chrome™. При работе с другими интернет-браузерами виртуальная клавиатура не защищает вводимые персональные данные от перехвата.

Виртуальная клавиатура не может защитить ваши персональные данные в случае взлома веб-сайта, требующего ввода таких данных, поскольку в этом случае информация попадет непосредственно в руки злоумышленников.

Многие программы-шпионы обладают функциями снятия снимков экрана, которые автоматически передаются злоумышленнику для последующего анализа и извлечения персональных данных пользователя. Виртуальная клавиатура защищает вводимые персональные данные от перехвата посредством снятия снимков экрана.

Виртуальная клавиатура не предотвращает снятие снимков экрана с помощью нажатия клавиши Print Screen и других комбинаций клавиш, заданных в параметрах операционной системы, а также снятие снимков экрана с помощью технологии DirectX.

Виртуальная клавиатура имеет следующие особенности:

- На клавиши виртуальной клавиатуры нужно нажимать с помощью мыши.
- В отличие от настоящей клавиатуры, на виртуальной клавиатуре невозможно одновременно нажать несколько клавиш. Поэтому, чтобы использовать комбинации клавиш (например, **ALT+F4**), нужно сначала нажать на первую клавишу (например, **ALT**), затем на следующую (например, **F4**), а затем повторно нажать на первую клавишу. Повторное нажатие заменяет отпускание клавиши на настоящей клавиатуре.
- На виртуальной клавиатуре язык ввода переключается с помощью того же сочетания клавиш, которое установлено в параметрах операционной системы для обычной клавиатуры. При этом на вторую клавишу нужно нажимать правой клавишей мыши (например, если в параметрах операционной системы для переключения языка ввода задана комбинация **LEFT ALT+SHIFT**, то на клавишу **LEFT ALT** нужно нажимать левой клавишей мыши, а на клавишу **SHIFT** нужно нажимать правой клавишей мыши).

Для защиты данных, вводимых с помощью виртуальной клавиатуры, после установки Антивируса Касперского необходимо перезагрузить компьютер.

Открыть виртуальную клавиатуру можно следующими способами:

- из контекстного меню значка программы в области уведомлений;
- из главного окна программы;
- из окна браузера Microsoft Internet Explorer, Mozilla Firefox или Google Chrome;
- с помощью значка быстрого вызова виртуальной клавиатуры в поле ввода на веб-сайтах;

Отображение значка быстрого вызова в полях ввода на веб-сайтах можно настроить.

- с помощью комбинации клавиш аппаратной клавиатуры;
- с помощью гаджета Антивирус Касперского (только для операционных систем Microsoft Windows Vista и Microsoft Windows 7).

➔ Чтобы открыть виртуальную клавиатуру из контекстного меню значка программы в области уведомлений,

выберите пункт **Виртуальная клавиатура** в контекстном меню значка программы (см. рис. ниже).

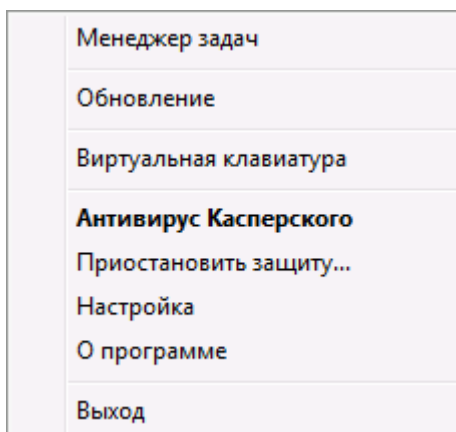



Рисунок 6. Контекстное меню значка программы

➔ Чтобы открыть виртуальную клавиатуру из главного окна программы,

в нижней части главного окна программы выберите раздел **Виртуальная клавиатура**.

➔ Чтобы открыть виртуальную клавиатуру из окна браузера,

нажмите на кнопку  **Виртуальная клавиатура** в панели инструментов браузера Microsoft Internet Explorer, Mozilla Firefox или Google Chrome.

➔ Чтобы открыть виртуальную клавиатуру с помощью аппаратной клавиатуры,

нажмите комбинацию клавиш **CTRL+ALT+SHIFT+P**.

➔ Чтобы открыть виртуальную клавиатуру с помощью гаджета,

нажмите на кнопку гаджета, для которой назначено это действие (см. раздел «Использование Kaspersky Gadget» на стр. 53).

➔ Чтобы настроить отображение значка быстрого вызова виртуальной клавиатуры в полях ввода на веб-сайтах, выполните следующие действия:

1. Откройте главное окно программы.
2. В верхней части окна перейдите по ссылке **Настройка**.
3. В открывшемся окне **Настройка** в разделе **Центр защиты** выберите подраздел **Безопасный ввод данных**.
4. В правой части окна в блоке **Виртуальная клавиатура** установите флажок **Показывать значок быстрого вызова в полях ввода** и нажмите на кнопку **Настройка**.

Откроется окно **Виртуальная клавиатура**.

5. В открывшемся окне задайте правила отображения значка быстрого вызова:
- На закладке **Категории** установите флажки для категорий веб-сайтов, на которых нужно отображать значок быстрого вызова в полях ввода.
 - Если вы хотите, чтобы значок быстрого вызова отображался в полях ввода на тех веб-сайтах, которые открываются в защищенном браузере при работе в режиме Безопасных платежей, на закладке **Категории** установите флажок **Показывать значок быстрого вызова в полях ввода Безопасных платежей**.
 - Если вы хотите включить отображение значка быстрого вызова в полях ввода на определенном веб-сайте, выполните следующие действия:
 - a. На закладке **Исключения** в списке **Показывать значок быстрого вызова на веб-сайтах** нажмите на кнопку **Добавить**.

Откроется окно **Показывать значок быстрого вызова**.
 - b. В открывшемся окне введите адрес веб-сайта в поле **Веб-адрес** и выберите один из вариантов отображения значка быстрого вызова на этом веб-сайте (**Показывать значок только на указанной веб-странице** или **Показывать значок на всем веб-сайте**).
6. В окне **Настройка** нажмите на кнопку **Применить**.

ЗАЩИТА ВВОДА ДАННЫХ С АППАРАТНОЙ КЛАВИАТУРЫ

При работе в интернете часто возникают ситуации, когда необходимо указать персональные данные, а также имя пользователя и пароль. Это происходит, например, при регистрации на веб-сайтах, совершении покупок в интернет-магазинах, использовании интернет-банкинга.

В таких случаях существует опасность перехвата персональной информации с помощью аппаратных перехватчиков или клавиатурных перехватчиков – программ, регистрирующих нажатие клавиш.

Защита ввода данных с аппаратной клавиатуры позволяет избежать перехвата данных, вводимых с клавиатуры.

Защита ввода данных с аппаратной клавиатуры работает только в интернет-браузерах Microsoft Internet Explorer, Mozilla Firefox и Google Chrome. При работе с другими интернет-браузерами данные, вводимые с аппаратной клавиатуры, не защищаются от перехвата.

Защита ввода данных с аппаратной клавиатуры не может защитить ваши персональные данные в случае взлома веб-сайта, требующего ввода таких данных, поскольку в этом случае информация попадет непосредственно в руки злоумышленников.

Вы можете настроить защиту ввода данных с клавиатуры на разных веб-сайтах. После того как защита ввода данных с клавиатуры настроена, не требуется выполнять дополнительные действия при вводе данных.

Для защиты ввода данных с аппаратной клавиатуры после установки Антивируса Касперского необходимо перезагрузить компьютер.

➡ *Чтобы настроить защиту ввода данных с клавиатуры, выполните следующие действия:*

1. Откройте главное окно программы.
2. В верхней части окна перейдите по ссылке **Настройка**.
3. В открывшемся окне **Настройка** в разделе **Центр защиты** выберите подраздел **Безопасный ввод данных**.

4. В правой части окна в блоке **Защита ввода данных с аппаратной клавиатуры** установите флажок **Защищать ввод данных с аппаратной клавиатуры** и нажмите на кнопку **Настройка**.

Откроется окно **Защита ввода с клавиатуры**.

5. В открывшемся окне задайте область защиты ввода данных с аппаратной клавиатуры:
 - На закладке **Категории** установите флажки для категорий веб-сайтов, на которых нужно защищать данные, вводимые с клавиатуры.
 - Если вы хотите, чтобы ввод данных с клавиатуры был защищен на тех веб-сайтах, которые открываются в защищенном браузере в режиме Безопасных платежей, на закладке **Категории** установите флажок **Защищать ввод данных с клавиатуры для Безопасных платежей**.
 - Если вы хотите, чтобы ввод данных с клавиатуры был защищен в полях для ввода паролей на всех веб-сайтах, на закладке **Категории** установите флажок **Защищать поля для ввода паролей на всех веб-сайтах**.
 - Если вы хотите включить защиту ввода данных с клавиатуры на определенном веб-сайте, выполните следующие действия:
 - a. На закладке **Исключения** в списке **Защищать ввод данных с клавиатуры на веб-сайтах** нажмите на кнопку **Добавить**.
Откроется окно **Защищаемый веб-сайт**.
 - b. В открывшемся окне введите адрес веб-сайта в поле **Веб-адрес** и выберите один из вариантов защиты ввода данных на этом веб-сайте (**Включить защиту только на указанной веб-странице** или **Включить защиту на всем веб-сайте**).
6. В окне **Настройка** нажмите на кнопку **Применить**.

УСТРАНЕНИЕ СЛЕДОВ АКТИВНОСТИ

При работе на компьютере действия пользователя регистрируются в операционной системе. При этом сохраняется следующая информация:

- данные о введенных пользователем поисковых запросах и посещенных веб-сайтах;
- сведения о запуске программ, открытии и сохранении файлов;
- записи в системном журнале Microsoft Windows;
- другая информация о действиях пользователя.

Сведения о действиях пользователя, содержащие конфиденциальную информацию, могут оказаться доступными злоумышленникам и посторонним лицам.

В состав Антивируса Касперского входит мастер устранения следов активности пользователя в системе.

➔ *Чтобы запустить мастер устранения следов активности, выполните следующие действия:*

1. Откройте главное окно программы.
2. В нижней части окна выберите раздел **Инструменты**.
3. В открывшемся окне в блоке **Устранение следов активности** нажмите на кнопку **Выполнить**.

Мастер состоит из последовательности окон (шагов), переключение между которыми осуществляется нажатием на кнопки **Назад** и **Далее**. Работа мастера завершается нажатием на кнопку **Завершить**. Для прекращения работы мастера на любом этапе следует нажать на кнопку **Отмена**.

Рассмотрим подробнее шаги мастера.

Шаг 1. Начало работы мастера

Убедитесь, что выбран вариант **Выполнить поиск следов активности пользователя**, и нажмите на кнопку **Далее**, чтобы начать работу мастера.

Шаг 2. Поиск следов активности

Мастер осуществляет поиск следов активности на вашем компьютере. Поиск может занять некоторое время. По завершении поиска мастер автоматически переходит к следующему шагу.

Шаг 3. Выбор действий для устранения следов активности

По завершении поиска мастер сообщает о найденных следах активности и предлагаемых действиях для их устранения (см. рис. ниже).

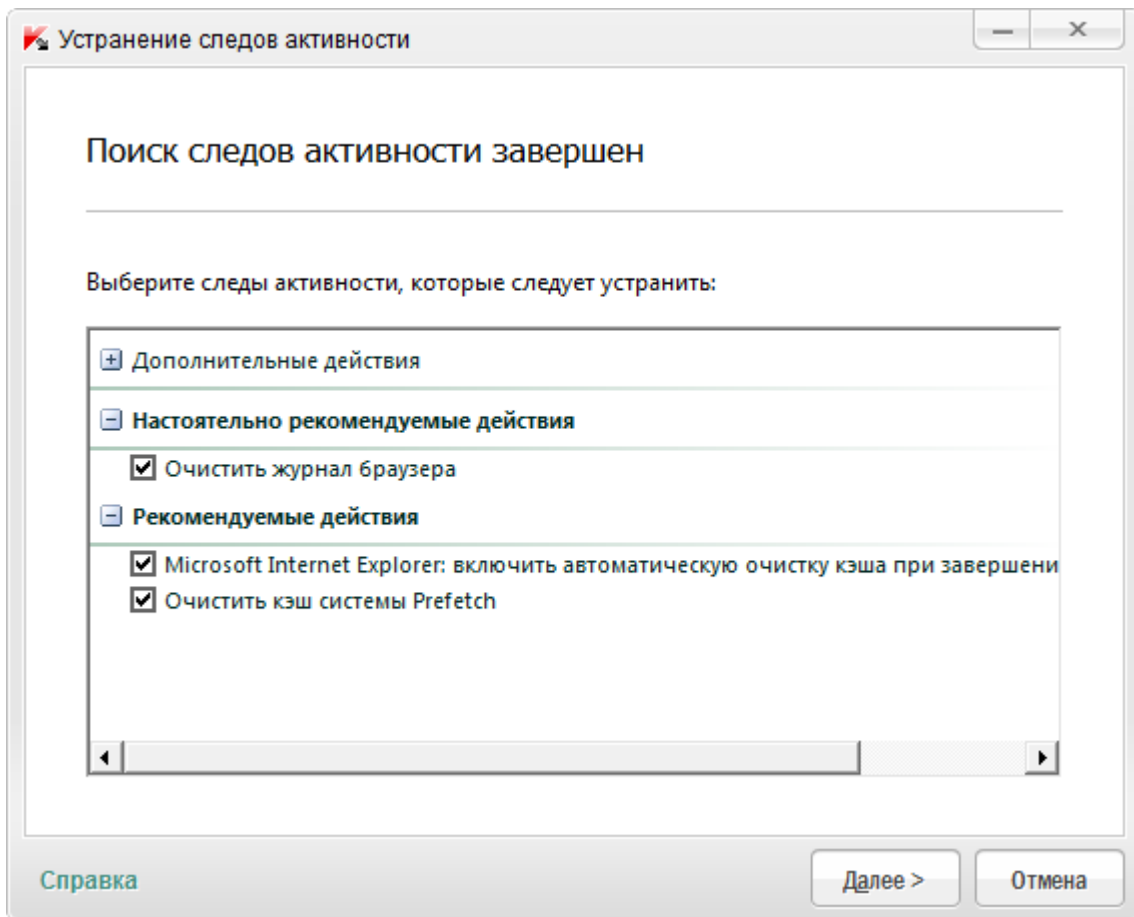


Рисунок 7. Найденные следы активности и рекомендации по их устранению

Для просмотра действий, включенных в группу, нажмите на значок **+**, расположенный слева от названия группы.

Чтобы мастер выполнил какое-либо действие, установите флажок слева от названия действия. По умолчанию выполняются все рекомендуемые и настоятельно рекомендуемые действия. Если вы не хотите выполнять какое-либо действие, снимите флажок рядом с ним.

Не рекомендуется снимать флажки, установленные по умолчанию. В результате этого действия безопасность вашего компьютера может оказаться под угрозой.

Сформировав набор действий для выполнения мастером, нажмите на кнопку **Далее**.

Шаг 4. Устранение следов активности

Мастер выполняет действия, выбранные на предыдущем шаге. Устранение следов активности может занять некоторое время. Для устранения некоторых следов активности может потребоваться перезагрузка компьютера, о чем мастер вас уведомит.

После устранения следов активности мастер автоматически перейдет к следующему шагу.

Шаг 5. Завершение работы мастера




Если вы хотите, чтобы устранение следов активности в дальнейшем выполнялось автоматически при завершении работы Антивируса Касперского, на завершающем шаге работы мастера установите флажок **Устранять следы активности при каждом завершении работы Антивируса Касперского**. Если вы планируете самостоятельно устранять следы активности с помощью мастера, не устанавливайте этот флажок.

Нажмите на кнопку **Завершить**, чтобы завершить работу мастера.

ОПРЕДЕЛЕНИЕ БЕЗОПАСНОСТИ ВЕБ-САЙТА

Антивирус Касперского позволяет проверить безопасность веб-сайта, прежде чем перейти по ссылке на этот веб-сайт. Для этого используется *модуль проверки ссылок*.

Модуль проверки ссылок встраивается в браузеры Microsoft Internet Explorer, Google Chrome и Mozilla Firefox и проверяет ссылки на открытой в браузере веб-странице. Рядом с каждой ссылкой Антивирус Касперского отображает один из следующих значков:

-  – если веб-страница, которая открывается по ссылке, безопасна по данным «Лаборатории Касперского»;
-  – если нет информации о безопасности веб-страницы, которая открывается по ссылке;
-  – если веб-страница, которая открывается по ссылке, опасна по данным «Лаборатории Касперского».

При наведении курсора мыши на значок отображается всплывающее окно с более подробным описанием ссылки.

По умолчанию Антивирус Касперского проверяет ссылки только в результатах поиска. Вы можете включить проверку ссылок на любом веб-сайте.

➡ *Чтобы включить проверку ссылок на любом веб-сайте, выполните следующие действия:*

1. Откройте главное окно программы.
2. В верхней части окна перейдите по ссылке **Настройка**.
3. В открывшемся окне **Настройка** в разделе **Центр защиты** выберите подраздел **Веб-Антивирус** и нажмите на кнопку **Настройка**.

Откроется окно **Веб-Антивирус**.

4. В открывшемся окне на закладке **Веб-фильтр** в блоке **Модуль проверки ссылок** нажмите на кнопку **Настройка**.

Откроется окно **Настройка модуля проверки ссылок**.

5. В открывшемся окне в блоке **Режим проверки** выберите вариант **Любые ссылки**.
6. В окне **Настройка** нажмите на кнопку **Применить**.

ИСПОЛЬЗОВАНИЕ ИГРОВОГО ПРОФИЛЯ ДЛЯ РАБОТЫ В ПОЛНОЭКРАННОМ РЕЖИМЕ

При одновременной работе Антивируса Касперского и некоторых приложений (в особенности компьютерных игр) в полноэкранном режиме иногда могут возникать следующие неудобства:

- работа приложения или игры замедляется из-за недостатка системных ресурсов;
- окна уведомлений Антивируса Касперского отвлекают от игры.

Чтобы не изменять параметры Антивируса Касперского вручную перед каждым переходом в полноэкранный режим, вы можете использовать Игровой профиль. Когда Игровой профиль включен, при переходе в полноэкранный режим автоматически изменяются параметры всех компонентов Антивируса Касперского таким образом, чтобы обеспечить оптимальную работу в этом режиме. При выходе из полноэкранного режима параметрам программы возвращаются значения, которые были установлены до перехода в полноэкранный режим.

➔ Чтобы включить использование Игрового профиля, выполните следующие действия:

1. Откройте окно настройки программы.
2. В левой части окна выберите в разделе **Дополнительные параметры** подраздел **Игровой профиль**.
3. Установите флажок **Использовать Игровой профиль** и в блоке **Параметры профиля** ниже укажите необходимые параметры использования Игрового профиля.

СОЗДАНИЕ И ИСПОЛЬЗОВАНИЕ ДИСКА АВАРИЙНОГО ВОССТАНОВЛЕНИЯ

Диск аварийного восстановления представляет собой программу Kaspersky Rescue Disk, записанную на съемный носитель (компакт-диск или USB-устройство).

Вы можете использовать Kaspersky Rescue Disk для проверки и лечения зараженного компьютера, который нельзя вылечить другим способом (например, с помощью антивирусных программ).

В ЭТОМ РАЗДЕЛЕ

Создание диска аварийного восстановления	45
Загрузка компьютера с помощью диска аварийного восстановления.....	47

СОЗДАНИЕ ДИСКА АВАРИЙНОГО ВОССТАНОВЛЕНИЯ

Создание диска аварийного восстановления заключается в формировании образа диска (файла формата ISO) с актуальной версией программы Kaspersky Rescue Disk и его записи на съемный носитель.

Исходный образ диска можно загрузить с сервера «Лаборатории Касперского» или скопировать с локального источника.

Диск аварийного восстановления создается с помощью *мастера создания и записи Kaspersky Rescue Disk*. Сформированный мастером файл образа rescued.iso сохраняется на жестком диске вашего компьютера:

- в операционной системе Microsoft Windows XP – в папке Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP13\Data\Rdisk\;
- в операционных системах Microsoft Windows Vista и Microsoft Windows 7 – в папке ProgramData\Kaspersky Lab\AVP13\Data\Rdisk\.

➤ Чтобы запустить мастер создания и записи *Kaspersky Rescue Disk*, выполните следующие действия:

1. Откройте главное окно программы.
2. В нижней части окна выберите раздел **Инструменты**.
3. В открывшемся окне в блоке **Kaspersky Rescue Disk** нажмите на кнопку **Создать**.

Мастер состоит из последовательности окон (шагов), переключение между которыми осуществляется нажатием на кнопки **Назад** и **Далее**. Работа мастера завершается нажатием на кнопку **Завершить**. Для прекращения работы мастера на любом этапе следует нажать на кнопку **Отмена**.

Рассмотрим подробнее шаги мастера.

Шаг 1. Начало работы мастера. Поиск существующего образа диска

В первом окне мастера представлена информация о программе *Kaspersky Rescue Disk*.

Если мастер обнаружит ранее созданный файл образа диска в предназначенной для этого папке (см. выше), то в первом окне мастера отобразится флажок **Использовать существующий образ**. Чтобы использовать найденный файл в качестве исходного образа диска и сразу перейти к шагу **Обновление файла образа** (см. ниже), установите этот флажок. Если вы не хотите использовать найденный образ диска, снимите этот флажок. Мастер перейдет к окну **Выбор источника образа диска**.

Шаг 2. Выбор источника образа диска

Если в первом окне мастера вы установили флажок **Использовать существующий образ**, то этот шаг пропускается.

На этом шаге вам следует выбрать источник образа диска из предложенных вариантов:

- Если у вас уже есть записанный диск аварийного восстановления или его образ (файл формата ISO), сохраненный на вашем компьютере или на ресурсе локальной сети, выберите вариант **Копировать образ с локального или сетевого диска**.
- Если у вас нет файла образа диска аварийного восстановления, и вы хотите загрузить его с сервера «Лаборатории Касперского» (размер файла составляет примерно 175 МБ), выберите вариант **Загрузить образ с сервера «Лаборатории Касперского»**.

Шаг 3. Копирование (загрузка) образа диска

Если в первом окне мастера вы установили флажок **Использовать существующий образ**, то этот шаг пропускается.

Если на предыдущем шаге вы выбрали вариант **Копировать образ с локального или сетевого диска**, нажмите на кнопку **Обзор**. Указав путь к файлу, нажмите на кнопку **Далее**. В окне мастера будет отображен процесс копирования образа диска.

Если на предыдущем шаге вы выбрали вариант **Загрузить образ с сервера «Лаборатории Касперского»**, то процесс загрузки образа диска отображается сразу.

По завершении копирования или загрузки образа диска мастер автоматически переходит к следующему шагу.

Шаг 4. Обновление файла образа диска

Процедура обновления файла образа диска включает в себя следующие действия:

- обновление баз программы;
- обновление конфигурационных файлов.

Конфигурационные файлы определяют возможность загрузки компьютера со съемного носителя (например, CD / DVD-диска или USB-устройства с Kaspersky Rescue Disk), полученного в результате работы мастера.

При обновлении баз программы используются базы, полученные при последнем обновлении Антивируса Касперского. Если базы устарели, рекомендуется выполнить задачу обновления и запустить мастер создания и записи Kaspersky Rescue Disk заново.

Для начала обновления файла образа нажмите на кнопку **Далее**. В окне мастера будет отображен ход выполнения обновления.

Шаг 5. Запись образа диска на носитель

На этом шаге мастер проинформирует вас об успешном создании образа диска и предложит записать образ диска на носитель.

Укажите носитель для записи Kaspersky Rescue Disk:

- Для записи на CD / DVD-диск выберите вариант **Записать на CD/DVD диск** и укажите диск, на который вы хотите записать образ диска.
- Для записи на USB-устройство выберите вариант **Записать на USB-устройство** и укажите устройство, на которое вы хотите записать образ диска.

«Лаборатория Касперского» не рекомендует записывать образ диска на устройства, не предназначенные исключительно для хранения данных, например, смартфоны, мобильные телефоны, КПК, MP3-плееры. В дальнейшем такие устройства, использованные для записи образа диска, могут работать неправильно.

- Для записи на жесткий диск на вашем компьютере или на другом компьютере, к которому вы имеете доступ по сети, выберите вариант **Сохранить образ в файл на локальном или сетевом диске** и укажите папку, в которую вы хотите записать образ диска, и имя файла формата ISO.

Шаг 6. Завершение работы мастера

Для завершения работы мастера нажмите на кнопку **Завершить**. Созданный диск аварийного восстановления вы можете использовать для загрузки компьютера (см. стр. 47), если в результате действий вирусов или вредоносных программ невозможно выполнить загрузку компьютера и запуск Антивируса Касперского в обычном режиме.

ЗАГРУЗКА КОМПЬЮТЕРА С ПОМОЩЬЮ ДИСКА АВАРИЙНОГО ВОССТАНОВЛЕНИЯ

Если в результате вирусной атаки невозможно загрузить операционную систему, воспользуйтесь диском аварийного восстановления.

Для загрузки операционной системы необходим CD / DVD-диск или USB-устройство с записанной на него программой Kaspersky Rescue Disk (см. раздел «Создание диска аварийного восстановления» на стр. 45).

Загрузка компьютера со съемного носителя не всегда возможна. В частности, она не поддерживается некоторыми устаревшими моделями компьютеров. Прежде чем выключить компьютер для последующей загрузки со съемного носителя, уточните возможность такой загрузки.

➔ Чтобы загрузить компьютер с помощью диска аварийного восстановления, выполните следующие действия:

1. В параметрах BIOS включите загрузку с CD / DVD-диска или USB-устройства (подробную информацию можно получить из документации к материнской плате вашего компьютера).
2. Поместите в дисковод зараженного компьютера CD / DVD-диск или подключите USB-устройство с предварительно записанной программой Kaspersky Rescue Disk.
3. Перезагрузите компьютер.

Более подробную информацию об использовании диска аварийного восстановления можно найти в руководстве пользователя Kaspersky Rescue Disk.

ЗАЩИТА ДОСТУПА К ПАРАМЕТРАМ АНТИВИРУСА КАСПЕРСКОГО С ПОМОЩЬЮ ПАРОЛЯ

На одном компьютере могут работать несколько пользователей с разным опытом и уровнем компьютерной грамотности. Неограниченный доступ разных пользователей к управлению Антивирусом Касперского и настройке его параметров может привести к снижению уровня защищенности компьютера.

Чтобы ограничить доступ к программе, вы можете задать пароль администратора и указать действия, при выполнении которых этот пароль должен запрашиваться:

- настройка параметров программы;
- управление Родительским контролем;
- завершение работы программы;
- удаление программы.

➔ Чтобы защитить доступ к Антивирусу Касперского с помощью пароля, выполните следующие действия:

1. Откройте главное окно программы.
2. В правом верхнем углу окна перейдите по ссылке **Настройка**.
3. В открывшемся окне **Настройка** в разделе **Центр защиты** выберите подраздел **Основные параметры**.
4. Установите флажок **Защитить паролем доступ к параметрам программы** и нажмите на кнопку **Настройка**.
Откроется окно **Защита паролем**.
5. В открывшемся окне заполните поля **Новый пароль** и **Подтверждение пароля**.
6. Если вы хотите изменить пароль, созданный ранее, введите его в поле **Старый пароль**.
7. В блоке параметров **Область действия пароля** укажите действия с программой, доступ к которым нужно защитить паролем.
8. В окне **Настройка** нажмите на кнопку **Применить**.

Забывший пароль восстановить нельзя. Для восстановления доступа к параметрам Антивируса Касперского при забытом пароле потребуется обращение в Службу технической поддержки.

ПРИОСТАНОВКА И ВОЗОБНОВЛЕНИЕ ЗАЩИТЫ КОМПЬЮТЕРА

Приостановка защиты означает выключение на некоторое время всех ее компонентов.

➔ Чтобы приостановить защиту компьютера, выполните следующие действия:

1. В контекстном меню значка программы в области уведомлений выберите пункт **Приостановить защиту**.

Откроется окно **Приостановка защиты** (см. рис. ниже).

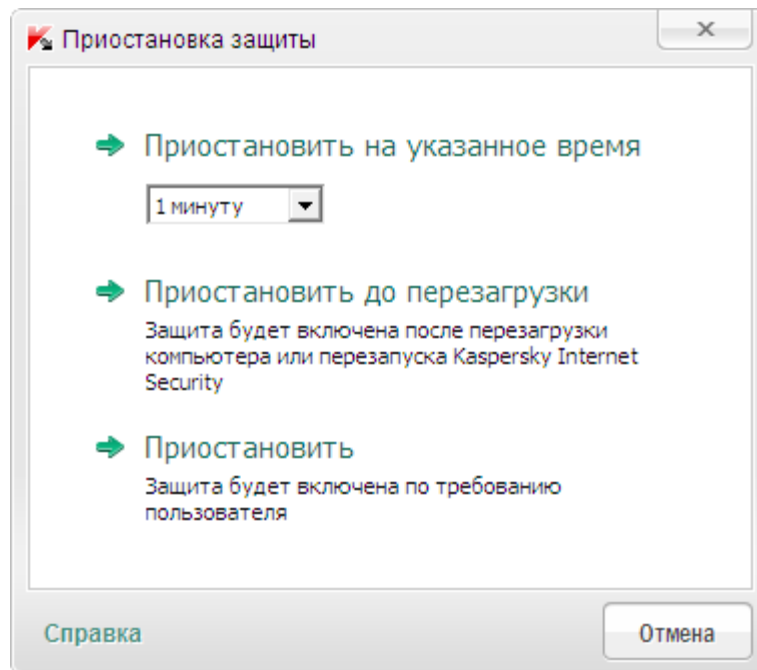


Рисунок 8. Окно **Приостановка защиты**

2. В окне **Приостановка защиты** выберите период, по истечении которого защита будет включена:

- **Приостановить на указанное время** – защита будет включена через интервал, выбранный в раскрывающемся списке ниже.
- **Приостановить до перезагрузки** – защита будет включена после перезапуска программы или перезагрузки системы (при условии, что включен автоматический запуск программы).
- **Приостановить** – защита будет включена тогда, когда вы решите возобновить ее.

➔ Чтобы возобновить защиту компьютера,


выберите пункт **Возобновить защиту** в контекстном меню значка программы в области уведомлений.

ПРОСМОТР ОТЧЕТА О РАБОТЕ ПРОГРАММЫ

Антивирус Касперского ведет отчеты о работе каждого компонента защиты. С помощью отчета вы можете получить статистическую информацию о работе программы (например, узнать, сколько обнаружено и обезврежено вредоносных объектов за определенный период, сколько раз за это время программа обновлялась, сколько обнаружено спам-сообщений и многое другое).

При работе на компьютере под управлением операционной системы Microsoft Windows Vista или Microsoft Windows 7 вы можете открыть отчеты с помощью Kaspersky Gadget. Для этого Kaspersky Gadget должен быть настроен таким образом, чтобы одной из его кнопок была назначена функция открывания окна отчетов (см. раздел «Использование Kaspersky Gadget» на стр. [53](#)).

➔ *Чтобы просмотреть отчет о работе программы, выполните следующие действия:*

1. Откройте окно **Отчеты** одним из следующих способов:
 - перейдите по ссылке **Отчеты** в верхней части главного окна программы;
 - нажмите на кнопку со значком  **Отчеты** в интерфейсе Kaspersky Gadget (только для операционных систем Microsoft Windows Vista и Microsoft Windows 7).

В окне **Отчеты** в виде диаграмм отображаются отчеты о работе программы.

2. Если вам нужно просмотреть подробный отчет о работе программы (например, о работе каждого из ее компонентов), нажмите на кнопку **Подробный отчет**, расположенную в нижней части окна **Отчеты**.

Откроется окно **Подробный отчет**, в котором данные представлены в табличном виде. Для удобства просмотра отчетов вы можете выбирать различные варианты группировки записей.

ВОССТАНОВЛЕНИЕ СТАНДАРТНЫХ ПАРАМЕТРОВ РАБОТЫ ПРОГРАММЫ

Вы в любое время можете восстановить параметры работы Антивируса Касперского, рекомендуемые «Лабораторией Касперского». Восстановление параметров осуществляется с помощью *мастера настройки программы*.

В результате работы мастера для всех компонентов защиты будет установлен уровень безопасности *Рекомендуемый*. При восстановлении рекомендуемого уровня безопасности вы можете выборочно сохранять ранее сделанные настройки параметров для компонентов программы.

➔ *Чтобы запустить мастер настройки программы, выполните следующие действия:*

1. Откройте главное окно программы.
2. В верхней части окна перейдите по ссылке **Настройка**.
3. В открывшемся окне **Настройка** запустите мастер настройки программы одним из следующих способов:
 - перейдите по ссылке **Восстановить** в левом нижнем углу окна;

- в верхней части окна выберите раздел **Дополнительно**, подраздел **Управление параметрами** и нажмите на кнопку **Восстановить** в блоке **Восстановление стандартных параметров** (см. рис. ниже).

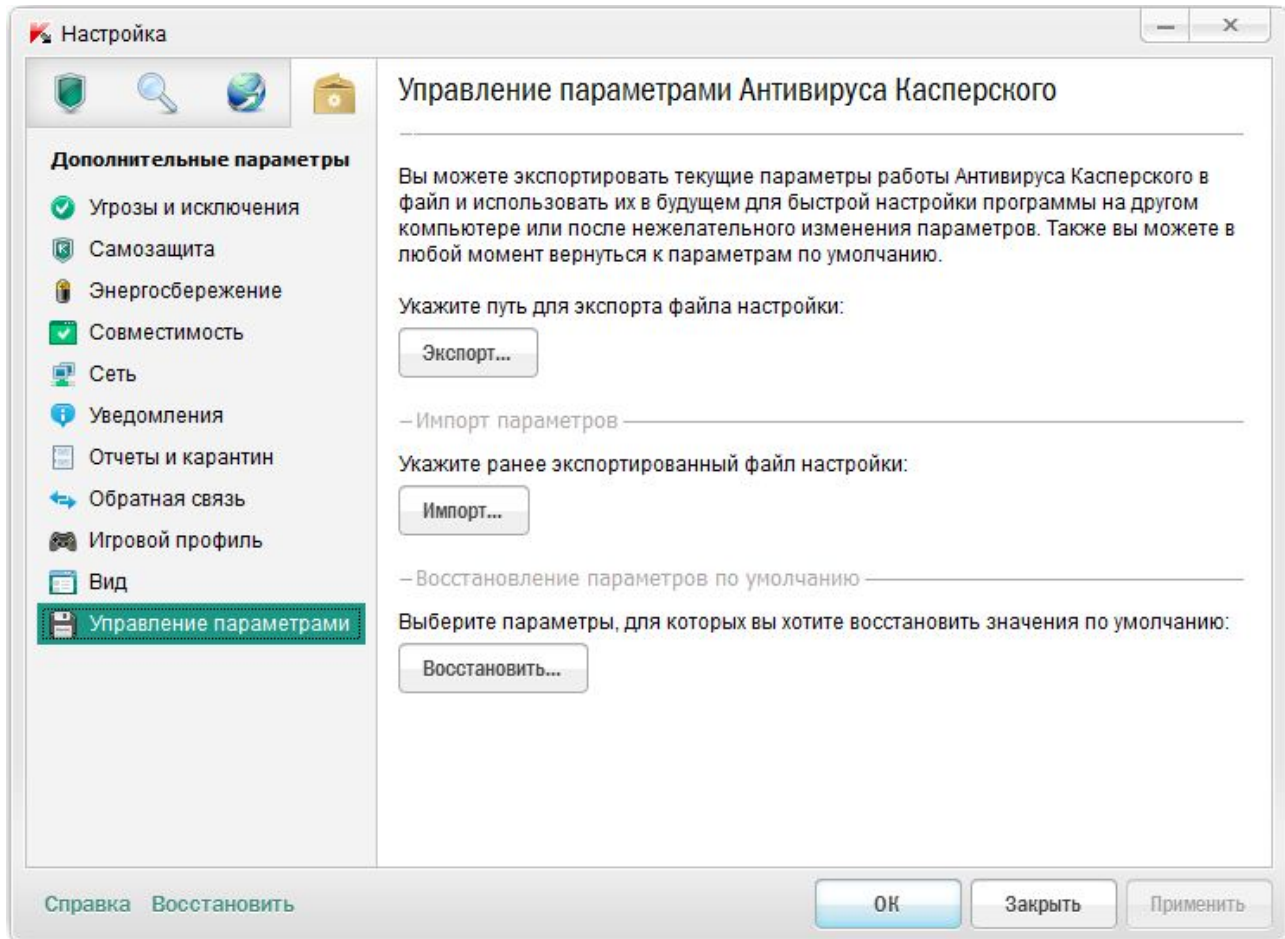


Рисунок 9. Окно **Настройка**, подраздел **Управление параметрами**

Рассмотрим подробнее шаги мастера.

Шаг 1. Начало работы мастера

Нажмите на кнопку **Далее**, чтобы продолжить работу мастера.

Шаг 2. Восстановление параметров

В этом окне мастера представлены компоненты защиты Антивируса Касперского, параметры которых были изменены пользователем. Если для какого-либо компонента были сформированы уникальные параметры, они также будут представлены в окне (см. рис. ниже).

Установите флажки для тех параметров, которые нужно сохранить и нажмите на кнопку **Далее**.

Шаг 3. Завершение восстановления

Для завершения работы мастера нажмите на кнопку **Завершить**.

ИМПОРТ ПАРАМЕТРОВ ПРОГРАММЫ В АНТИВИРУС КАСПЕРСКОГО, УСТАНОВЛЕННЫЙ НА ДРУГОМ КОМПЬЮТЕРЕ

Настроив программу, вы можете применить параметры ее работы к Антивирусу Касперского, установленному на другом компьютере. В результате программа на обоих компьютерах будет настроена одинаково. Это полезно, например, в том случае, когда Антивирус Касперского установлен и на домашнем, и на офисном компьютере.

Перенос параметров Антивируса Касперского с одного компьютера на другой производится в три этапа:

1. Экспорт параметров программы в файл настройки.
2. Перенос файла настройки на другой компьютер (например, по электронной почте или на съемном носителе).
3. Применение параметров из файла настройки к программе, установленной на другом компьютере.

➡ *Чтобы сохранить параметры программы Антивируса Касперского в файле настройки, выполните следующие действия:*

1. Откройте главное окно программы.
2. В верхней части окна перейдите по ссылке **Настройка**.
3. В верхней части окна **Настройка** выберите в разделе **Дополнительно** подраздел **Управление параметрами**.
4. В подразделе **Управление параметрами** нажмите на кнопку **Экспорт**.
5. В открывшемся окне введите название файла настройки и укажите место его сохранения.
6. Нажмите на кнопку **ОК**.

➡ *Чтобы применить параметры из файла настройки к программе, установленной на другом компьютере, выполните следующие действия:*

1. Откройте главное окно программы.
2. В верхней части окна перейдите по ссылке **Настройка**.
3. В верхней части окна **Настройка** выберите в разделе **Дополнительно** подраздел **Управление параметрами**.
4. В подразделе **Управление параметрами** нажмите на кнопку **Импорт**.
5. В открывшемся окне выберите файл, из которого вы хотите импортировать параметры Антивируса Касперского.
6. Нажмите на кнопку **ОК**.

ИСПОЛЬЗОВАНИЕ KASPERSKY GADGET

При использовании Антивируса Касперского на компьютере под управлением операционной системы Microsoft Windows Vista или Microsoft Windows 7 вам доступен Kaspersky Gadget (далее также *гаджет*). После установки Антивируса Касперского на компьютер под управлением операционной системы Microsoft Windows 7 гаджет появляется на рабочем столе автоматически. После установки программы на компьютер под управлением операционной системы Microsoft Windows Vista гаджет нужно добавить на боковую панель Microsoft Windows вручную (см. документацию на операционную систему).

Цветовой индикатор гаджета сигнализирует о состоянии защиты вашего компьютера, так же, как индикатор, расположенный в главном окне программы (см. раздел «Анализ состояния защиты компьютера и устранение проблем безопасности» на стр. 29). Зеленый цвет означает, что компьютер защищен, желтый цвет свидетельствует о наличии проблем в защите, красный – о серьезной угрозе безопасности компьютера. Серый цвет индикатора означает, что работа программы остановлена.


С помощью гаджета вы можете выполнять следующие действия:

- возобновлять работу программы, если она была приостановлена;
- открывать главное окно программы;
- проверять отдельные объекты на вирусы;
- открывать окно просмотра новостей.

Также вы можете настроить кнопки гаджета, чтобы выполнять дополнительные действия:

- запускать обновление;
- изменять параметры работы программы;
- просматривать отчеты программы;
- приостанавливать защиту;
- открывать виртуальную клавиатуру;
- открывать окно Менеджера задач.

➤ *Чтобы запустить программу с помощью гаджета,*

нажмите на значок  **Включить**, расположенный в центре гаджета.

➤ *Чтобы открыть главное окно программы с помощью гаджета,*

нажмите на изображение монитора в центре гаджета.

➤ *Чтобы проверить объект на вирусы с помощью гаджета,*


перетащите объект проверки на гаджет.

Процесс выполнения задачи будет отображаться в окне **Менеджер задач**.

➤ *Чтобы открыть окно просмотра новостей с помощью гаджета,*

нажмите на значок , который отображается в центре гаджета при появлении новости.

➤ Чтобы настроить гаджет, выполните следующие действия:

1. Откройте окно настройки гаджета, нажав на значок , появляющийся в правом верхнем углу блока с гаджетом при наведении курсора мыши.
2. В раскрывающихся списках, соответствующих кнопкам гаджета, выберите действия, которые должны выполняться при нажатии на кнопки гаджета.
3. Нажмите на кнопку **ОК**.

УЧАСТИЕ В KASPERSKY SECURITY NETWORK (KSN)

Чтобы повысить эффективность защиты вашего компьютера, Антивирус Касперского использует данные, полученные от пользователей во всем мире. Для сбора этих данных предназначена сеть Kaspersky Security Network.

Kaspersky Security Network (KSN) – это инфраструктура онлайн-служб и сервисов, предоставляющая доступ к оперативной базе знаний «Лаборатории Касперского» о репутации файлов, интернет-ресурсов и программного обеспечения. Использование данных Kaspersky Security Network обеспечивает более высокую скорость реакции Антивируса Касперского на новые виды угроз, повышает эффективность работы некоторых компонентов защиты, а также снижает вероятность ложных срабатываний.

Участие пользователей в Kaspersky Security Network позволяет «Лаборатории Касперского» оперативно собирать информацию о типах и источниках новых угроз, разрабатывать способы их нейтрализации, уменьшать количество ложных срабатываний. Участие в Kaspersky Security Network обеспечивает вам доступ к данным о репутации программ и веб-сайтов.

В ЭТОМ РАЗДЕЛЕ

Включение и выключение участия в Kaspersky Security Network	54
Проверка подключения к Kaspersky Security Network.....	55

ВКЛЮЧЕНИЕ И ВЫКЛЮЧЕНИЕ УЧАСТИЯ В KASPERSKY SECURITY NETWORK

Участие в Kaspersky Security Network является добровольным. Вы можете включить или выключить использование Kaspersky Security Network во время установки Антивируса Касперского и / или в любой момент после установки программы.

➤ Чтобы включить или выключить участие в Kaspersky Security Network, выполните следующие действия:

1. Откройте главное окно программы.
2. В верхней части окна перейдите по ссылке **Настройка**.
3. В открывшемся окне **Настройка** в разделе **Дополнительные параметры** выберите подраздел **Обратная связь**.
4. В правой части окна выполните одно из следующих действий:
 - если вы хотите участвовать в KSN, установите флажок **Я согласен участвовать в Kaspersky Security Network**;
 - если вы не хотите участвовать в KSN, снимите флажок **Я согласен участвовать в Kaspersky Security Network**.

ПРОВЕРКА ПОДКЛЮЧЕНИЯ К KASPERSKY SECURITY NETWORK

Подключение к Kaspersky Security Network может отсутствовать по следующим причинам:

- Вы не участвуете в Kaspersky Security Network.
- Ваш компьютер не подключен к интернету.
- Текущий статус ключа не позволяет осуществить подключение к Kaspersky Security Network.

Текущий статус ключа отображается в окне **Лицензирование** (см. раздел «**Приобретение лицензии и продление срока ее действия**» на стр. [28](#)).

➔ Чтобы проверить подключение к Kaspersky Security Network, выполните следующие действия:

1. Откройте главное окно программы.
2. В верхней части окна нажмите на кнопку **Защита из облака**.

В левой части открывшегося окна отображается статус подключения к Kaspersky Security Network.

ПЕРЕХОД С АНТИВИРУСА КАСПЕРСКОГО К ИСПОЛЬЗОВАНИЮ KASPERSKY INTERNET SECURITY

Антивирус Касперского позволяет перейти к использованию программы Kaspersky Internet Security без дополнительной загрузки и установки программного обеспечения.

Kaspersky Internet Security – это программа, предназначенная для комплексной защиты вашего компьютера. Она обладает рядом дополнительных возможностей, которые реализуются с помощью следующих модулей и функций:

- Контроль программ;
- Родительский контроль;
- Сетевой экран;
- Защита от сетевых атак;
- Безопасные платежи;
- Гео-фильтр;
- Блокирование доступа к опасным веб-сайтам;
- Мониторинг сети;
- Анти-Спам;
- Анти-Баннер.

Вы можете временно переключиться на пробную версию Kaspersky Internet Security, чтобы изучить ее возможности, или немедленно перейти к работе с коммерческой версией программы.

При использовании программы по подписке, а также при работе с программой в некоторых регионах временное переключение на работу с пробной версией Kaspersky Internet Security не предусмотрено.

В ЭТОМ РАЗДЕЛЕ

Временное переключение на пробную версию.....	56
Переключение на коммерческую версию.....	57

ВРЕМЕННОЕ ПЕРЕКЛЮЧЕНИЕ НА ПРОБНУЮ ВЕРСИЮ

Вы можете временно переключиться на пробную версию Kaspersky Internet Security, чтобы оценить его возможности. При желании вы сможете приобрести лицензию для постоянной работы с программой.

➤ *Чтобы временно переключиться на работу с Kaspersky Internet Security, выполните следующие действия:*

1. Откройте главное окно программы.
2. В нижней части окна выберите раздел **Расширение защиты**.
3. В открывшемся окне нажмите на кнопку **Пробная версия**.

Будет запущен мастер миграции.

При использовании программы по подписке, а также при работе с программой в некоторых регионах временное переключение на работу с пробной версией Kaspersky Internet Security не предусмотрено. В этих случаях раздел **Расширение защиты** в главном окне программы отсутствует.

Рассмотрим подробнее шаги мастера.

Шаг 1. Запрос на активацию пробной версии Kaspersky Internet Security

При успешном выполнении запроса на активацию Kaspersky Internet Security мастер автоматически переходит к следующему шагу.

Шаг 2. Начало расширения защиты

На этом шаге мастер выводит на экран сообщение о готовности к выполнению миграции. Для продолжения работы мастера нажмите на кнопку **Далее**.

Шаг 3. Удаление несовместимых программ

На этом шаге мастер проверяет, нет ли на вашем компьютере программ, несовместимых с Kaspersky Internet Security. Если таких программ нет, мастер автоматически перейдет к следующему шагу. Если такие программы будут найдены, мастер выведет их список в окне и предложит вам удалить их.

После удаления несовместимых программ может потребоваться перезагрузка операционной системы. После перезагрузки мастер запустится автоматически, и процесс миграции будет продолжен.

Шаг 4. Переход к использованию Kaspersky Internet Security

На этом шаге выполняется подключение компонентов Kaspersky Internet Security, что может занять некоторое время. По завершении процесса мастер автоматически перейдет к следующему шагу.

Шаг 5. Перезапуск программы

На завершающем шаге миграции требуется перезапустить программу. Для этого нажмите на кнопку **Завершить** в окне мастера.

Шаг 6. Завершение активации

После перезапуска программы мастер запускается автоматически. При успешной активации пробной версии Kaspersky Internet Security в окне мастера отображается информация о сроке, в течение которого вы можете использовать пробную версию.

Шаг 7. Анализ системы

На этом этапе производится сбор информации о программах, входящих в состав Microsoft Windows. Эти программы попадают в список доверенных программ, которые не имеют ограничений на действия, совершаемые в системе.

По завершении анализа мастер автоматически переходит к следующему шагу.

Шаг 8. Завершение миграции

Для завершения работы мастера нажмите на кнопку **Завершить**.

Повторное временное переключение на пробную версию Kaspersky Internet Security не предусмотрено.

ПЕРЕКЛЮЧЕНИЕ НА КОММЕРЧЕСКУЮ ВЕРСИЮ

Если вы хотите переключиться на коммерческую версию Kaspersky Internet Security, вам понадобится код активации коммерческой версии программы, с помощью которого вы можете ее активировать (см. раздел «Активация программы» на стр. [27](#)).

➤ *Чтобы приобрести код активации для Kaspersky Internet Security, выполните следующие действия:*

1. Откройте главное окно программы.
2. В нижней части окна выберите раздел **Расширение защиты**.
3. В открывшемся окне нажмите на кнопку **Купить код активации**.

Вы перейдете на веб-сайт интернет-магазина, где сможете приобрести код активации для Kaspersky Internet Security.

При использовании программы по подписке, а также при работе с программой в некоторых регионах временное переключение на работу с пробной версией Kaspersky Internet Security не предусмотрено. В этих случаях раздел **Расширение защиты** в главном окне программы отсутствует.

ОБРАЩЕНИЕ В СЛУЖБУ ТЕХНИЧЕСКОЙ ПОДДЕРЖКИ

Этот раздел содержит информацию о способах получения технической поддержки и о том, какие условия требуются для получения помощи от Службы технической поддержки.

В ЭТОМ РАЗДЕЛЕ

Способы получения технической поддержки	58
Техническая поддержка по телефону	58
Получение технической поддержки через Личный кабинет	59
Использование файла трассировки и скрипта AVZ	60

СПОСОБЫ ПОЛУЧЕНИЯ ТЕХНИЧЕСКОЙ ПОДДЕРЖКИ

Если вы не нашли решения вашей проблемы в документации к программе или в одном из источников информации о программе (см. раздел «Источники информации о программе» на стр. [9](#)), рекомендуем обратиться в Службу технической поддержки «Лаборатории Касперского». Сотрудники Службы технической поддержки ответят на ваши вопросы об установке и использовании программы.

Прежде чем обратиться в Службу технической поддержки, ознакомьтесь с правилами предоставления технической поддержки (<http://support.kaspersky.ru/support/rules>).

Вы можете связаться со специалистами Службы технической поддержки одним из следующих способов:

- Позвонить по телефону. Этот способ позволяет проконсультироваться по телефону со специалистами русскоязычной или интернациональной Службы технической поддержки.
- Отправить запрос из Личного кабинета на веб-сайте Службы технической поддержки. Этот способ позволяет вам связаться со специалистами Службы технической поддержки через форму запроса.

Техническая поддержка предоставляется только пользователям, которые приобрели коммерческую лицензию на использование программы. Техническая поддержка для владельцев пробных лицензий не осуществляется.

ТЕХНИЧЕСКАЯ ПОДДЕРЖКА ПО ТЕЛЕФОНУ

Если возникла неотложная проблема, вы можете позвонить специалистам русскоязычной или международной технической поддержки (<http://support.kaspersky.ru/support/international>).

Перед обращением в Службу технической поддержки, пожалуйста, ознакомьтесь с правилами предоставления поддержки (<http://support.kaspersky.ru/support/details>). Это позволит нашим специалистам быстрее помочь вам.

ПОЛУЧЕНИЕ ТЕХНИЧЕСКОЙ ПОДДЕРЖКИ ЧЕРЕЗ ЛИЧНЫЙ КАБИНЕТ

Личный кабинет – это ваш персональный раздел (<https://my.kaspersky.ru>) на сайте Службы технической поддержки.

Для доступа к Личному кабинету вам требуется зарегистрироваться на странице регистрации (<https://my.kaspersky.com/ru/registration>). Вам нужно указать адрес электронной почты и пароль для доступа в Личный кабинет.

В Личном кабинете вы можете выполнять следующие действия:

- отправлять запросы в Службу технической поддержки и Вирусную лабораторию;
- обмениваться сообщениями со Службой технической поддержки без использования электронной почты;
- отслеживать состояние ваших запросов в реальном времени;
- просматривать полную историю ваших запросов в Службу технической поддержки;
- получать копию файла ключа в случае, если файл ключа был утерян или удален.

Электронный запрос в Службу технической поддержки

Вы можете отправить электронный запрос в Службу технической поддержки на русском, английском, немецком, французском или испанском языках.

В полях формы электронного запроса вам нужно указать следующие сведения:

- тип запроса;
- название и номер версии программы;
- текст запроса;
- номер клиента и пароль;
- электронный адрес.

Специалист Службы технической поддержки направляет ответ на ваш вопрос в ваш Личный кабинет и по адресу электронной почты, который вы указали в электронном запросе.

Электронный запрос в Вирусную лабораторию

Некоторые запросы требуется направлять не в Службу технической поддержки, а в Вирусную лабораторию.

Вы можете направлять в Вирусную лабораторию запросы следующих типов:

- *Неизвестная вредоносная программа* – вы подозреваете, что файл содержит вирус, но Антивирус Касперского не обнаруживает его в качестве зараженного.
Специалисты Вирусной лаборатории анализируют присылаемый вредоносный код и при обнаружении неизвестного ранее вируса добавляют его описание в базу данных, доступную при обновлении антивирусных программ.
- *Ложное срабатывание антивируса* – Антивирус Касперского определяет файл как содержащий вирус, но вы уверены, что файл не является вирусом.
- *Запрос на описание вредоносной программы* – вы хотите получить описание вируса, обнаруженного Антивирусом Касперского, на основе названия этого вируса.

Вы также можете направлять запросы в Вирусную лабораторию со страницы с формой запроса (<http://support.kaspersky.ru/virlab/helpdesk.html>), не регистрируясь в Личном кабинете. При этом вам не требуется указывать код активации программы.

ИСПОЛЬЗОВАНИЕ ФАЙЛА ТРАССИРОВКИ И СКРИПТА AVZ

После того как вы проинформируете специалистов Службы технической поддержки о возникшей проблеме, они могут попросить вас сформировать отчет с информацией об операционной системе и отправить его в Службу технической поддержки. Также специалисты Службы технической поддержки могут попросить вас создать *файл трассировки*. Файл трассировки позволяет отследить процесс пошагового выполнения команд программы и обнаружить, на каком этапе работы программы возникает ошибка.

В результате анализа присланных вами данных специалисты Службы технической поддержки могут создать и отправить вам скрипт AVZ. Выполнение скриптов AVZ позволяет проводить анализ запущенных процессов на наличие вредоносного кода, проверять систему на наличие вредоносного кода, лечить / удалять зараженные файлы и создавать отчеты о результатах проверки системы.

В ЭТОМ РАЗДЕЛЕ

Создание отчета о состоянии системы	60
Отправка файлов данных	61
Выполнение скрипта AVZ	62

СОЗДАНИЕ ОТЧЕТА О СОСТОЯНИИ СИСТЕМЫ

➤ *Чтобы создать отчет о состоянии системы, выполните следующие действия:*

1. Откройте главное окно программы.
2. По ссылке **Поддержка** в нижней части окна откройте окно **Поддержка**.
3. В открывшемся окне нажмите на кнопку **Мониторинг проблем**.
Откроется окно **Мониторинг проблем**.
4. В открывшемся окне нажмите на кнопку **Создать отчет о системе**.

Отчет о состоянии системы формируется в форматах HTML и XML и сохраняется в архиве sysinfo.zip. По окончании сбора информации о системе вы можете просмотреть отчет.

➤ *Чтобы просмотреть отчет, выполните следующие действия:*

1. Откройте главное окно программы.
2. По ссылке **Поддержка** в нижней части окна откройте окно **Поддержка**.
3. В открывшемся окне нажмите на кнопку **Мониторинг проблем**.
Откроется окно **Мониторинг проблем**.
4. В открывшемся окне перейдите по ссылке **Просмотреть отчет**.
Откроется окно проводника Microsoft Windows.
5. В открывшемся окне откройте архив sysinfo.zip, содержащий файлы отчета.

ОТПРАВКА ФАЙЛОВ ДАННЫХ

После создания файлов трассировки и отчета о состоянии системы их необходимо отправить специалистам Службы технической поддержки «Лаборатории Касперского».

Чтобы загрузить файлы на сервер Службы технической поддержки, вам понадобится номер запроса (см. раздел «Получение технической поддержки через Личный кабинет» на стр. 59). Этот номер доступен в вашем Личном кабинете на веб-сайте Службы технической поддержки при наличии активного запроса.

➔ *Чтобы загрузить файлы данных на сервер Службы технической поддержки, выполните следующие действия:*

1. Откройте главное окно программы.
2. По ссылке **Поддержка** в нижней части окна откройте окно **Поддержка**.
3. В открывшемся окне нажмите на кнопку **Мониторинг проблем**.
Откроется окно **Мониторинг проблем**.
4. В открывшемся окне нажмите на кнопку **Отправить служебную информацию в Службу технической поддержки**.
Откроется окно **Отправка отчета**.
5. Установите флажки рядом с теми данными, которые вы хотите отправить в Службу технической поддержки, и нажмите на кнопку **Отправить**.
Откроется окно **Введите номер запроса**.
6. Укажите номер, присвоенный вашему запросу при обращении в Службу технической поддержки через Личный кабинет, и нажмите на кнопку **ОК**.

Выбранные файлы данных будут упакованы и отправлены на сервер Службы технической поддержки.

Если связаться со Службой технической поддержки по какой-либо причине невозможно, вы можете сохранить файлы данных на вашем компьютере и впоследствии отправить их из Личного кабинета.

➔ *Чтобы сохранить файлы данных на диске, выполните следующие действия:*

1. Откройте главное окно программы.
2. По ссылке **Поддержка** в нижней части окна откройте окно **Поддержка**.
3. В открывшемся окне нажмите на кнопку **Мониторинг проблем**.
4. Откроется окно **Мониторинг проблем**.
5. В открывшемся окне нажмите на кнопку **Отправить служебную информацию в Службу технической поддержки**.
Откроется окно **Отправка отчета**.
6. Установите флажки рядом с теми данными, которые вы хотите отправить в Службу технической поддержки, и нажмите на кнопку **Отправить**.
Откроется окно **Введите номер запроса**.

7. Нажмите на кнопку **Отмена** и в открывшемся окне подтвердите сохранение файлов на диске, нажав на кнопку **Да**.

Откроется окно сохранения архива.

8. Задайте имя архива и подтвердите сохранение.

Созданный архив вы можете отправить в Службу технической поддержки через Личный кабинет.

ВЫПОЛНЕНИЕ СКРИПТА AVZ

Не рекомендуется вносить изменения в текст скрипта, присланного вам специалистами «Лаборатории Касперского». В случае возникновения проблем в ходе выполнения скрипта обращайтесь в Службу технической поддержки (см. раздел «Способы получения технической поддержки» на стр. [58](#)).

➔ Чтобы выполнить скрипт AVZ, выполните следующие действия:

1. Откройте главное окно программы.
2. По ссылке **Поддержка** в нижней части окна откройте окно **Поддержка**.
3. В открывшемся окне нажмите на кнопку **Мониторинг проблем**.

Откроется окно **Мониторинг проблем**.

4. В открывшемся окне нажмите на кнопку **Выполнить скрипт**.

Откроется окно **Выполнение скрипта AVZ**.

5. Скопируйте текст скрипта, полученного от специалистов Службы технической поддержки, вставьте его в поле ввода в открывшемся окне и нажмите на кнопку **Далее**.

Запустится выполнение скрипта.

В случае успешного выполнения скрипта работа мастера завершится автоматически. Если во время выполнения скрипта возникнет сбой, мастер выведет на экран соответствующее сообщение.

ГЛОССАРИЙ

К

KASPERSKY SECURITY NETWORK (KSN)

Инфраструктура онлайн-служб и сервисов, предоставляющая доступ к оперативной базе знаний «Лаборатории Касперского» о репутации файлов, веб-ресурсов и программного обеспечения. Использование данных Kaspersky Security Network обеспечивает более высокую скорость реакции программ «Лаборатории Касперского» на новые виды угроз, повышает эффективность работы некоторых компонентов защиты, а также снижает вероятность ложных срабатываний.

А

АКТИВАЦИЯ ПРОГРАММЫ

Перевод программы в полнофункциональный режим. Активация выполняется пользователем во время или после установки программы. Для активации программы пользователю необходим код активации.

АРХИВ

Один или несколько файлов, упакованных в один файл в сжатом виде. Для архивирования и разархивирования данных требуется специальная программа – архиватор.

Б

БАЗА ВРЕДОНОСНЫХ ВЕБ-АДРЕСОВ

Список адресов веб-ресурсов, содержимое которых может быть расценено как опасное. Список сформирован специалистами «Лаборатории Касперского», регулярно обновляется и входит в поставку программы «Лаборатории Касперского».

БАЗА ФИШИНГОВЫХ ВЕБ-АДРЕСОВ

Список адресов веб-ресурсов, которые определены специалистами «Лаборатории Касперского» как фишинговые. База регулярно обновляется и входит в поставку программы «Лаборатории Касперского».

БАЗЫ

Базы данных, которые содержат описания угроз компьютерной безопасности, известных «Лаборатории Касперского» на момент выпуска баз. Записи в базах позволяют обнаруживать в проверяемых объектах вредоносный код. Базы формируются специалистами «Лаборатории Касперского» и обновляются каждый час.

БЛОКИРОВАНИЕ ОБЪЕКТА

Запрет доступа к объекту со стороны внешних программ. Заблокированный объект не может быть прочитан, выполнен, изменен или удален.

В

ВИРУС

Программа, которая заражает другие программы – добавляет в них свой код, чтобы получить управление при запуске зараженных файлов. Это простое определение дает возможность выявить основное действие, выполняемое вирусом – заражение.

ВИРУСНАЯ АТАКА

Ряд целенаправленных попыток заразить компьютер вирусом.

ВОЗМОЖНО ЗАРАЖЕННЫЙ ОБЪЕКТ

Объект, код которого содержит модифицированный код известной угрозы, или код, напоминающий код угрозы по своему поведению.

ВОЗМОЖНЫЙ СПАМ

Сообщение, которое нельзя однозначно классифицировать как спам, но которое обладает некоторыми признаками спама (например, некоторые виды рассылок и рекламных сообщений).

Д

ДОВЕРЕННЫЙ ПРОЦЕСС

Программный процесс, файловые операции которого не контролируются программой «Лаборатории Касперского» в режиме постоянной защиты. При обнаружении подозрительной активности доверенного процесса Антивирус Касперского исключает этот процесс из списка доверенных и блокирует его действия.

ДОСТУПНОЕ ОБНОВЛЕНИЕ

Пакет обновлений модулей программы «Лаборатории Касперского», в состав которого включены набор срочных обновлений, собранных за некоторый период, и изменения в архитектуре программы.

З

ЗАГРУЗОЧНЫЙ СЕКТОР ДИСКА

Загрузочный сектор – это особый сектор на жестком диске компьютера, дискете или другом устройстве хранения информации. Содержит сведения о файловой системе диска и программу-загрузчик, отвечающую за запуск операционной системы.

Существует ряд вирусов, поражающих загрузочные секторы дисков, которые так и называются – загрузочные вирусы (boot-вирусы). Программа «Лаборатории Касперского» позволяет проверять загрузочные секторы на присутствие вирусов и лечить их в случае заражения.

ЗАДАЧА

Функции, выполняемые программой «Лаборатории Касперского», реализованы в виде задач, например: **Постоянная защита файлов, Полная проверка компьютера, Обновление баз.**

ЗАРАЖЕННЫЙ ОБЪЕКТ

Объект, участок кода которого полностью совпадает с участком кода известной угрозы. Специалисты «Лаборатории Касперского» не рекомендуют вам работать с такими объектами.

И

ИСКЛЮЧЕНИЕ

Исключение – объект, исключаемый из проверки программой «Лаборатории Касперского». Исключать из проверки можно файлы определенного формата, файлы по маске, некоторую область (например, папку или программу), процессы программ или объекты по типу угрозы согласно классификации Вирусной энциклопедии. Для каждой задачи могут быть заданы свои исключения.

К

КАРАНТИН

Специальное хранилище, в которое программа помещает резервные копии файлов, измененных или удаленных во время лечения. Копии файлов хранятся в специальном формате и не представляют опасности для компьютера.

КЛАВИАТУРНЫЙ ПЕРЕХВАТЧИК

Программа, предназначенная для скрытой записи информации о клавишах, нажимаемых пользователем во время работы на компьютере. Клавиатурные перехватчики также называют клавиатурными шпионами или кейлоггерами.

КОД АКТИВАЦИИ

Код, который вы получаете, приобретая коммерческую лицензию Антивируса Касперского. Этот код необходим для активации программы.

Код активации представляет собой последовательность из двадцати латинских букв и цифр, в формате xxxxx-xxxx-xxxx-xxxx.

КОМПОНЕНТЫ ЗАЩИТЫ

Части Антивируса Касперского, предназначенные для защиты компьютера от отдельных типов угроз (например, Анти-Спам, Анти-Фишинг). Каждый компонент защиты относительно независим от других компонентов и может быть отключен или настроен отдельно.

Л

ЛОЖНОЕ СРАБАТЫВАНИЕ

Ситуация, когда незараженный объект определяется программой «Лаборатории Касперского» как зараженный ввиду того, что его код напоминает код вируса.

М

МАСКА ФАЙЛА

Представление имени файла общими символами. Основными символами, используемыми в масках файлов, являются * и ? (где * - любое число любых символов, а ? – любой один символ).

Н

НЕИЗВЕСТНЫЙ ВИРУС

Новый вирус, информации о котором нет в базах. Как правило, неизвестные вирусы обнаруживаются программой в объектах при помощи эвристического анализатора, и таким объектам присваивается статус возможно зараженных.

НЕСОВМЕСТИМАЯ ПРОГРАММА

Антивирусная программа стороннего производителя или программа «Лаборатории Касперского», не поддерживающая управление через Антивирус Касперского.

О

ОБНОВЛЕНИЕ

Процедура замены / добавления новых файлов (баз или программных модулей), получаемых с серверов обновлений «Лаборатории Касперского».

ОБЪЕКТЫ АВТОЗАПУСКА

Набор программ, необходимых для запуска и правильной работы установленных на вашем компьютере операционной системы и программного обеспечения. Каждый раз при старте операционная система запускает эти объекты. Существуют вирусы, способные поражать именно такие объекты, что может привести, например, к блокированию запуска операционной системы.

П

ПАКЕТ ОБНОВЛЕНИЙ

Пакет файлов для обновления модулей программы. Программа «Лаборатории Касперского» копирует пакеты обновлений с серверов обновлений «Лаборатории Касперского», затем автоматически устанавливает и применяет их.

ПАРАМЕТРЫ ЗАДАЧИ

Параметры работы программы, специфичные для каждого типа задач.

ПАРАМЕТРЫ ПРОГРАММЫ

Параметры работы программы, общие для всех типов ее задач и отвечающие за работу программы в целом, например: параметры производительности программы, параметры ведения отчетов, параметры карантина.

ПОТЕНЦИАЛЬНО ЗАРАЖАЕМЫЙ ОБЪЕКТ

Объект, который в силу своей структуры или формата может быть использован злоумышленниками в качестве «контейнера» для размещения и распространения вредоносного кода. Как правило, это исполняемые файлы, например, с расширением com, exe, dll и другими. Риск внедрения в такие файлы вредоносного кода достаточно высок.

ПРОВЕРКА ТРАФИКА

Проверка в режиме реального времени с использованием информации текущей (последней) версии баз объектов, передаваемых по всем протоколам (например, HTTP, FTP и прочим).

ПРОГРАММНЫЕ МОДУЛИ

Файлы, входящие в состав дистрибутива программы «Лаборатории Касперского» и отвечающие за реализацию его основных задач. Каждому типу задач, реализуемых программой (Постоянная защита, Проверка по требованию, Обновление), соответствует свой исполняемый модуль. Запуская из главного окна полную проверку вашего компьютера, вы инициируете запуск модуля этой задачи.

ПРОКСИ-СЕРВЕР

Служба в компьютерных сетях, позволяющая клиентам выполнять косвенные запросы к другим сетевым службам. Сначала клиент подключается к прокси-серверу и запрашивает какой-либо ресурс (например, файл), расположенный на другом сервере. Затем прокси-сервер либо подключается к указанному серверу и получает ресурс у него, либо возвращает ресурс из собственного кеша (в случаях, если прокси имеет свой кеш). В некоторых случаях запрос клиента или ответ сервера может быть изменен прокси-сервером в определенных целях.

ПРОТОКОЛ

Четко определенный и стандартизованный набор правил, регулирующих взаимодействие между клиентом и сервером. К ряду хорошо известных протоколов и связанных с ними служб относятся: HTTP, FTP и NNTP.

Р

РУТКИТ

Программа или набор программ для скрытия следов присутствия злоумышленника или вредоносной программы в системе.

В системах Windows под руткитом принято подразумевать программу, которая внедряется в систему и перехватывает системные функции (Windows API). Перехват и модификация низкоуровневых API-функций, в первую очередь, позволяет такой программе достаточно качественно маскировать свое присутствие в системе. Кроме того, как правило, руткит может маскировать присутствие в системе любых описанных в его конфигурации процессов, каталогов и файлов на диске, ключей в реестре. Многие руткиты устанавливают в систему свои драйверы и службы (они также являются «невидимыми»).

С

СЕРВЕРЫ ОБНОВЛЕНИЙ «ЛАБОРАТОРИИ КАСПЕРСКОГО»

HTTP-серверы «Лаборатории Касперского», с которых программа «Лаборатории Касперского» получает обновления баз и модулей программы.

СКРИПТ

Небольшая компьютерная программа или независимая часть программы (функция), как правило, написанная для выполнения конкретной задачи. Наиболее часто применяется при использовании программ, встраиваемых в гипертекст. Скрипты запускаются, например, когда вы открываете некоторые веб-сайты.

Если включена постоянная защита, программа отслеживает запуск скриптов, перехватывает их и проверяет на присутствие вирусов. В зависимости от результатов проверки вы можете запретить или разрешить выполнение скрипта.

СПАМ

Несанкционированная массовая рассылка электронных сообщений, чаще всего рекламного характера.

СРОК ДЕЙСТВИЯ ЛИЦЕНЗИИ

Срок действия лицензии – период времени, в течение которого вы можете пользоваться функциями программы и дополнительными услугами.

СТЕПЕНЬ УГРОЗЫ

Показатель вероятности, с которой компьютерная программа может представлять угрозу для операционной системы. Степень угрозы вычисляется с помощью эвристического анализа на основании критериев двух типов:

- статических (например, информация об исполняемом файле программы: размер файла, дата создания и тому подобное);
- динамических, которые применяются во время моделирования работы программы в виртуальном окружении (анализ вызовов программой системных функций).

Степень угрозы позволяет выявить поведение, типичное для вредоносных программ. Чем ниже степень угрозы, тем больше действий в системе разрешено программе.

Т

ТЕХНОЛОГИЯ iCHECKER

Технология, позволяющая увеличить скорость антивирусной проверки за счет исключения тех объектов, которые не были изменены с момента предыдущей проверки, при условии, что параметры проверки (базы программы и настройки) не были изменены. Информация об этом хранится в специальной базе. Технология применяется как в режиме постоянной защиты, так и в режиме проверки по требованию.

Например, у вас есть файл архива, который был проверен программой «Лаборатории Касперского» и которому был присвоен статус *не заражен*. В следующий раз этот архив будет исключен из проверки, если он не был изменен и не менялись параметры проверки. Если вы изменили состав архива, добавив в него новый объект, изменили параметры проверки, обновили базы программы, архив будет проверен повторно.

Ограничения технологии iChecker:

- технология не работает с файлами больших размеров, так как в этом случае проверить весь файл быстрее, чем вычислять, был ли он изменен с момента последней проверки;
- технология поддерживает ограниченное число форматов.

ТРАССИРОВКА

Отладочное выполнение программы, при котором после выполнения каждой команды происходит остановка и отображается результат этого шага.

У

УДАЛЕНИЕ ОБЪЕКТА

Способ обработки объекта, при котором происходит его физическое удаление с того места, где он был обнаружен программой (жесткий диск, папка, сетевой ресурс). Такой способ обработки рекомендуется применять к опасным объектам, лечение которых по тем или иным причинам невозможно.

УДАЛЕНИЕ СООБЩЕНИЯ

Способ обработки электронного сообщения, при котором происходит его физическое удаление. Такой способ рекомендуется применять к сообщениям, однозначно содержащим спам или вредоносный объект. Перед удалением сообщения его копия сохраняется в карантине (если данная функциональность не отключена).

УПАКОВАННЫЙ ФАЙЛ

Файл архива, который содержит в себе программу-распаковщик и инструкции операционной системе для ее выполнения.

УРОВЕНЬ БЕЗОПАСНОСТИ

Под уровнем безопасности понимается предустановленный набор параметров работы компонента программы.

Уязвимость

Недостаток в операционной системе или программе, который может быть использован производителями вредоносного программного обеспечения для проникновения в систему или программу и нарушения ее целостности. Большое количество уязвимостей в системе делает ее работу ненадежной, так как внедрившиеся в систему вирусы могут вызывать сбои в работе как самой системы, так и установленных программ.

Ф

Фишинг

Вид интернет-мошенничества, заключающийся в рассылке электронных сообщений с целью кражи конфиденциальной информации, как правило, финансового характера.

Ц

Цифровая подпись

Зашифрованный блок данных, который входит в состав документа или программы. Цифровая подпись используется для идентификации автора документа или программы. Для создания цифровой подписи автор документа или программы должен иметь цифровой сертификат, который подтверждает личность автора.

Цифровая подпись позволяет проверить источник и целостность данных, и защититься от подделки.

Э

Эвристический анализатор

Технология обнаружения угроз, информация о которых еще не занесена в базы «Лаборатории Касперского». Эвристический анализатор позволяет обнаруживать объекты, поведение которых в системе похоже на поведение угроз. Объекты, обнаруженные с помощью эвристического анализатора, признаются возможно зараженными. Например, возможно зараженным может быть признан объект, который содержит последовательности команд, свойственные вредоносным объектам (открытие файла, запись в файл).

ЗАО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

«Лаборатория Касперского» – известный в мире производитель систем защиты компьютеров от угроз: вирусов и других вредоносных программ, нежелательной почты (спама), сетевых и хакерских атак.

В 2008 году «Лаборатория Касперского» вошла в четверку ведущих мировых лидеров рынка программных решений для обеспечения информационной безопасности для конечных пользователей (рейтинг «IDC Worldwide Endpoint Security Revenue by Vendor»). По результатам исследования КОМКОН TGI-Russia 2009, «Лаборатория Касперского» – самый предпочитаемый производитель систем защиты для домашних пользователей в России.

«Лаборатория Касперского» основана в России в 1997 году. Сегодня «Лаборатория Касперского» – это международная группа компаний с центральным офисом в Москве и пятью региональными дивизионами, управляющими деятельностью компании в России, Западной и Восточной Европе, на Ближнем Востоке, в Африке, в Северной и Южной Америке, в Японии, Китае и других странах Азиатско-Тихоокеанского региона. В компании работает более 2000 квалифицированных специалистов.

Продукты. Продукты «Лаборатории Касперского» защищают как домашние компьютеры, так и компьютерные сети организаций.

Линейка персональных продуктов включает антивирусные приложения для настольных компьютеров и ноутбуков, для карманных компьютеров, смартфонов и других мобильных устройств.

Компания предлагает программы и сервисы для защиты рабочих станций, файловых и веб-серверов, почтовых шлюзов, сетевых экранов. Использование этих решений в сочетании с централизованными средствами управления позволяет построить и эксплуатировать эффективную автоматизированную защиту организации от компьютерных угроз. Продукты «Лаборатории Касперского» сертифицированы крупными тестовыми лабораториями, совместимы с программным обеспечением многих поставщиков программного обеспечения и оптимизированы для работы на многих аппаратных платформах.

Вирусные аналитики «Лаборатории Касперского» работают круглосуточно. Каждый день они находят сотни новых компьютерных угроз, создают средства их обнаружения и лечения и включают их в базы, используемые программами «Лаборатории Касперского». *Антивирусная база «Лаборатории Касперского» обновляется ежедневно, база Анти-Спама – каждые 5 минут.*

Технологии. Многие технологии, без которых трудно представить себе современный антивирус, впервые разработаны именно «Лабораторией Касперского». Не случайно программное ядро Антивируса Касперского используют в своих продуктах многие другие разработчики программ: среди них SafeNet (USA), Alt-N Technologies (USA), Blue Coat Systems (USA), Check Point Software Technologies (Israel), Clearswift (UK), CommuniGate Systems (USA), Critical Path (Ireland), D-Link (Taiwan), M86 Security (USA), GFI (Malta), IBM (USA), Juniper Networks (USA), LANDesk (USA), Microsoft (USA), NETASQ (France), NETGEAR (USA), Parallels (Russia), SonicWALL (USA), WatchGuard Technologies (USA), ZyXEL Communications (Taiwan). Многие из инновационных технологий компании подтверждены патентами.

Достижения. За годы борьбы с компьютерными угрозами «Лаборатория Касперского» завоевала сотни наград. Например, в 2010 году Антивирус Касперского получил несколько высших наград Advanced+ в тестах, проведенных авторитетной австрийской антивирусной лабораторией AV-Comparatives. Но главная награда «Лаборатории Касперского» – это приверженность пользователей по всему миру. Продукты и технологии компании защищают более 300 миллионов пользователей. Количество организаций, являющихся ее клиентами, превышает 200 тысяч.

Веб-сайт «Лаборатории Касперского»:

<http://www.kaspersky.ru>

Вирусная энциклопедия:

<http://www.securelist.com/ru/>

Антивирусная лаборатория:

newvirus@kaspersky.com (только для отправки возможно зараженных файлов в архивированном виде)

<http://support.kaspersky.ru/virlab/helpdesk.html>

(для запросов вирусным аналитикам)

Веб-форум «Лаборатории Касперского»:

<http://forum.kaspersky.com>

ИНФОРМАЦИЯ О СТОРОННЕМ КОДЕ

Информация о стороннем коде содержится в файле legal_notices.txt, расположенном в папке установки программы.

УВЕДОМЛЕНИЯ О ТОВАРНЫХ ЗНАКАХ

Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.

Google Chrome – товарный знак Google, Inc.

Intel и Pentium – товарные знаки Intel Corporation, зарегистрированные в Соединенных Штатах Америки и в других странах.

Microsoft, Windows, Windows Vista и Internet Explorer – товарные знаки Microsoft Corporation, зарегистрированные в Соединенных Штатах Америки и в других странах.

Mozilla и Firefox – товарные знаки Mozilla Foundation.

ПРЕДМЕТНЫЙ УКАЗАТЕЛЬ

К

Kaspersky Gadget.....	53
Kaspersky Security Network	54

А

Активация программы	27
код активации.....	24
лицензия.....	23
пробная версия	17, 56
Анализ безопасности	29
Анти-Фишинг	38
Аппаратные требования	13

Б

Базы программы.....	30
---------------------	----

В

Веб-Антивирус	
Веб-фильтр	44
модуль проверки ссылок.....	44
Виртуальная клавиатура.....	39
Восстановление параметров по умолчанию	50
Восстановление после заражения	33
Вылеченный объект	32

Г

Гаджет	53
--------------	----

Д

Диагностика	29
Диск аварийного восстановления	45
Дополнительные инструменты	
восстановление после заражения.....	33
диск аварийного восстановления.....	45
устранение следов активности	42

Ж

Журнал событий.....	50
---------------------	----

З

ЗАО.....	69
Зараженный объект.....	64

И

Игровой профиль.....	45
Импорт / экспорт параметров	52
Источник обновлений.....	30

К

Карантин	
восстановление объекта	32
Клавиатурные перехватчики	
виртуальная клавиатура	39
защита ввода с аппаратной клавиатуры	41
Ключ	23
Код активации	24
Компоненты программы	12
Конфиденциальные данные	37

Л

ЛАБОРАТОРИЯ КАСПЕРСКОГО	69
Лицензионное соглашение	23
Лицензия	23
код активации	24
Лицензионное соглашение	23

М

Модуль проверки ссылок	
Веб-Антивирус	44

О

Обновление	30
Ограничение доступа к программе	48
Отчеты	50

П

Поиск уязвимостей	36
Полноэкранный режим работы программ	45
Почтовый Антивирус	35
Проблемы безопасности	29
Программные требования	13
Просмотр статистики	50

С

Состояние защиты	29
Статистика	50
Статус защиты	29

Т

Трассировка	
загрузка результатов трассировки	61

У

Уведомления	28
Угрозы безопасности	29
Удаление программы	21
УСТАНОВКА ПРОГРАММЫ	15
Уязвимость	36