KASPERSKY lab

Kaspersky Total Security

Руководство пользователя

Версия программы: 16.0 Maintenance Release 1

Уважаемый пользователь!

Спасибо за то, что выбрали наш продукт. Мы надеемся, что этот документ поможет вам в работе и ответит на большинство возникающих вопросов.

Документ и связанные с ним графические изображения могут быть использованы только в информационных, некоммерческих или личных целях.

Документ может быть изменен без предварительного уведомления. Последнюю версию документа вы можете найти на сайте «Лаборатории Касперского» по адресу http://www.kaspersky.ru/docs.

Дата редакции документа: 30.11.2015

http://www.kaspersky.ru
https://help.kaspersky.com
http://support.kaspersky.ru

Содержание

Об этом руководстве

Этот документ представляет собой Руководство пользователя Kaspersky Total Security.

Для успешного использования Kaspersky Total Security пользователям нужно быть знакомым с интерфейсом используемой операционной системы, владеть основными приемами работы в ней, уметь работать с электронной почтой и интернетом.

Руководство предназначено для следующих целей:

- Помочь установить Kaspersky Total Security, активировать и использовать программу.
- Обеспечить быстрый поиск информации для решения вопросов, связанных с работой Kaspersky Total Security.
- Рассказать о дополнительных источниках информации о программе и способах получения технической поддержки.

В этом разделе

В этом документе

Этот документ содержит следующие разделы.

Источники информации о программе (см. стр. 16)

Этот раздел содержит описание источников информации о программе.

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

Kaspersky Total Security (см. стр. 19)

Этот раздел содержит описание функций, компонентов и комплекта поставки Kaspersky Total Security, перечень аппаратных и программных требований Kaspersky Total Security.

Установка и удаление программы (см. стр. 28)

Этот раздел содержит пошаговые инструкции по установке и удалению Kaspersky Total Security.

Лицензирование программы (см. стр. 45)

Этот раздел содержит информацию об основных понятиях, связанных с лицензированием программы.

Работа с уведомлениями программы (см. стр. 57)

Этот раздел содержит информацию о работе с уведомлениями программы.

Анализ состояния защиты компьютера и устранение проблем безопасности (см. стр. 58)

Этот раздел содержит информацию о том, как проверить состояние защиты компьютера и устранить проблемы безопасности.

Обновление баз и программных модулей (см. стр. 59)

Этот раздел содержит пошаговые инструкции по обновлению баз и программных модулей.

Проверка компьютера (см. стр. 62)

Этот раздел содержит пошаговые инструкции по проверке компьютера на вирусы, вредоносные программы и уязвимости.

Восстановление удаленного или вылеченного программой объекта (см. стр. 66)

Этот раздел содержит пошаговые инструкции о том, как восстановить удаленный или вылеченный объект.

Восстановление операционной системы после заражения (см. стр. 67)

Этот раздел содержит информацию о восстановлении операционной системы после заражения вирусами.

Защита электронной почты (см. стр. 71)

Этот раздел содержит информацию о том, как защитить электронную почту от спама, вирусов и других программ, представляющих угрозу.

Защита персональных данных в интернете (см. стр. 74)

Этот раздел содержит информацию о том, как сделать работу в интернете безопасной и защитить ваши данные от кражи.

Защита финансовых операций и покупок в интернете (см. стр. 86)

Этот раздел содержит информацию о том, как вы можете защитить свои финансовые операции и покупки в интернете с помощью Kaspersky Total Security.

Защита от сбора информации о ваших действиях в интернете (см. стр. 94)

Этот раздел содержит информацию о том, как с помощью Kaspersky Total Security защитить вас от сбора информации о ваших действиях в интернете.

Защита от баннеров при посещении веб-сайтов (см. стр. 100)

Этот раздел содержит информацию о том, как с помощью Kaspersky Total Security блокировать отображение баннеров на веб-сайтах.

Устранение следов работы на компьютере и в интернете (см. стр. 103)

Этот раздел содержит информацию об удалении следов активности пользователя с компьютера.

Контроль работы пользователей на компьютере и в интернете (см. стр. 106)

Этот раздел содержит информацию о том, как с помощью Kaspersky Total Security контролировать действия пользователей на компьютере и в интернете.

Удаленное управление защитой компьютера (см. стр. 119)

Этот раздел содержит информацию о том, как удаленно управлять защитой вашего компьютера через портал My Kaspersky.

Сохранение ресурсов операционной системы для компьютерных игр (см. стр. 122)

Этот раздел содержит инструкцию о том, как повысить производительность операционной системы для компьютерных игр и других программ.

Работа с неизвестными программами (см. стр. 123)

Этот раздел содержит информацию о предотвращении несанкционированных действий программ на компьютере.

Режим Безопасных программ (см. стр. 137)

Этот раздел содержит информацию о режиме Безопасных программ.

Удаление данных без возможности восстановления (см. стр. 141)

Этот раздел содержит информацию о том, как с помощью Kaspersky Total Security удалить данные, чтобы злоумышленники не могли восстановить их.

Удаление неиспользуемых данных (см. стр. 144)

Этот раздел содержит информацию об удалении временных и неиспользуемых файлов.

Резервное копирование данных (см. стр. 147)

Этот раздел содержит информацию о том, как с помощью Kaspersky Total Security выполнять резервное копирование данных.

Хранение данных в сейфах (см. стр. 157)

Этот раздел содержит информацию о том, как защитить файлы и папки на вашем компьютере с помощью сейфов.

Защита доступа к управлению Kaspersky Total Security с помощью пароля (см. стр. 160)

Этот раздел содержит инструкцию по защите параметров программы с помощью пароля.

Приостановка и возобновление защиты компьютера (см. стр. 161)

Этот раздел содержит пошаговые инструкции по включению и выключению программы.

Восстановление стандартных параметров работы программы (см. стр. 163)

Этот раздел содержит инструкцию о том, как восстановить стандартные параметры работы программы.

Просмотр отчета о работе программы (см. стр. 164)

Этот раздел содержит инструкцию о том, как просмотреть отчеты о работе программы.

Применение параметров программы на другом компьютере (см. стр. 165)

Этот раздел содержит информацию о том, как экспортировать параметры программы и применить их на другом компьютере.

Участие в Kaspersky Security Network (см. стр. 167)

Этот раздел содержит информацию о том, что такое Kaspersky Security Network, и как принять участие в программе Kaspersky Security Network.

Работа с программой из командной строки (см. стр. 170)

Этот раздел содержит информацию об управлении программой с помощью командной строки.

Обращение в Службу технической поддержки (см. стр. 171)

Этот раздел содержит информацию о способах и условиях получения технической поддержки.

Ограничения и предупреждения (см. стр. 178)

Этот раздел содержит информацию о некритичных для работы программы ограничениях.

Глоссарий (см. стр. 185)

Этот раздел содержит список терминов, которые встречаются в тексте документа, а также определения этих терминов.

АО «Лаборатория Касперского» (см. стр. 196)

Этот раздел содержит информацию о АО «Лаборатория Касперского».

Информация о стороннем коде (см. стр. 198)

Этот раздел содержит информацию о стороннем коде, используемом в программе.

Уведомления о товарных знаках (см. стр. 199)

В этом разделе перечислены товарные знаки сторонних правообладателей, использованные в документе.

Предметный указатель

Этот раздел позволяет быстро найти необходимые сведения в документе.

Условные обозначения

В этом документе используются условные обозначения (см. таблицу ниже).

Таблица 1. Условные обозначения

Пример текста	Описание условного обозначения
Обратите внимание на то, что...	Предупреждения выделены красным цветом и заключены в рамку. Предупреждения содержат информацию о действиях, которые могут иметь нежелательные последствия.
Рекомендуется использовать...	Примечания заключены в рамку. Примечания содержат дополнительную и справочную информацию.
Пример:	Примеры приведены в блоках на голубом фоне под заголовком «Пример».
Обновление – это... Возникает событие *Базы устарели*.	Курсивом выделены следующие элементы текста: • новые термины; • названия статусов и событий программы.

Пример текста	Описание условного обозначения
Нажмите на клавишу **ENTER**. Нажмите комбинацию клавиш **ALT**+**F4**.	Названия клавиш клавиатуры выделены полужирным шрифтом и прописными буквами. Названия клавиш, соединенные знаком + (плюс), означают комбинацию клавиш. Такие клавиши требуется нажимать одновременно.
Нажмите на кнопку **Включить**.	Названия элементов интерфейса программы, например, полей ввода, пунктов меню, кнопок, выделены полужирным шрифтом.
► *Чтобы настроить расписание задачи, выполните следующие действия:*	Вводные фразы инструкций выделены курсивом и значком «стрелка».
В командной строке введите текст `help` Появится следующее сообщение: `Укажите дату в формате ДД:ММ:ГГ.`	Специальным стилем выделены следующие типы текста: • текст командной строки; • текст сообщений, выводимых программой на экран; • данные, которые требуется ввести с клавиатуры.
<Имя пользователя>	Переменные заключены в угловые скобки. Вместо переменной требуется подставить соответствующее ей значение, опустив угловые скобки.

Источники информации о программе

Этот раздел содержит описание источников информации о программе.

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

В этом разделе

Источники для самостоятельного поиска информации

Вы можете использовать следующие источники для самостоятельного поиска информации о Kaspersky Total Security:

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

Если вы не нашли решения возникшей проблемы самостоятельно, обратитесь в Службу технической поддержки «Лаборатории Касперского» (см. раздел «Обращение в Службу технической поддержки» на стр. 171).

Для использования источников информации на веб-сайтах требуется подключение к интернету.

Страница Kaspersky Total Security на веб-сайте «Лаборатории Касперского»

На странице Kaspersky Total Security (http://www.kaspersky.ru/total-security-multi-device) вы можете получить общую информацию о программе, ее возможностях и особенностях работы.

Страница Kaspersky Total Security содержит ссылку на интернет-магазин. В нем вы можете приобрести программу или продлить право пользования программой.

Страница Kaspersky Total Security в Базе знаний

База знаний – это раздел веб-сайта Службы технической поддержки.

На странице Kaspersky Total Security в Базе знаний (http://support.kaspersky.ru/kts2016) вы найдете статьи, которые содержат полезную информацию, рекомендации и ответы на часто задаваемые вопросы о приобретении, установке и использовании программы.

Статьи Базы знаний могут отвечать на вопросы, которые относятся не только к Kaspersky Total Security, но и к другим программам «Лаборатории Касперского». Статьи Базы знаний также могут содержать новости Службы технической поддержки.

Электронная справка

Программа содержит файлы полной и контекстной справки.

В полной справке вы можете найти информацию о настройке и использовании Kaspersky Total Security.

В контекстной справке вы можете найти информацию об окнах Kaspersky Total Security: описание параметров Kaspersky Total Security и ссылки на описания задач, в которых используются эти параметры.

Справка может быть включена в состав программы либо располагаться онлайн на веб-ресурсе «Лаборатории Касперского». Если справка расположена онлайн, то при ее вызове будет открыто окно браузера. Для отображения онлайн-справки требуется соединение с интернетом.

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.

Kaspersky Total Security

Этот раздел содержит описание функций, компонентов и комплекта поставки Kaspersky Total Security, перечень аппаратных и программных требований Kaspersky Total Security.

В этом разделе

Что нового

В Kaspersky Total Security появились следующие новые возможности:

- Сняты ограничения поддержки Microsoft® Windows® 10.
- Добавлены уведомления об истечении срока действия лицензии по стандарту Microsoft.
- В операционной системе Microsoft Windows 10 уведомления программы заменены на всплывающие сообщения по стандарту Microsoft.
- Программа «Защити друга» перенесена на портал My Kaspersky. Регистрация и вход в программу «Защити друга» теперь выполняется при подключении к порталу My Kaspersky. Просмотр страниц программы «Защити друга» выполняется на портале My Kaspersky.
- Добавлена поддержка протокола HTTP/2.
- Добавлена частичная поддержка браузеров Яндекс.Браузер и Microsoft Edge.
- Добавлена поддержка виртуальных рабочих столов в Microsoft Windows 10.

- Улучшен графический интерфейс.
- Улучшен значок Экранной клавиатуры. Значок больше не мешает вводить данные в поля ввода.
- Добавлен помощник по установке. При установке программного обеспечения на компьютер помощник по установке автоматически снимает флажки напротив предложений об установке дополнительных программ и блокирует установку этих программ, а также отключает отображение шагов установки, содержащих рекламу.

Комплект поставки

Вы можете приобрести программу одним из следующих способов:

- В коробке. Распространяется через магазины наших партнеров.
- Через интернет-магазин. Распространяется через интернет-магазины «Лаборатории Касперского» (например, http://www.kaspersky.ru, раздел «Интернет-магазин») или компаний-партнеров.

Если вы приобретаете программу в коробке, в комплект поставки входят следующие компоненты:

- запечатанный конверт с установочным компакт-диском, на котором записаны файлы программы и файлы документации к программе;
- краткое руководство пользователя, содержащее код активации программы;
- Лицензионное соглашение, в котором указано, на каких условиях вы можете пользоваться программой.

> Состав комплекта поставки может быть различным в зависимости от региона, в котором распространяется программа.

Если вы приобретаете Kaspersky Total Security через интернет-магазин, вы копируете программу с сайта интернет-магазина. Информация, необходимая для активации программы, в том числе код активации, высылается вам по электронной почте после оплаты.

О программе Kaspersky Total Security

Kaspersky Total Security обеспечивает комплексную защиту от различных видов информационных угроз, сетевых и мошеннических атак, а также спама. Для решения задач комплексной защиты в составе Kaspersky Total Security предусмотрены различные функции и компоненты защиты.

Защита компьютера

Компоненты защиты предназначены для защиты компьютера от различных видов информационных угроз, сетевых атак, мошенничества, а также спама. Каждый тип угроз обрабатывается отдельным компонентом защиты (см. описание компонентов далее в этом разделе). Вы можете включать и выключать компоненты защиты независимо друг от друга, а также настраивать их работу.

В дополнение к постоянной защите, реализуемой компонентами защиты, рекомендуется периодически выполнять *проверку* вашего компьютера на присутствие вирусов и других программ, представляющих угрозу. Это необходимо делать для того чтобы исключить возможность распространения вредоносных программ, которые не были обнаружены компонентами защиты, например, из-за установленного низкого уровня защиты или по другим причинам.

Для поддержки Kaspersky Total Security в актуальном состоянии необходимо *обновление* баз и программных модулей, используемых в работе программы.

Некоторые специфические задачи, которые требуется выполнять эпизодически (например, устранение следов активности пользователя в операционной системе), выполняются с помощью *дополнительных инструментов и мастеров*.

Защиту вашего компьютера в реальном времени обеспечивают следующие компоненты защиты:

> Ниже описана работа компонентов защиты в режиме работы Kaspersky Total Security, рекомендованном специалистами «Лаборатории Касперского» (то есть при параметрах работы программы, заданных по умолчанию).

Файловый Антивирус

Файловый Антивирус позволяет избежать заражения файловой системы компьютера. Компонент запускается при старте операционной системы, постоянно находится в оперативной памяти компьютера и проверяет все открываемые, сохраняемые и запускаемые файлы на вашем компьютере и на всех присоединенных дисках. Kaspersky Total Security перехватывает каждое обращение к файлу и проверяет этот файл на присутствие известных вирусов и других программ, представляющих угрозу. Дальнейшая работа с файлом возможна только в том случае, если файл не заражен или был успешно вылечен программой. Если файл по каким-либо причинам невозможно вылечить, он будет удален. При этом копия файла будет помещена на карантин. Если на место удаленного файла поместить зараженный файл с таким же именем, в карантине сохраняется только копия последнего файла. Копия предыдущего файла с таким же именем не сохраняется.

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 IM-клиентами. Компонент защищает информацию, поступающую на ваш компьютер по протоколам IM-клиентов. IM-Антивирус обеспечивает безопасную работу со многими программами, предназначенными для обмена мгновенными сообщениями.

Контроль программ

Контроль программ регистрирует действия, совершаемые программами в операционной системе, и регулирует деятельность программ, исходя из того, к каким группам компонент относит эти программы. Для каждой группы программ задан набор правил. Эти правила регламентируют доступ программ к различным ресурсам операционной системы.

Контроль изменений в операционной системе

Компонент Контроль изменений в операционной системе контролирует изменения, которые вносят в параметры операционной системы другие программы, и уведомляет вас о таких изменениях. К контролируемым параметрам относятся, например, некоторые параметры браузера или параметры прокси-сервера.

Доступ к веб-камере

Компонент Доступ к веб-камере блокирует несанкционированный доступ программ к веб-камере и показывает уведомление о том, что доступ заблокирован.

Сетевой экран

Сетевой экран обеспечивает безопасность вашей работы в локальных сетях и в интернете. Компонент фильтрует всю сетевую активность согласно правилам двух типов: *правилам для программ* и *пакетным правилам*.

Мониторинг сети

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

Мониторинг активности

Компонент Мониторинг активности позволяет откатить в операционной системе действия вредоносных программ.

Защита от сетевых атак

Компонент Защита от сетевых атак запускается при старте операционной системы и отслеживает во входящем трафике активность, характерную для сетевых атак. Обнаружив попытку атаки на компьютер, Kaspersky Total Security блокирует любую сетевую активность атакующего компьютера в отношении вашего компьютера.

Анти-Спам

Анти-Спам встраивается в установленный на вашем компьютере почтовый клиент и проверяет все входящие почтовые сообщения на наличие спама. Все письма, содержащие спам, помечаются специальным заголовком. Вы можете настраивать действия Анти-Спама с письмами, содержащими спам (например, автоматическое удаление, помещение в специальную папку).

Анти-Фишинг

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

Анти-Баннер

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

Защита от сбора данных

Компонент Защита от сбора данных обнаруживает запросы, отправляемые браузером на сервисы отслеживания, и может модифицировать запросы на сервисы отслеживания и ответы от них таким образом, чтобы защитить вас от сбора информации о ваших действиях в интернете.

Безопасные платежи

Безопасные платежи обеспечивают защиту конфиденциальных данных при работе с сервисами интернет-банкинга и платежными системами, а также предотвращают кражу платежных средств при проведении платежей онлайн.

Безопасный ввод данных

Защита ввода данных с аппаратной клавиатуры обеспечивает защиту персональных данных, вводимых на веб-сайтах, от клавиатурных перехватчиков. Экранная клавиатура позволяет избежать перехвата данных, вводимых через аппаратную клавиатуру, и защищает персональные данные от перехвата посредством снятия снимков экрана.

Режим Безопасных программ

Режим Безопасных программ обеспечивает защиту компьютера от запуска программ, которые могут быть небезопасными. В режиме Безопасных программ разрешен запуск только тех программ, которые Kaspersky Total Security считает доверенными (например, на основании информации о программе из Kaspersky Security Network, доверия к цифровой подписи).

Родительский контроль

Для защиты детей и подростков от угроз, связанных с работой на компьютере и в интернете, предназначены функции Родительского контроля.

Родительский контроль позволяет установить гибкие ограничения доступа к интернет-ресурсам и программам для разных пользователей компьютера в зависимости от их возраста. Кроме того, Родительский контроль позволяет просматривать статистические отчеты о действиях контролируемых пользователей.

Управление в интернете

Если на компьютере установлена программа Kaspersky Total Security, и у вас есть учетная запись на портале My Kaspersky, вы можете управлять защитой этого компьютера удаленно.

Резервное копирование

Функциональность резервного копирования предназначена для защиты ваших данных от потери в результате сбоев в работе оборудования. Kaspersky Total Security позволяет выполнять резервное копирование на съемные диски, сетевые и онлайн-хранилища по расписанию. Вы можете копировать файлы по категориям, а также указывать количество хранимых версий одного и того же файла.

Виртуальные сейфы

Для защиты ваших конфиденциальных данных от несанкционированного доступа предназначены виртуальные сейфы. Открыть сейф и просмотреть данные можно только после ввода пароля.

Аппаратные и программные требования

Общие требования:

- 480 МБ свободного места на жестком диске.
- CD- / DVD-ROM (для установки с установочного CD-диска).
- Подключение к интернету (для установки и активации программы, а также обновления баз и программных модулей).

- Microsoft® Internet Explorer® 8.0 или выше.

  > Для работы с порталом My Kaspersky рекомендуется использовать Microsoft Internet Explorer 9.0 или выше.

- Microsoft Windows® Installer 3.0 или выше.
- Microsoft .NET Framework 4 или выше.
- Защита от несанкционированного доступа к веб-камере предоставляется только для совместимых моделей веб-камер (http://support.kaspersky.ru/12004).

Требования для операционных систем Microsoft Windows XP Home Edition (Service Pack 3 или выше), Microsoft Windows XP Professional (Service Pack 3 или выше), Microsoft Windows XP Professional x64 Edition (Service Pack 2 или выше):

- процессор 1 ГГц или выше;
- 512 МБ свободной оперативной памяти.

Требования для операционных систем Microsoft Windows Vista® Home Basic (Service Pack 1 или выше), Microsoft Windows Vista Home Premium (Service Pack 1 или выше), Microsoft Windows Vista Business (Service Pack 1 или выше), Microsoft Windows Vista Enterprise (Service Pack 1 или выше), Microsoft Windows Vista Ultimate (Service Pack 1 или выше), Microsoft Windows 7 Starter (Service Pack 1 или выше), Microsoft Windows 7 Home Basic (Service Pack 1 или выше), Microsoft Windows 7 Home Premium (Service Pack 1 или выше), Microsoft Windows 7 Professional (Service Pack 1 или выше), Microsoft Windows 7 Ultimate (Service Pack 1 или выше), Microsoft Windows 8, Microsoft Windows 8 Pro, Microsoft Windows 8 Enterprise, Microsoft Windows 8.1 (Windows 8.1 Update), Microsoft Windows 8.1 Pro (Windows 8.1 Update), Microsoft Windows 8.1 Enterprise (Windows 8.1 Update), Microsoft Windows 10 Home, Microsoft Windows 10 Enterprise, Microsoft Windows 10 Pro:

- процессор 1 ГГц или выше;
- 1 ГБ свободной оперативной памяти (для 32-разрядной операционной системы), 2 ГБ свободной оперативной памяти (для 64-разрядной операционной системы).

Поддерживаемые браузеры:

- Microsoft Internet Explorer версий 8.0, 9.0, 10.0, 11.0.

  > Браузеры Internet Explorer 10 и Internet Explorer 11 в стиле нового интерфейса Windows не поддерживаются.

- Mozilla™ Firefox™ версий 31.x и выше.
- Google Chrome™ версий 36.x и выше.

  > Kaspersky Total Security поддерживает работу с браузером Google Chrome версий 37.x и 38.x как в 32-разрядной, так и в 64-разрядной операционной системе.

Требования для планшетных компьютеров:

- Microsoft Tablet PC;
- процессор Intel® Celeron® 1.66 ГГц или выше;
- 1000 МБ свободной оперативной памяти.

Требования для нетбуков:

- процессор Intel Atom™ 1600 МГц или выше;
- 1024 МБ свободной оперативной памяти;
- дисплей 10.1 дюймов с разрешением 1024x600;
- графический чипсет Intel GMA 950.

Требования для программы Kaspersky Password Manager при установке на Microsoft Windows XP Home (32-разрядная) Service Pack 3 или выше, Microsoft Windows XP Professional (32-разрядная) Service Pack 3 или выше, Microsoft Windows XP Professional (64-разрядная) Service Pack 2 или выше:

- Microsoft Internet Explorer (версия 8 или выше);
- Mozilla Firefox 31 или выше;
- Google Chrome 36 или выше;
- Яндекс.Браузер 14.10 или выше.

Установка и удаление программы

Этот раздел содержит пошаговые инструкции по установке и удалению Kaspersky Total Security.

В этом разделе

Стандартная процедура установки

Kaspersky Total Security 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 шаге установки следует закрыть окно мастера.

> Если программа будет использована для защиты более чем одного компьютера (максимально допустимое количество компьютеров определяется условиями Лицензионного соглашения), то процедура установки будет одинаковой на всех компьютерах.

► *Чтобы установить Kaspersky Total Security на ваш компьютер,*

на установочном диске запустите файл с расширением exe.

Далее установка программы выполняется с помощью стандартного мастера установки.

В некоторых регионах установочный диск не содержит установочного пакета программы. На установочном диске содержится только файл autorun, при запуске которого открывается окно загрузки программы.

► *Чтобы установить Kaspersky Total Security с помощью файла autorun, выполните следующие действия:*

1. В окне загрузки программы нажмите на кнопку **Загрузить и установить**.

   При нажатии на кнопку **Загрузить и установить** в «Лабораторию Касперского» отправляется информация о версии вашей операционной системы.

2. Если выполнить загрузку не удалось, по ссылке **Загрузить и установить вручную с веб-сайта** перейдите на веб-страницу и загрузите программу вручную.

Для установки Kaspersky Total Security вы также можете самостоятельно загрузить установочный пакет из интернета. При этом для некоторых языков локализации мастер установки отображает несколько дополнительных шагов установки.

Вместе с программой устанавливаются расширения для браузеров, обеспечивающие безопасную работу в интернете.

При первом запуске программы Kaspersky Total Security с момента ее установки воспроизведение или запись аудио и видео могут быть прерваны в программах записи или воспроизведения аудио и видео. Это необходимо для того, чтобы включилась функциональность контроля доступа программ к устройствам записи звука (см. раздел «О доступе программ к устройствам записи звука» на стр. 132). Системная служба управления средствами работы со звуком будет перезапущена при первом запуске программы Kaspersky Total Security.

В этом разделе

Шаг 1. Поиск более новой версии программы

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

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

Если мастер обнаружит на серверах обновлений «Лаборатории Касперского» более актуальную версию Kaspersky Total Security, 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 установочного пакета на ваш компьютер и запустит установку новой версии.

Шаг 2. Начало установки программы

На этом шаге мастер установки предлагает вам установить программу.

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

В зависимости от типа установки и языка локализации на этом шаге 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 Kaspersky Total Security с установочного пакета, полученного через интернет.

На этом шаге 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 условия Лицензионного соглашения не приняты, установка программы не производится.

Шаг 4. Положение о Kaspersky Security Network

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

Ознакомьтесь с Положением о Kaspersky Security Network. Если вы согласны со всеми его пунктами, в окне мастера нажмите на кнопку **Принять**.

Если вы не хотите принимать участие в программе Kaspersky Security Network, нажмите на кнопку **Отказаться**.

После принятия или отказа от участия в Kaspersky Security Network установка программы продолжится.

Шаг 5. Установка

Для некоторых версий Kaspersky Total Security, распространяемых по подписке, перед установкой требуется ввести пароль, предоставленный поставщиком услуг.

После ввода пароля начинается установка программы.

Установка программы занимает некоторое время. Дождитесь ее завершения.

По завершении установки мастер автоматически переходит к следующему шагу.

Во время установки Kaspersky Total Security 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;
  - наличие прав администратора у пользователя, выполняющего установку программы.

  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 Kaspersky Total Security не может удалить автоматически, необходимо удалить вручную. Во время удаления несовместимых программ потребуется перезагрузка операционной системы, после чего установка Kaspersky Total Security продолжится автоматически.

- *Наличие на компьютере вредоносных программ*. При обнаружении на компьютере вредоносных программ, 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 шаге мастер информирует вас о завершении установки программы.

Чтобы начать работу с Kaspersky Total Security немедленно, убедитесь, что флажок **Запустить Kaspersky Total Security** установлен, и нажмите на кнопку **Завершить**.

Если перед завершением работы мастера вы сняли флажок **Запустить Kaspersky Total Security**, программу нужно запустить вручную.

В некоторых случаях для завершения установки может потребоваться перезагрузка операционной системы.

Шаг 7. Активация программы

При первом запуске Kaspersky Total Security запускается мастер активации программы.

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

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

Вам предлагаются следующие варианты активации Kaspersky Total Security:

- **Активировать программу**. Выберите этот вариант и введите код активации (см. раздел «О коде активации» на стр. 51), если вы приобрели лицензию на использование программы.

  Если в поле ввода вы укажете код активации Kaspersky Internet Security или Kaspersky Anti-Virus, по завершении активации запустится процедура перехода на Kaspersky Internet Security или Kaspersky Anti-Virus.

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

Для активации программы необходимо подключение к интернету.

В процессе активации программы может потребоваться пройти регистрацию на портале My Kaspersky.

Шаг 8. Регистрация пользователя

Этот шаг доступен не во всех версиях Kaspersky Total Security.

Зарегистрированные пользователи получают возможность отправлять запросы в Службу технической поддержки и Вирусную Лабораторию через портал My Kaspersky, возможность удобно управлять кодами активации, а также получают оперативную информацию о новых программах и специальных предложениях «Лаборатории Касперского».

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

В некоторых случаях регистрация пользователя необходима для использования программы.

Шаг 9. Завершение активации

Мастер информирует вас об успешном завершении активации Kaspersky Total Security.

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

Установка программы из командной строки

Вы можете установить Kaspersky Total Security с помощью командной строки.

Синтаксис командной строки:

```
<путь к файлу установочного пакета> [параметры]
```

Подробная инструкция и перечень параметров установки приведены на сайте Службы технической поддержки (http://support.kaspersky.ru/12003).

Подготовка программы к работе

Для полноценной поддержки браузеров программой Kaspersky Total Security в браузерах должно быть установлено и включено расширение Kaspersky Protection. Kaspersky Total Security с помощью расширения Kaspersky Protection внедряет в веб-страницу, открытую в Защищенном браузере, и в трафик скрипт. Программа использует этот скрипт для взаимодействия с веб-страницей и для передачи данных в банки, чьи веб-сайты защищаются с помощью компонента Безопасные платежи. Программа защищает передаваемые скриптом данные с помощью цифровой подписи. Kaspersky Total Security может внедрять скрипт без использования расширения Kaspersky Protection.

Kaspersky Total Security подписывает передаваемые скриптом данные с помощью установленных антивирусных баз и запросов в Kaspersky Security Network. Программа передает запросы в Kaspersky Security Network независимо от того, приняли вы условия Положения о Kaspersky Security Network или нет.

Расширение Kaspersky Protection устанавливается в браузеры одновременно с установкой Kaspersky Total Security.

После установки Kaspersky Total Security требуется включить расширение Kaspersky Protection:

- В браузере Mozilla™ Firefox™ для включения расширения требуется разрешить его установку в окне браузера.
- В браузере Google Chrome™ требуется разрешить включение Kaspersky Protection. В случае отказа от включения расширения в дальнейшем потребуется установить и включить Kaspersky Protection самостоятельно, загрузив его из интернет-магазина Chrome™ или со страницы на веб-сайте Службы технической поддержки (http://support.kaspersky.com/interactive/google/ru/kis2016plugin).

В браузере Microsoft Internet Explorer расширение Kaspersky Protection включается автоматически.

Если ваш компьютер работает под управлением операционной системы Windows 10, в браузере Microsoft Internet Explorer требуется установить расширение Kaspersky Protection вручную. Вы можете перейти к установке расширения с помощью информационного сообщения в Центре уведомлений (см. раздел «Анализ состояния защиты компьютера и устранение проблем безопасности» на стр. 58).

Обновление предыдущей версии программы

Установка Kaspersky Total Security поверх Kaspersky Total Security предыдущей версии или поверх Kaspersky CRYSTAL

Если на вашем компьютере уже установлена программа Kaspersky Total Security предыдущей версии или программа Kaspersky CRYSTAL, вы можете обновить ее до Kaspersky Total Security новой версии. При наличии действующей лицензии на использование Kaspersky CRYSTAL или предыдущей версии Kaspersky Total Security вам не понадобится активировать программу: мастер установки автоматически получит информацию о лицензии и применит ее во время установки Kaspersky Total Security.

Если вы создавали контейнер в Kaspersky CRYSTAL, то при первом обращении к контейнеру Kaspersky Total Security преобразует контейнер в сейф. Файлы в сейфе станут доступны по завершении преобразования.

Установка Kaspersky Total Security поверх Kaspersky Internet Security

Если вы устанавливаете Kaspersky Total Security на компьютер, на котором уже установлена программа Kaspersky Internet Security с действующей лицензией, мастер активации 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 установлена программа Kaspersky Internet Security. Вы сможете использовать Kaspersky Internet Security в течение срока действия лицензии на использование Kaspersky Internet Security предыдущей версии.
- Продолжить установку новой версии Kaspersky Total Security. В этом случае программа будет установлена и активирована согласно стандартному сценарию.

Kaspersky Total Security 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 шаге установки следует закрыть окно мастера.

Если программа будет использована для защиты более чем одного компьютера (максимально допустимое количество компьютеров определяется условиями Лицензионного соглашения), то процедура установки будет одинаковой на всех компьютерах.

► *Чтобы установить Kaspersky Total Security на ваш компьютер,*

на установочном диске запустите файл с расширением exe.

Далее установка программы выполняется с помощью стандартного мастера установки.

В некоторых регионах установочный диск не содержит установочного пакета программы. На установочном диске содержится только файл autorun, при запуске которого открывается окно загрузки программы.

► *Чтобы установить Kaspersky Total Security с помощью файла autorun, выполните следующие действия:*

1. В окне загрузки программы нажмите на кнопку **Загрузить и установить**.

   При нажатии на кнопку **Загрузить и установить** в «Лабораторию Касперского» отправляется информация о версии вашей операционной системы.

2. Если выполнить загрузку не удалось, по ссылке **Загрузить и установить вручную с веб-сайта** перейдите на веб-страницу и загрузите программу вручную.

Для установки Kaspersky Total Security вы также можете самостоятельно загрузить установочный пакет из интернета. При этом для некоторых языков локализации мастер установки отображает несколько дополнительных шагов установки.

Вместе с программой устанавливаются расширения для браузеров, обеспечивающие безопасную работу в интернете.

При первом запуске программы Kaspersky Total Security с момента ее установки воспроизведение или запись аудио и видео могут быть прерваны в программах записи или воспроизведения аудио и видео. Это необходимо для того, чтобы включилась функциональность контроля доступа программ к устройствам записи звука (см. раздел «О доступе программ к устройствам записи звука» на стр. 132). Системная служба управления средствами работы со звуком будет перезапущена при первом запуске программы Kaspersky Total Security.

Обновление предыдущей версии программы имеет ограничения (см. раздел «Ограничения и предупреждения» на стр. 178).

В этом разделе

Шаг 1. Поиск более новой версии программы

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

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

Если мастер обнаружит на серверах обновлений «Лаборатории Касперского» более актуальную версию Kaspersky Total Security, 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 установочного пакета на ваш компьютер и запустит установку новой версии.

Шаг 2. Начало установки программы

На этом шаге мастер установки предлагает вам установить программу.

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

> В зависимости от типа установки и языка локализации на этом шаге 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 Kaspersky Total Security с установочного пакета, полученного через интернет.

На этом шаге 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 условия Лицензионного соглашения не приняты, установка программы не производится.

Шаг 4. Положение о Kaspersky Security Network

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

Ознакомьтесь с Положением о Kaspersky Security Network. Если вы согласны со всеми его пунктами, в окне мастера нажмите на кнопку **Принять**.

Если вы не хотите принимать участие в программе Kaspersky Security Network, нажмите на кнопку **Отказаться**.

После принятия или отказа от участия в Kaspersky Security Network установка программы продолжится.

Шаг 5. Установка

Для некоторых версий Kaspersky Total Security, распространяемых по подписке, перед установкой требуется ввести пароль, предоставленный поставщиком услуг.

После ввода пароля начинается установка программы.

Установка программы занимает некоторое время. Дождитесь ее завершения.

По завершении установки мастер автоматически переходит к следующему шагу.

Во время установки Kaspersky Total Security 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;
    - наличие прав администратора у пользователя, выполняющего установку программы.

    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 Kaspersky Total Security не может удалить автоматически, необходимо удалить вручную. Во время удаления несовместимых программ потребуется перезагрузка операционной системы, после чего установка Kaspersky Total Security продолжится автоматически.

- *Наличие на компьютере вредоносных программ*. При обнаружении на компьютере вредоносных программ, 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 шаге мастер информирует вас о завершении установки программы.

По завершении установки необходимо перезагрузить операционную систему.

Если флажок **Запустить Kaspersky Total Security** установлен, после перезагрузки программа будет запущена автоматически.

Если перед завершением работы мастера вы сняли флажок **Запустить Kaspersky Total Security**, программу нужно запустить вручную.

Удаление программы

В результате удаления Kaspersky Total Security компьютер и ваши персональные данные окажутся незащищенными.

Удаление Kaspersky Total Security выполняется с помощью мастера установки.

► *Чтобы запустить мастер в операционной системе Microsoft Windows 7 и ниже,*

в меню **Пуск** выберите пункт **Все Программы** → **Kaspersky Total Security** → **Удалить Kaspersky Total Security**.

► *Чтобы запустить мастер в операционной системе Microsoft Windows 8 и выше, выполните следующие действия:*

1. На начальном экране по правой клавише мыши на плитке Kaspersky Total Security вызовите панель инструментов.
2. Нажмите на кнопку **Удалить** в панели инструментов.
3. В открывшемся окне выберите в списке Kaspersky Total Security.
4. Нажмите на кнопку **Удалить** в верхней части списка.

В этом разделе

Шаг 1. Ввод пароля для удаления программы

Чтобы удалить Kaspersky Total Security, требуется ввести пароль для доступа к параметрам программы. Если вы по каким-либо причинам не можете указать пароль, удаление программы будет невозможно.

Этот шаг отображается только в случае, если был установлен пароль на удаление программы.

Шаг 2. 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 о лицензии.

► *Чтобы сохранить данные для повторного использования, 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.
- **Файлы карантина** – файлы, проверенные программой и помещенные на карантин.

  При удалении Kaspersky Total Security с компьютера файлы на карантине будут недоступны. Для работы с этими файлами нужно установить Kaspersky Total Security.

- **Параметры работы программы** – значения параметров работы программы, установленные во время ее настройки.

  «Лаборатория Касперского» не гарантирует поддержку параметров предыдущей версии программы. После установки более новой версии программы рекомендуем проверить правильность ее настройки.

  Вы также можете экспортировать параметры защиты при помощи командной строки, используя команду:

  `avp.com EXPORT <имя_файла>`

- **Данные iChecker** – файлы, содержащие информацию об объектах, уже проверенных с помощью технологии iChecker.

- **Базы Анти-Спама** – базы, содержащие образцы спам-сообщений, добавленных пользователем.
- **Виртуальные сейфы** – файлы, которые вы помещали на хранение в Виртуальные сейфы.

Шаг 3. Подтверждение удаления программы

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

Шаг 4. Удаление программы. Завершение удаления

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

После завершения удаления Kaspersky Total Security вы можете указать причины удаления программы на веб-сайте «Лаборатории Касперского». Для этого требуется перейти на веб-сайт «Лаборатории Касперского» по кнопке **Заполнить форму**.

> Эта функциональность может быть недоступна в некоторых регионах.

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 снова.

Лицензирование программы

Этот раздел содержит информацию об основных понятиях, связанных с лицензированием программы.

В этом разделе

О Лицензионном соглашении

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

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

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 и не должны 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 Kaspersky Total Security.

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.

Чтобы работать с программой, вы должны приобрести лицензию на использование программы.

Лицензия имеет ограниченный срок действия. По истечении срока действия лицензии вам может предоставляться льготный период, в течение которого вы можете использовать все функции программы без ограничений.

Если вы не продлили срок действия лицензии (см. раздел «Продление срока действия лицензии» на стр. 55), по истечении льготного периода программа может перейти в режим ограниченной функциональности (см. раздел «О режиме ограниченной функциональности» на стр. 47). В режиме ограниченной функциональности некоторые функции программы недоступны. Продолжительность режима ограниченной функциональности зависит от вашего региона и условий лицензирования. По истечении срока действия режима ограниченной функциональности становятся недоступными все функции программы. Информацию о сроке действия льготного периода и режима ограниченной функциональности вы найдете в окне **Лицензирование**, открывающемся по ссылке **Лицензия**, расположенной в нижней части главного окна.

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

Перед приобретением лицензии вы можете ознакомиться с пробной версией Kaspersky Total Security без выплаты вознаграждения. Пробная версия Kaspersky Total Security выполняет свои функции в течение короткого ознакомительного периода. После окончания ознакомительного периода Kaspersky Total Security прекращает выполнять все свои функции. Для продолжения использования программы требуется приобрести лицензию.

Если вы не хотите возобновлять защиту вашего компьютера, вы можете удалить Kaspersky Total Security (см. раздел «Удаление программы» на стр. 41).

О режиме ограниченной функциональности

В таблице ниже можно посмотреть, какие функции Kaspersky Total Security доступны, а какие недоступны, когда программа работает в режиме ограниченной функциональности. Если в графе «Режим ограниченной функциональности» указано значение «есть», это значит, что функциональность доступна в режиме ограниченной функциональности. Если в графе «Режим ограниченной функциональности» указано значение «нет», функциональность недоступна. Дополнительная информация указана в графе «Ограничения».

Таблица 2. Функциональность Kaspersky Total Security в режиме ограниченной функциональности

Функциональность	Ограничения	Режим ограниченной функциональности
Файловый Антивирус		есть
Проверка на вирусы	Доступен запуск проверки вручную. Проверка по расписанию и настройка параметров проверки недоступны.	есть
Проверка на уязвимости		нет
Обновление баз и программных модулей	Настройка параметров недоступна.	есть
Защита от рекламных программ и программ-шпионов		есть

Функциональность	Ограничения	Режим ограниченной функциональности
Веб-Антивирус	Работает без ограничений.	есть
Почтовый Антивирус	Работает без ограничений.	есть
IM-Антивирус	Работает без ограничений.	есть
Эвристический анализ	Работает без ограничений.	есть
Защита от руткитов		нет
Защита от эксплойтов		нет
Мониторинг активности		нет
Защита от фишинга		есть
Проверка репутации файлов и ссылок в Kaspersky Security Network	Работает без ограничений.	есть
Дополнительные средства защиты и управления	Работает без ограничений.	есть
Проверка ссылок		нет
Безопасный ввод данных		нет
Диск аварийного восстановления	Есть возможность загрузить через интерфейс программы.	есть
Защита паролем параметров программы	Работает без ограничений.	есть
Производительность	Доступна настройка параметров производительности программы.	есть
Менеджер задач	Менеджер задач только отображает результаты проверки, нет возможности управлять проверкой или ее параметрами.	есть

Функциональность	Ограничения	Режим ограниченной функциональности
Игровой профиль	Работает без ограничений.	есть
Угрозы и исключения	Работает без ограничений.	есть
Самозащита	Работает без ограничений.	есть
Карантин	Работает без ограничений.	есть
Уведомления	Можно настроить только получение рекламных сообщений от «Лаборатории Касперского».	есть
«Защити друга»	Доступны все возможности участия в программе «Защити друга».	есть
Настройка отображения программы	Работает без ограничений.	есть
Личный кабинет		есть
Восстановление после заражения	Работает без ограничений.	есть
Контроль программ		нет
Сетевой экран		нет
Защита от сетевых атак		нет
Анти-Спам		нет
Анти-Баннер		нет
Безопасные платежи		нет
Безопасный поиск		нет
Защита от сбора данных		нет

Функциональность	Ограничения	Режим ограниченной функциональности
Устранение следов активности		нет
Родительский контроль		нет
Защита доступа к веб-камере		нет
Уведомление при подключении к небезопасной сети Wi-Fi		нет
Мониторинг сети		нет
Контроль изменений операционной системы		нет
Kaspersky Password Manager	Программа Kaspersky Password Manager доступна, если она была установлена до включения режима ограниченной функциональности. Если программа не была установлена, ее установка в режиме ограниченной защиты невозможна. Запуск Kaspersky Password Manager из окна Kaspersky Total Security в режиме ограниченной функциональности невозможен.	нет
Удаление неиспользуемых данных		нет
Необратимое удаление данных		нет
Виртуальные сейфы	Доступно только получение доступа к данным в ранее созданных сейфах.	нет

Функциональность	Ограничения	Режим ограниченной функциональности
Резервное копирование	Доступно только восстановление данных из ранее созданных резервных копий.	нет
Удаленное управление	Только просмотр и управление кодами активации.	есть

О коде активации

Код активации – это код, который вы получаете, приобретая лицензию на использование Kaspersky Total Security. 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 Kaspersky Total Security, код активации указан в документации или на коробке, в которой находится установочный компакт-диск.
- Если вы приобрели Kaspersky Total Security 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 Kaspersky Total Security 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 обратитесь в Службу технической поддержки «Лаборатории Касперского» (http://support.kaspersky.ru).

О подписке

Подписка на Kaspersky Total Security – это использование программы с выбранными параметрами (дата окончания, количество защищаемых устройств). Подписку на Kaspersky Total Security можно оформить у поставщика услуг (например, у интернет-провайдера). Вы можете приостанавливать или возобновлять подписку, продлевать ее в автоматическом режиме, а также отказываться от нее. Подпиской можно управлять через ваш персональный кабинет на веб-сайте поставщика услуги.

Поставщики услуг могут предоставлять два типа подписки на использование Kaspersky Total Security: подписку на обновление и подписку на обновление и защиту.

Подписка может быть ограниченной (например, на один год) или неограниченной (без даты окончания). Для продолжения работы Kaspersky Total Security после окончания ограниченной подписки необходимо самостоятельно продлить ее. Неограниченная подписка продлевается автоматически при условии своевременного внесения предоплаты поставщику услуг.

Если подписка ограничена, по ее окончании вам предоставляется льготный период для продления подписки, в течение которого функциональность программы сохранена.

Если подписка не продлена, по истечении льготного периода Kaspersky Total Security прекращает обновлять базы программы (для подписки на обновление), взаимодействовать с Kaspersky Security Network, а также прекращает защищать компьютер и запускать задачи проверки (для подписки на обновление и защиту).

Чтобы использовать Kaspersky Total Security по подписке, нужно применить код активации, предоставленный поставщиком услуг. В некоторых случаях код активации может загружаться и применяться автоматически. При использовании программы по подписке вы не можете применить другой код активации для продления срока действия лицензии. Это возможно только после окончания подписки.

Если на момент регистрации подписки Kaspersky Total Security уже используется по действующей лицензии, то после регистрации подписки Kaspersky Total Security будет использоваться по подписке. Код активации, с помощью которого до этого была активирована программа, можно применить на другом компьютере.

Чтобы отказаться от подписки, необходимо связаться с поставщиком услуг, у которого вы приобрели Kaspersky Total Security.

В зависимости от поставщика услуг, набор возможных действий при управлении подпиской может различаться. Кроме того, может не предоставляться льготный период, в течение которого доступно продление подписки.

О предоставлении данных

В целях повышения уровня защиты информации и улучшения качества работы Kaspersky Total Security вы соглашаетесь в автоматическом режиме предоставить в «Лабораторию Касперского» информацию статистического и служебного характера, включая, но не ограничиваясь: информацию об установленном на компьютере программном обеспечении, данные о лицензии, информацию об обнаруженных угрозах и заражениях, контрольные суммы обрабатываемых объектов, техническую информацию о компьютере и подключенных к нему устройствах, информацию об активности работы устройства в сети Интернет. С более подробной информацией вы можете ознакомиться на сайте (http://help.kaspersky.com).

Если вы участвуете в программе Kaspersky Security Network, вы соглашаетесь в автоматическом режиме передавать в «Лабораторию Касперского» следующую информацию (http://help.kaspersky.com), полученную в результате работы Kaspersky Total Security на компьютере. Ознакомиться с Положением о Kaspersky Security Network вы можете в окне **Параметры дополнительных средств защиты**.

Полученная информация защищается «Лабораторией Касперского» в соответствии с установленными законом требованиями и действующими правилами «Лаборатории Касперского».

«Лаборатория Касперского» использует полученную информацию только в обезличенном виде и в виде данных общей статистики. Данные общей статистики формируются автоматически из исходной полученной информации и не содержат персональных и иных конфиденциальных данных. Исходная полученная информация уничтожается по мере накопления (один раз в год). Данные общей статистики хранятся бессрочно.

Приобретение лицензии

Вы можете приобрести лицензию или продлить срок ее действия. При приобретении лицензии вы получите код активации, с помощью которого нужно активировать программу (см. раздел «Активация программы» на стр. 54).

► *Чтобы приобрести лицензию, выполните следующие действия:*

1. Откройте главное окно программы.
2. Откройте окно **Лицензирование** одним из следующих способов:
   - по ссылке **Лицензия отсутствует**, расположенной в нижней части главного окна, если программа не активирована;
   - по ссылке **Лицензия**, расположенной в нижней части главного окна, если программа активирована.
3. В открывшемся окне нажмите на кнопку **Купить код активации**.

Откроется веб-страница интернет-магазина «Лаборатории Касперского» или компании-партнера, где вы можете приобрести лицензию.

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 Kaspersky Total Security, появляющиеся в области уведомлений панели задач.

► *Чтобы активировать программу Kaspersky Total Security, выполните следующие действия:*

1. Откройте главное окно программы.
2. По ссылке **Ввести код активации**, расположенной в нижней части главного окна программы, откройте окно **Активация**.

3. В окне **Активация** введите код активации в поле ввода и нажмите на кнопку **Активировать**.

   Будет выполнен запрос на активацию программы.

4. Введите регистрационные данные пользователя.

   В зависимости от условий использования программа может запросить у вас аутентификацию на портале My Kaspersky. Если вы не являетесь зарегистрированным пользователем, заполните поля формы регистрации, чтобы получить дополнительные возможности.

   Зарегистрированные пользователи могут выполнять следующие действия:

   - отправлять запросы в Службу технической поддержки и Вирусную Лабораторию;
   - управлять кодами активации;
   - получать информацию о новых программах и специальных предложениях «Лаборатории Касперского».

   > Этот шаг доступен не во всех версиях Kaspersky Total Security.

5. Нажмите на кнопку **Завершить** в окне **Активация**, чтобы завершить процесс активации.

Продление срока действия лицензии

Вы можете продлить срок действия лицензии, если он подходит к концу. Для этого вы можете указать резервный код активации, не дожидаясь истечения срока действия лицензии. По истечении срока действия лицензии программа Kaspersky Total Security будет автоматически активирована с помощью резервного кода активации.

► *Чтобы указать резервный код активации для автоматического продления срока действия лицензии, выполните следующие действия:*

1. Откройте главное окно программы.
2. По ссылке **Лицензия**, расположенной в нижней части главного окна, откройте окно **Лицензирование**.
3. В открывшемся окне в блоке **Резервный код активации** нажмите на кнопку **Ввести код активации**.
4. Введите код активации в соответствующие поля и нажмите на кнопку **Добавить**.

   Kaspersky Total Security отправит данные на сервер активации «Лаборатории Касперского» для проверки.
5. Нажмите на кнопку **Завершить**.

Резервный код активации будет отображаться в окне **Лицензирование**.

Программа автоматически активируется с помощью резервного кода активации по истечении срока действия лицензии. Вы также можете самостоятельно активировать программу с помощью резервного кода активации нажатием на кнопку **Активировать сейчас**. Кнопка доступна, если программа не активировалась автоматически. Кнопка недоступна до истечения срока действия лицензии.

Если вы указали в качестве резервного кода активации уже примененный ранее на этом или другом компьютере код активации, при продлении срока действия лицензии датой активации программы считается дата первой активации программы с помощью этого кода активации.

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 операционной 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 операционной 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 специалистами «Лаборатории Касперского» по умолчанию.

Уведомление может быть закрыто автоматически при перезагрузке компьютера, закрытии Kaspersky Total Security или в режиме Connected Standby в Windows 8. Уведомления компонента Контроль программ автоматически закрываются по истечении 500 секунд. Уведомления о запуске программы автоматически закрываются по истечении 1 часа. При автоматическом закрытии уведомления Kaspersky Total Security выполняет действие, рекомендованное по умолчанию.

Уведомления не отображаются в течение первого часа работы программы в случае приобретения компьютера с предустановленной программой Kaspersky Total Security (OEM-поставка). Программа обрабатывает обнаруженные объекты в соответствии с рекомендуемыми действиями. Результаты обработки сохраняются в отчете.

Анализ состояния защиты компьютера и устранение проблем безопасности

О появлении проблем в защите компьютера сигнализирует индикатор, расположенный в верхней части главного окна программы. Зеленый цвет индикатора 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.

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

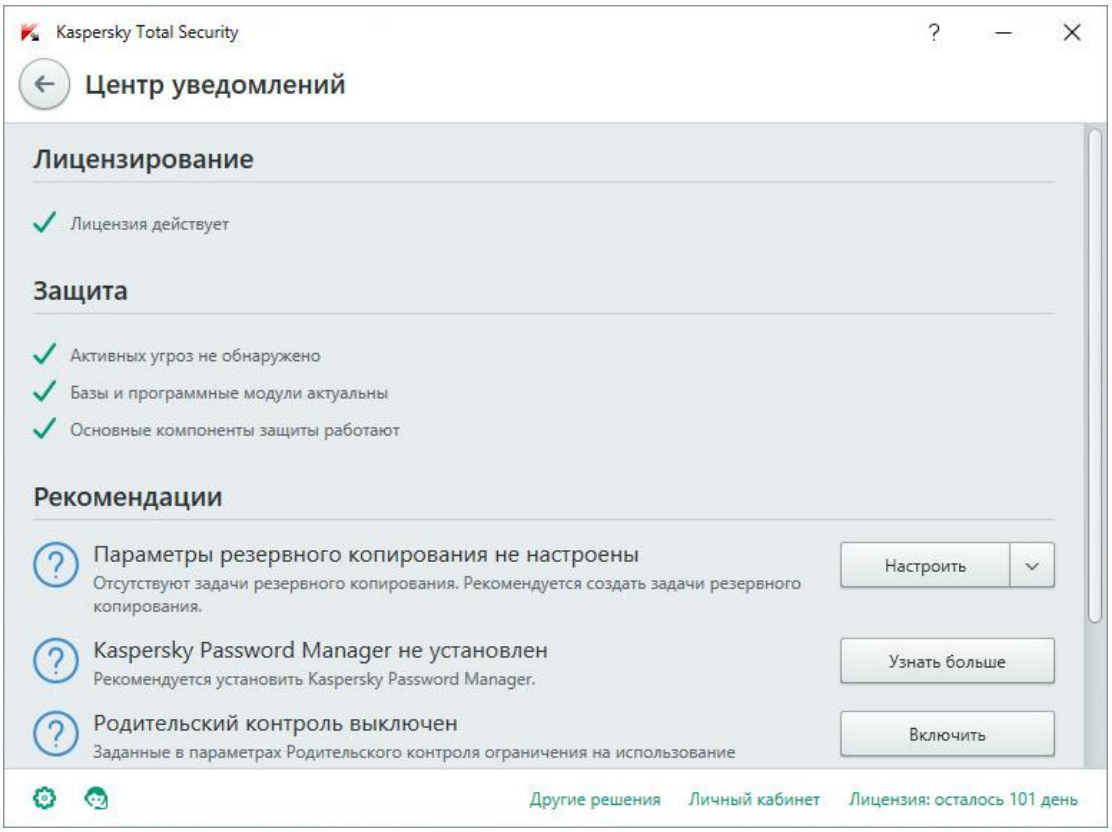

Рисунок 1. Окно Центр уведомлений

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 программных модулей

Этот раздел содержит информацию об обновлении баз и программных модулей.

В этом разделе

Об обновлении баз и программных модулей

Пакет установки Kaspersky Total Security включает в себя базы и программные модули. С помощью этих баз программа обеспечивает *начальный уровень защиты*:

- Kaspersky Total Security обнаруживает большинство угроз с помощью Kaspersky Security Network, для чего требуется подключение к интернету.
- Kaspersky Total Security не обнаруживает рекламные программы, программы автодозвона и другие легальные программы, которые могут быть использованы злоумышленником для нанесения вреда компьютеру или данным пользователя.

Для полной защиты рекомендуется обновить базы и программные модули сразу после установки программы.

Обновление баз и программных модулей выполняется поэтапно:

1. Kaspersky Total Security запускает обновление баз и программных модулей согласно указанным параметрам: автоматически, по расписанию или по вашему требованию. Программа обращается к источнику обновлений, где хранится пакет обновлений баз и программных модулей.
2. Kaspersky Total Security сравнивает имеющиеся базы с базами, находящимися в источнике обновлений. Если базы отличаются, Kaspersky Total Security загружает отсутствующие части баз.

После этого программа использует обновленные базы и программные модули для проверки компьютера на вирусы и другие программы, представляющие угрозу.

Вы можете использовать следующие источники обновлений:

- Серверы обновлений «Лаборатории Касперского».
- HTTP или FTP-сервер.
- Сетевая папка.

Обновление баз и программных модулей имеет следующие особенности и ограничения:

- Базы устаревают по истечении двух дней.
- Для загрузки пакета обновлений с серверов обновлений «Лаборатории Касперского» требуется соединение с интернетом.
- Обновление баз и программных модулей недоступно в следующих случаях:
  - Истек срок действия лицензии, и не предусмотрен льготный период или режим ограниченной функциональности.
  - Используется высокоскоростное мобильное подключение к интернету. Это ограничение действует при работе в операционной системе Microsoft Windows 8 и выше, если выбран автоматический режим обновления или режим обновления по расписанию и установлено ограничение трафика при высокоскоростном мобильном подключении. Чтобы в этом случае выполнялось обновление баз и программный модулей, требуется снять флажок **Ограничивать трафик при лимитном подключении** в окне **Настройка** → **Дополнительно** → **Сеть**.
  - Программа используется по подписке, и вы приостановили подписку на веб-сайте поставщика услуг.

Запуск обновления баз и программных модулей

► *Чтобы запустить обновление баз и программных модулей из контекстного меню значка программы,*

в контекстном меню значка программы в области уведомлений панели задач выберите пункт **Обновление**.

► *Чтобы запустить обновление баз и программных модулей из главного окна программы, выполните следующие действия:*

1. Откройте главное окно программы и нажмите на кнопку **Обновление**.

   Откроется окно **Обновление**.

2. В окне **Обновление** нажмите на кнопку **Обновить**.

Проверка компьютера

Это раздел содержит информацию о проверке компьютера на наличие вирусов и других программ, представляющих угрозу.

В этом разделе

Полная проверка

Во время полной проверки по умолчанию Kaspersky Total Security проверяет следующие объекты:

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

Рекомендуется выполнить полную проверку сразу после установки Kaspersky Total Security на компьютер.

► *Чтобы запустить полную проверку, выполните следующие действия:*

1. Откройте главное окно программы.
2. Нажмите на кнопку **Проверка**.

   Откроется окно **Проверка**.
3. В окне **Проверка** выберите раздел **Полная проверка**.
4. В разделе **Полная проверка** нажмите на кнопку **Запустить проверку**.

Kaspersky Total Security начнет полную проверку компьютера.

Выборочная проверка

С помощью выборочной проверки вы можете проверить на вирусы и другие программы, представляющие угрозу, файл, папку или диск.

Запустить выборочную проверку вы можете следующими способами:

- из контекстного меню объекта;
- из главного окна программы.

► *Чтобы запустить выборочную проверку 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. рис. ниже) и выберите пункт **Проверить на вирусы**.

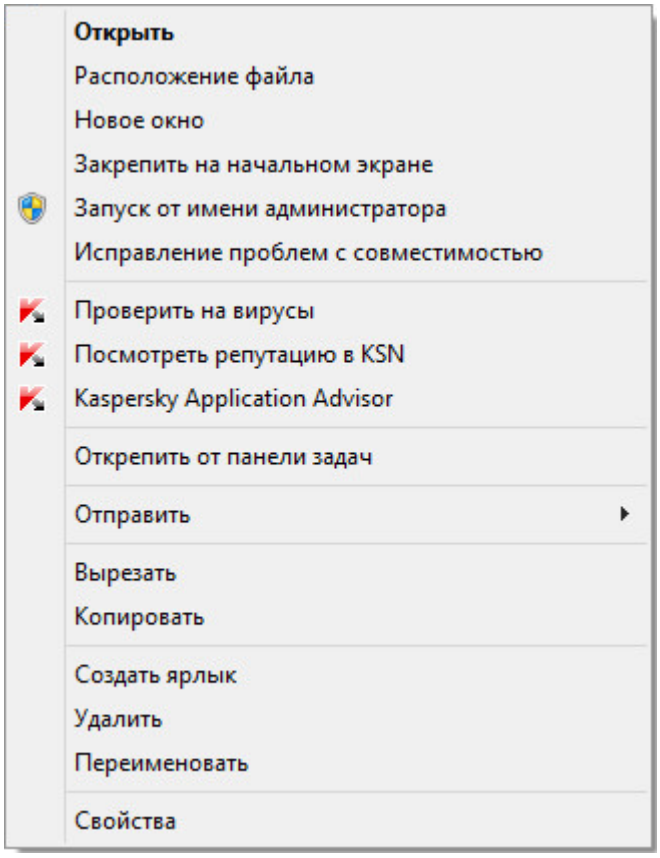

Рисунок 2. Контекстное меню объекта

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

1. Откройте главное окно программы.
2. Нажмите на кнопку **Проверка**.

   Откроется окно **Проверка**.
3. В окне **Проверка** выберите раздел **Выборочная проверка**.
4. Укажите объекты, которые нужно проверить, одним из следующих способов:
   - Перетащите объекты в окно **Выборочная проверка**.
   - Нажмите на кнопку **Добавить** и укажите объект в открывшемся окне выбора файла или папки.
5. Нажмите на кнопку **Запустить проверку**.

Быстрая проверка

Во время быстрой проверки Kaspersky Total Security по умолчанию проверяет следующие объекты:

- объекты, которые загружаются при запуске операционной системы;
- системная память;
- загрузочные сектора диска.

► *Чтобы запустить быструю проверку, выполните следующие действия:*

1. Откройте главное окно программы.
2. Нажмите на кнопку **Проверка**.

   Откроется окно **Проверка**.
3. В окне **Проверка** выберите раздел **Быстрая проверка**.
4. В разделе **Быстрая проверка** нажмите на кнопку **Запустить проверку**.

Kaspersky Total Security начнет быструю проверку компьютера.

Поиск уязвимостей

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 уязвимостей позволяет найти такие «слабые места» в защите компьютера. Найденные уязвимости рекомендуется устранить.

► *Чтобы запустить поиск уязвимостей, выполните следующие действия:*

1. Откройте главное окно программы.
2. Нажав на кнопку **Больше функций**, расположенную в нижней части главного окна, откройте окно **Инструменты**.
3. В левой части окна **Инструменты** по ссылке **Поиск уязвимостей** откройте окно **Поиск уязвимостей**.
4. В окне **Поиск уязвимостей** нажмите на кнопку **Запустить проверку**.

Kaspersky Total Security начнет проверку вашего компьютера на наличие уязвимостей.

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.

Kaspersky Total Security не выполняет лечение приложений из Магазина Windows. Если в результате проверки такое приложение признано опасным, оно будет удалено с вашего компьютера.

При удалении приложений из Магазина Windows Kaspersky Total Security не создает резервные копии. Для восстановления таких объектов необходимо использовать средства восстановления операционной системы (подробную информацию можно получить из документации к операционной системе, установленной на вашем компьютере) либо обновить приложения через Магазин Windows.

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

1. Откройте главное окно программы.
2. Нажав на кнопку **Больше функций**, расположенную в нижней части главного окна, откройте окно **Инструменты**.
3. В левой части окна **Инструменты** по ссылке **Карантин** откройте окно **Карантин**.
4. В открывшемся окне **Карантин** выберите нужный файл в списке и нажмите на кнопку **Восстановить**.

Восстановление операционной системы после заражения

Этот раздел содержит информацию о восстановлении операционной системы после заражения вирусами.

В этом разделе

О восстановлении 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 м*астер восстановления после заражения*, устраняющий следы пребывания в операционной 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 операционной 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 операционной системы, системные сбои или применение неправильно работающих программ – оптимизаторов операционной системы.

После исследования мастер анализирует полученную информацию с целью выявления в операционной 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.

Восстановление операционной системы с помощью мастера восстановления

► *Чтобы запустить мастер восстановления после заражения, выполните следующие действия:*

1. Откройте главное окно программы.

2. Нажав на кнопку **Больше функций**, расположенную в нижней части главного окна, откройте окно **Инструменты**.

3. В левой части окна **Инструменты** по ссылке **Восстановление после заражения** запустите мастер восстановления после заражения.

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 операционной системы

Убедитесь, что в окне мастера выбран вариант **Выполнить поиск повреждений, связанных с активностью вредоносных программ**, 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 повреждений

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

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

Для просмотра повреждений, включенных в группу, нажмите на значок , расположенный слева от названия группы.

Чтобы мастер устранил какое-либо повреждение, установите флажок слева от названия повреждения. По умолчанию мастер устраняет повреждения из группы рекомендуемых и настоятельно рекомендуемых к устранению. Если вы не хотите устранять какое-либо повреждение, 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 повреждений

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

Шаг 5. Завершение работы мастера

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

О диске аварийного восстановления

Диск аварийного восстановления представляет собой программу Kaspersky Rescue Disk, записанную на съемный диск (CD-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).

Если вы купили программу Kaspersky Total Security в коробке, то на установочном диске помимо установочного пакета Kaspersky Total Security находится также Kaspersky Rescue Disk. Вы можете использовать этот установочный диск в качестве диска аварийного восстановления.

Более подробную информацию об использовании Kaspersky Rescue Disk вы найдете на веб-сайте Службы технической поддержки (http://support.kaspersky.ru/viruses/rescuedisk/main).

Защита электронной почты

Этот раздел содержит информацию о том, как защитить электронную почту от спама, вирусов и других программ, представляющих угрозу.

В этом разделе

Настройка Почтового Антивируса

Kaspersky Total Security 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 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 настроить Почтовый Антивирус, выполните следующие действия:*

1. Откройте главное окно программы.
2. Нажмите на кнопку в нижней части окна программы.

   Откроется окно **Настройка**.
3. В левой части окна выберите в разделе **Защита** компонент Почтовый Антивирус.

   В окне отобразятся параметры Почтового Антивируса.
4. Убедитесь, что переключатель в верхней части окна, включающий / выключающий Почтовый Антивирус, включен.

5. Выберите уровень безопасности:

   - **Рекомендуемый**. При установке этого уровня безопасности Почтовый Антивирус проверяет входящие и исходящие сообщения, вложенные архивы, а также выполняет эвристический анализ с уровнем детализации **Средний**.

   - **Низкий**. При установке этого уровня безопасности Почтовый Антивирус проверяет только входящие сообщения и не проверяет вложенные архивы.

   - **Высокий**. При установке этого уровня безопасности Почтовый Антивирус проверяет входящие и исходящие сообщения, вложенные архивы, а также проводит эвристический анализ с уровнем детализации **Глубокий**.

6. В раскрывающемся списке **Действие при обнаружении угрозы** выберите действие, которое Почтовый Антивирус будет выполнять при обнаружении зараженного объекта (например, лечить).

Если угрозы в почтовом сообщении не были 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 Kaspersky Total Security. В случае удаления объекта Kaspersky Total Security создает его резервную копию и помещает на карантин (см. раздел «Восстановление удаленного или вылеченного программой объекта» на стр. 66).

Если во время проверки программа Kaspersky Total Security обнаружила в тексте сообщения пароль к архиву, пароль будет использован для проверки содержания этого архива на наличие вредоносных программ. Пароль при этом не сохраняется. При проверке архива выполняется его распаковка. Если во время распаковки архива произошел сбой в работе программы, вы можете вручную удалить файлы, которые при распаковке сохраняются по следующему пути: %systemroot%\temp. Файлы имеют префикс PR.

Блокирование нежелательной почты (спама)

Если вы получаете большое количество нежелательной почты (спама), включите компонент Анти-Спам и установите для него уровень безопасности **Рекомендуемый**.

► *Чтобы включить Анти-Спам и установить уровень безопасности Рекомендуемый , выполните следующие действия:*

1. Откройте главное окно программы.
2. Нажмите на кнопку в нижней части окна программы.

   Откроется окно **Настройка**.
3. В левой части окна выберите раздел **Защита**.
4. В правой части раздела **Защита** выберите компонент Анти-Спам.

   В окне отобразятся параметры Анти-Спама.
5. В правой части окна включите Анти-Спам с помощью переключателя.
6. Убедитесь, что в блоке **Уровень безопасности** установлен уровень безопасности **Рекомендуемый**.

Компонент Анти-Спам может анализировать только сообщения, загружаемые с почтового сервера целиком, независимо от используемого протокола.

Защита персональных данных в интернете

Этот раздел содержит информацию о том, как сделать работу в интернете безопасной и защитить ваши данные от кражи.

В этом разделе

О защите персональных данных в интернете

С помощью Kaspersky Total Security вы можете защитить от кражи свои персональные данные:

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

В состав Kaspersky Total Security входят компоненты и инструменты, позволяющие защитить ваши персональные 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, Анти-Спам и IM-Антивирус. Включите эти компоненты, чтобы обеспечить максимально эффективную защиту от фишинга.

Для защиты от перехвата данных, введенных с клавиатуры, предназначена Экранная клавиатура и защита ввода данных с аппаратной клавиатуры.

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

Для защиты данных при использовании сервисов интернет-банкинга и при оплате покупок в интернет-магазинах предназначены функции Безопасных платежей.

Для защиты от пересылки персональных данных через интернет предназначен один из инструментов Родительского контроля (см. раздел «Использование Родительского контроля» на стр. 106).

Об Экранной клавиатуре

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 персональных данных с помощью аппаратных перехватчиков или клавиатурных перехватчиков – программ, регистрирующих нажатие клавиш. Экранная клавиатура позволяет избежать перехвата данных, вводимых с клавиатуры.

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

Экранная клавиатура имеет следующие особенности:

- На клавиши Экранной клавиатуры нужно нажимать с помощью мыши.
- В отличие от настоящей клавиатуры, на Экранной 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 Экранной 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 Экранной клавиатуры, после установки Kaspersky Total Security необходимо перезагрузить компьютер.

Использование Экранной клавиатуры имеет следующие ограничения:

- Экранная клавиатура защищает от перехвата персональных данных только при работе с браузерами Microsoft Internet Explorer, Mozilla Firefox и Google Chrome. При работе с другими браузерами Экранная клавиатура не защищает вводимые персональные данные от перехвата.
- Экранная клавиатура недоступна в браузере Microsoft Internet Explorer (версии 10 и 11) в стиле нового интерфейса Windows. В этом случае рекомендуется вызывать Экранную клавиатуру из интерфейса Kaspersky Total Security.
- Экранная 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.
- Экранная клавиатура не предотвращает снятие снимков экрана с помощью нажатия клавиши **PRINT SCREEN** и других комбинаций клавиш, заданных в параметрах операционной системы.

- При запуске Экранной клавиатуры в браузере Microsoft Internet Explorer перестает работать функция автозаполнения полей ввода, так как реализация системы автозаполнения позволяет злоумышленникам перехватывать вводимые данные.
- Kaspersky Total Security не защищает от создания снимков экрана в операционной системе Microsoft Windows 8 и 8.1 (только 64-разрядные), если открыто окно Экранной клавиатуры, но не запущен процесс Защищенного браузера.

В списке выше перечислены основные ограничения, которые имеет функциональность защиты ввода данных. Полный перечень ограничений приводится в статье на сайте Службы технической поддержки «Лаборатории Касперского» (http://support.kaspersky.ru/12005).

Запуск Экранной клавиатуры

Открыть Экранную клавиатуру можно следующими способами:

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

  Отображение значка быстрого вызова в полях ввода на веб-сайтах можно настроить (см. раздел «Настройка отображения значка Экранной клавиатуры» на стр. 79).

  При использовании Экранной клавиатуры Kaspersky Total Security отключает функцию автозаполнения полей ввода на веб-сайтах.

- с помощью комбинации клавиш аппаратной клавиатуры.

► *Чтобы открыть Экранную клавиатуру из контекстного меню значка программы в области уведомлений,*

выберите пункт **Инструменты** → **Экранная клавиатура** (см. рис. ниже).

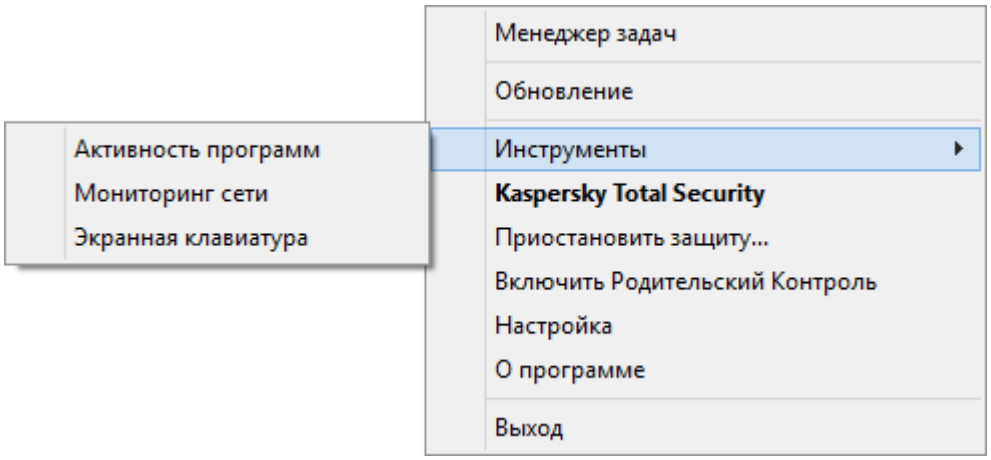

Рисунок 3. Контекстное меню Kaspersky Total Security

► *Чтобы открыть Экранную клавиатуру из окна программы, выполните следующие действия:*

1. Откройте главное окно программы.
2. Нажав на кнопку **Больше функций**, расположенную в нижней части главного окна, откройте окно **Инструменты**.
3. В левой части окна **Инструменты** по ссылке **Экранная клавиатура** откройте Экранную клавиатуру.

► *Чтобы открыть Экранную клавиатуру из панели инструментов браузера Google Chrome, Microsoft Internet Explorer или Mozilla Firefox, выполните следующие действия:*

1. Нажмите на кнопку **Kaspersky Protection** в панели инструментов браузера.
2. В раскрывшемся меню выберите пункт **Экранная клавиатура**.

► *Чтобы открыть Экранную клавиатуру с помощью аппаратной клавиатуры,*

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

Настройка отображения значка Экранной клавиатуры

► *Чтобы настроить отображение значка быстрого вызова Экранной клавиатуры в полях ввода на веб-сайтах, выполните следующие действия:*

1. Откройте главное окно программы.
2. Нажмите на кнопку в нижней части окна программы.

   Откроется окно **Настройка**.
3. В разделе **Дополнительно** выберите подраздел **Безопасный ввод данных**.

   В окне отобразятся параметры для настройки безопасного ввода данных.
4. Если необходимо, в блоке **Экранная клавиатура** установите флажок **Открывать Экранную клавиатуру по комбинации клавиш CTRL+ALT+SHIFT+P**.
5. Если вы хотите, чтобы значок вызова Экранной клавиатуры отображался в полях ввода на всех веб-сайтах, установите флажок **Показывать значок быстрого вызова в полях ввода**.
6. Если вы хотите, чтобы значок вызова Экранной клавиатуры отображался только при открытии веб-сайтов определенных категорий, выполните следующие действия:

   a. В блоке **Экранная клавиатура** по ссылке **Изменить категории** откройте окно **Параметры Безопасного ввода данных**.

   b. Установите флажки для категорий веб-сайтов, на которых нужно отображать значок вызова Экранной клавиатуры в полях ввода.

      Значок вызова Экранной клавиатуры будет отображаться при открытии веб-сайта, относящегося к какой-либо из выбранных категорий.
7. Если вы хотите включить или выключить отображение значка вызова Экранной клавиатуры на определенном веб-сайте, выполните следующие действия:

   a. В блоке **Экранная клавиатура** по ссылке **Изменить категории** откройте окно **Параметры Безопасного ввода данных**.

   b. По ссылке **Настройка исключений** откройте окно **Исключения для Экранной клавиатуры**.

c. В нижней части окна нажмите на кнопку **Добавить**.

d. Откроется окно для добавления исключения для Экранной клавиатуры.

e. Введите адрес веб-сайта в поле **Маска веб-адреса**.

f. В блоке **Область применения** укажите, где должен отображаться (или не отображаться) значок вызова Экранной клавиатуры: на указанной странице или на всех страницах веб-сайта.

g. В блоке **Значок Экранной клавиатуры** укажите, должен ли отображаться или нет значок вызова Экранной клавиатуры.

h. Нажмите на кнопку **Добавить**.

   Указанный веб-сайт появится в списке в окне **Исключения для Экранной клавиатуры**.

При открытии указанного веб-сайта значок вызова Экранной клавиатуры будет отображаться в полях ввода в соответствии с настроенными параметрами.

Защита ввода данных с аппаратной клавиатуры

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

Защита ввода данных с аппаратной клавиатуры имеет следующие ограничения:

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

В списке выше перечислены основные ограничения, которые имеет функциональность защиты ввода данных. Полный перечень ограничений приводится в статье на сайте Службы технической поддержки «Лаборатории Касперского» (http://support.kaspersky.ru/12005).

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.

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

1. Откройте главное окно программы.
2. Нажмите на кнопку в нижней части окна программы.

   Откроется окно **Настройка**.
3. В разделе **Дополнительно** выберите подраздел **Безопасный ввод данных**.

   В окне отобразятся параметры безопасного ввода данных.
4. В нижней части окна в блоке **Защита ввода данных с аппаратной клавиатуры** установите флажок **Защищать ввод данных с аппаратной клавиатуры**.
5. Откройте окно **Параметры Безопасного ввода данных** по ссылке **Изменить категории** в нижней части блока **Защита ввода данных с аппаратной клавиатуры**.
6. Установите флажки для категорий веб-сайтов, на которых нужно защищать данные, вводимые с клавиатуры.
7. Если вы хотите включить или выключить защиту ввода данных с клавиатуры на определенном веб-сайте, выполните следующие действия:

   a. Откройте окно **Исключения для защиты ввода с аппаратной клавиатуры** по ссылке **Настройка исключений**.

   b. В открывшемся окне нажмите на кнопку **Добавить**.

   c. Откроется окно для добавления исключения для аппаратной клавиатуры.

d. В открывшемся окне введите адрес веб-сайта в поле **Маска веб-адреса**.

e. Выберите один из вариантов защиты ввода данных на этом веб-сайте: **Применить к указанной странице** или **Применить ко всему веб-сайту**.

f. Выберите действие защиты ввода данных на этом веб-сайте: **Защищать** или **Не защищать**.

g. Нажмите на кнопку **Добавить**.

Указанный веб-сайт появится в списке в окне **Исключения для защиты ввода с аппаратной клавиатуры**. При открытии указанного веб-сайта будет действовать защита ввода данных в соответствии с настроенными параметрами.

Настройка уведомлений об уязвимостях сети Wi-Fi

Во время работы в сети Wi-Fi ваши конфиденциальные данные могут быть похищены, если сеть Wi-Fi недостаточно защищена. Kaspersky Total Security проверяет сеть Wi-Fi при каждом вашем подключении к сети Wi-Fi. Если сеть Wi-Fi небезопасна (например, используется уязвимый протокол шифрования или имя сети Wi-Fi (SSID) является популярным), программа показывает уведомление о том, что вы подключаетесь к небезопасной сети Wi-Fi. По ссылке в окне уведомления вы можете узнать, как обезопасить себя при работе в сети Wi-Fi.

► *Чтобы настроить уведомления об уязвимостях сети Wi-Fi, выполните следующие действия:*

1. Откройте главное окно программы.
2. Нажмите на кнопку в нижней части окна программы.

   Откроется окно **Настройка**.
3. В левой части окна выберите раздел **Защита**.
4. В правой части раздела **Защита** выберите подраздел **Сетевой экран**.

   В окне отобразятся параметры компонента Сетевой экран.

5. Установите флажок **Уведомлять об уязвимостях при подключении к сети Wi-Fi**, если он был снят. Если вы не хотите получать уведомления, снимите этот флажок. По умолчанию флажок установлен.

6. Если флажок **Уведомлять об уязвимостях при подключении к сети Wi-Fi** установлен, вы можете настроить дополнительные параметры отображения уведомлений:

   - Установите флажок **Запрещать передачу пароля в интернете в незащищенном виде и показывать уведомление**, чтобы блокировать передачу пароля в незащищенном текстовом виде при заполнении поля **Пароль** в интернете. По умолчанию флажок снят.

   - По ссылке **Восстановить скрытые уведомления** восстановите значения параметров отображения уведомлений о передаче пароля в незащищенном виде. Если ранее вы заблокировали отображение уведомлений о передаче пароля в незащищенном виде, эти уведомления снова будут отображаться.

Проверка безопасности веб-сайта

Kaspersky Total Security позволяет проверить безопасность веб-сайта, прежде чем вы перейдете по ссылке на этот веб-сайт. Для проверки веб-сайтов используется компонент *Проверка ссылок*.

> Проверка ссылок недоступна в браузере Microsoft Internet Explorer (версии 10 и 11) в стиле нового интерфейса Windows.

Компонент Проверка ссылок проверяет ссылки на веб-странице, открытой в браузере Microsoft Internet Explorer, Google Chrome или Mozilla Firefox. Рядом с проверенной ссылкой Kaspersky Total Security 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 Kaspersky Total Security проверяет ссылки только в результатах поиска. Вы можете включить проверку ссылок на любом веб-сайте.

► *Чтобы настроить проверку ссылок на веб-сайтах, выполните следующие действия:*

1. Откройте главное окно программы.
2. Нажмите на кнопку в нижней части окна программы.

   Откроется окно **Настройка**.
3. В разделе **Защита** выберите подраздел **Веб-Антивирус**.

   В окне отобразятся параметры Веб-Антивируса.
4. По ссылке **Расширенная настройка** в нижней части окна откройте окно дополнительных параметров Веб-Антивируса.
5. В блоке **Проверка ссылок** установите флажок **Проверять ссылки**.
6. Чтобы Kaspersky Total Security проверял содержимое всех веб-сайтов, выберите вариант **На всех веб-сайтах, кроме указанных**.
7. Если необходимо, укажите веб-страницы, которым вы доверяете, в окне **Исключения**. Окно открывается по ссылке **Настроить исключения**. Kaspersky Total Security не будет проверять содержимое указанных веб-страниц, а также зашифрованные соединения с указанными веб-сайтами.
8. Чтобы Kaspersky Total Security проверял содержимое только определенных веб-страниц, выполните следующие действия:

   a. Выберите вариант **Только на указанных веб-сайтах**.

   b. По ссылке **Настроить проверяемые веб-сайты** откройте окно **Проверяемые веб-сайты**.

   c. Нажмите на кнопку **Добавить**.

d. Введите адрес веб-страницы, содержимое которой необходимо проверять.

e. Выберите статус проверки веб-страницы (*Активно* – Kaspersky Total Security проверяет содержимое веб-страницы).

f. Нажмите на кнопку **Добавить**.

   Указанная веб-страница появится в списке в окне **Проверяемые веб-сайты**. Kaspersky Total Security будет проверять ссылки на этой веб-странице.

9. Если вы хотите настроить дополнительные параметры проверки ссылок, в окне **Дополнительные параметры Веб-Антивируса** в блоке **Проверка ссылок** по ссылке **Настроить проверку ссылок** откройте окно **Проверка ссылок**.

10. Чтобы Kaspersky Total Security предупреждал о безопасности ссылок на всех веб-страницах, в блоке **Проверяемые ссылки** выберите вариант **Любые ссылки**.

11. Чтобы Kaspersky Total Security отображал информацию о принадлежности ссылки к определенной категории содержимого веб-сайтов (например, *Нецензурная лексика*), выполните следующие действия:

    a. Установите флажок **Отображать информацию о категориях содержимого веб-сайтов**.

    b. Установите флажки напротив категорий содержимого веб-сайтов, информацию о которых необходимо отображать в комментарии.

Kaspersky Total Security будет проверять ссылки на указанных веб-страницах и отображать информации о категориях ссылок в соответствии с настроенными параметрами.

Защита финансовых операций и покупок в интернете

Этот раздел содержит информацию о том, как вы можете защитить свои финансовые операции и покупки в интернете с помощью Kaspersky Total Security.

В этом разделе

О защите финансовых операций и покупок в интернете

Для защиты конфиденциальных данных, которые вы вводите на веб-сайтах банков и платежных систем (например, номера банковской карты, пароля для доступа к сервисам интернет-банкинга), а также для предотвращения кражи платежных средств при проведении платежей онлайн Kaspersky Total Security предлагает открывать такие веб-сайты в Защищенном браузере.

Защищенный браузер – это специальный режим работы браузера, который используется для защиты ваших данных при работе на веб-сайтах банков или платежных систем. Защищенный браузер запускается в изолированной среде, чтобы другие программы не

могли внедриться в процесс Защищенного браузера. Kaspersky Total Security создает специальные профили браузеров Mozilla Firefox и Google Chrome, чтобы установленные сторонние расширения не могли повлиять на работу Защищенного браузера. Программа не влияет на ваши данные, которые браузеры могут сохранять в созданных профилях.

Браузеры, не соответствующие программным требованиям (см. раздел «Аппаратные и программные требования» на стр. 25), не работают в режиме Защищенного браузера, вместо них в режиме Защищенного браузера запускается Internet Explorer или браузер, заданный в параметрах программы.

При работе в Защищенном браузере программа предоставляет защиту от следующих видов угроз:

- Недоверенные модули. Проверка на наличие недоверенных модулей выполняется при каждом переходе на веб-сайт банка или платежной системы.
- Руткиты. Проверка на наличие руткитов выполняется при запуске Защищенного браузера.
- Известные уязвимости операционной системы. Проверка на наличие уязвимостей операционной системы выполняется при запуске Защищенного браузера.
- Недействительные сертификаты веб-сайтов банков или платежных систем. Проверка сертификатов выполняется при переходе на веб-сайт банка или платежной системы. Проверка сертификатов выполняется по базе скомпрометированных сертификатов.

Когда вы открываете веб-сайт в Защищенном браузере, вокруг окна браузера появляется рамка. Цвет рамки сигнализирует о статусе защиты.

Существуют следующие варианты цветовой индикации рамки окна браузера:

- Зеленый цвет рамки. Означает, что все проверки выполнены успешно. Вы можете продолжить работу в Защищенном браузере.
- Желтый цвет рамки. Означает, что во время проверок были обнаружены проблемы безопасности, которые необходимо устранить.

Программа может обнаружить следующие угрозы и проблемы безопасности:

- Недоверенный модуль. Требуется проверка компьютера и лечение.
- Руткит. Требуется проверка компьютера и лечение.
- Уязвимость операционной системы. Требуется установить обновления операционной системы.
- Недействительный сертификат веб-сайта банка или платежной системы.

Если вы не устраните обнаруженные угрозы, безопасность сеанса подключения к веб-сайту банка или платежной системы не гарантируется. События, связанные с запуском и работой Защищенного браузера с пониженной защитой, записываются в журнал событий Windows.

Желтый цвет рамки также может означать, что запуск Защищенного браузера невозможен из-за технических ограничений. Например, запущен гипервизор стороннего производителя или ваш компьютер не поддерживает технологию аппаратной виртуализации.

Для взаимодействия со страницами защищенных веб-сайтов Kaspersky Total Security внедряет на страницы веб-сайтов специально подготовленный скрипт. Программа внедряет скрипт как самостоятельно, так и с помощью расширения Kaspersky Protection (см. раздел «Подготовка программы к работе» на стр. 35). Также расширение требуется для полноценной поддержки Защищенного браузера. Если расширение не установлено, браузер предложит установить его при первом запуске в режиме Защищенного браузера. Если вы отказались от установки расширения Kaspersky Protection, вы можете установить его позднее.

Запуск Защищенного браузера невозможен, если снят флажок **Включить самозащиту** в разделе **Дополнительные параметры**, подраздел **Самозащита** окна настройки программы.

Настройка параметров Безопасных платежей

► *Чтобы настроить Безопасные платежи, выполните следующие действия:*

1. Откройте главное окно программы.
2. Нажмите на кнопку в нижней части окна программы.

   Откроется окно **Настройка**.
3. В левой части окна выберите раздел **Защита**.
4. В правой части раздела **Защита** выберите подраздел **Безопасные платежи**.

   В окне отобразятся параметры компонента Безопасные платежи.
5. Включите компонент Безопасные платежи с помощью переключателя в верхней части окна.
6. Чтобы включить уведомление об уязвимостях, обнаруженных в операционной системе перед запуском Защищенного браузера, установите флажок **Уведомлять об уязвимостях в операционной системе**.

Настройка Безопасных платежей для определенного веб-сайта

► *Чтобы настроить Безопасные платежи для определенного веб-сайта, выполните следующие действия:*

1. Откройте главное окно программы.
2. Нажмите на кнопку **Безопасные платежи**.

   Откроется окно **Безопасные платежи**.
3. По ссылке **Добавить веб-сайт в Безопасные платежи** откройте в правой части окна поля для добавления информации о веб-сайте.

4. В поле **Веб-сайт для Безопасных платежей** введите адрес веб-сайта, который нужно открывать в Защищенном браузере.

   Перед адресом веб-сайта должен быть указан протокол HTTPS (например, https://example.com), по умолчанию используемый Защищенным браузером.

5. По ссылке **Добавить описание** откройте поле **Описание** и введите название или описание этого веб-сайта.

6. Выберите способ запуска Защищенного браузера при открытии этого веб-сайта:

   - Если вы хотите, чтобы веб-сайт каждый раз открывался в Защищенном браузере, выберите вариант **Запускать Защищенный браузер**.
   - Если вы хотите, чтобы программа Kaspersky Total Security запрашивала, какое действие выполнять при открытии веб-сайта, выберите вариант **Запрашивать действие**.
   - Если вы хотите выключить Безопасные платежи для этого веб-сайта, выберите вариант **Не запускать Защищенный браузер**.

7. В правой части окна нажмите на кнопку **Добавить**.

Веб-сайт отобразится в списке в левой части окна.

Включение автоматической активации расширения Kaspersky Protection

► *Чтобы включить автоматическую активацию расширения Kaspersky Protection, выполните следующие действия:*

1. Откройте главное окно программы.
2. Нажмите на кнопку в нижней части окна программы.

   Откроется окно **Настройка**.

3. В левой части окна выберите раздел **Защита**.

4. В правой части раздела **Защита** выберите раздел **Веб-Антивирус**.
5. В открывшемся окне **Параметры Веб-Антивируса** по ссылке **Расширенная настройка** откройте окно **Дополнительные параметры Веб-Антивируса**.
6. В блоке **Расширение Kaspersky Protection** установите флажок **Автоматически активировать расширение Kaspersky Protection в браузерах**.

О защите от создания снимков экрана

Kaspersky Total Security блокирует несанкционированное создание снимков экрана программами-шпионами, защищая ваши данные при работе с защищаемыми веб-сайтами. Защита от создания снимков экрана включена по умолчанию. Если защита была выключена вручную, вы можете включить ее в окне настройки программы (см. раздел «Включение защиты от создания снимков экрана» на стр. 92).

Программа Kaspersky Total Security, установленная в 64-разрядной операционной системе Microsoft Windows 8, Microsoft Windows 8.1 или Microsoft Windows 10, использует технологию гипервизора для защиты от создания снимков экрана.

Функциональность защиты от создания снимков экрана с помощью гипервизора Kaspersky Total Security имеет следующие ограничения в 64-разрядных операционных системах Microsoft Windows 8, Microsoft Windows 8.1 или Microsoft Windows 10:

- Функциональность недоступна при запуске гипервизора сторонней программы, например программы для виртуализации компании VMware™. После завершения работы гипервизора сторонней программы функциональность защиты от создания снимков экрана снова становится доступной.
- Функциональность недоступна, если центральный процессор вашего компьютера не поддерживает технологию аппаратной виртуализации. Уточнить, поддерживает ли процессор вашего компьютера технологию аппаратной виртуализации, можно в технической документации для вашего компьютера или на веб-сайте производителя процессора.
- Функциональность недоступна, если в момент запуска Защищенного браузера обнаружен работающий гипервизор сторонней программы, например программы компании VMware.

Включение защиты от создания снимков экрана

► *Чтобы включить защиту от создания снимков экрана, выполните следующие действия:*

1. Откройте главное окно программы.
2. Нажмите на кнопку  в нижней части окна программы.

   Откроется окно **Настройка**.
3. В левой части окна выберите раздел **Защита**.
4. В правой части раздела **Защита** выберите подраздел **Безопасные платежи** и убедитесь, что переключатель Безопасных платежей включен.

   Откроется окно **Параметры Безопасных платежей**.
5. В блоке **Дополнительно** установите флажок **Блокировать создание снимков экрана при работе в Защищенном браузере**. Флажок отображается в 64-разрядной версии Windows 8, Windows 8.1 и Windows 10.

О защите данных буфера обмена

Kaspersky Total Security блокирует несанкционированный доступ программ к буферу обмена во время проведения платежных операций, предотвращая кражу данных злоумышленниками. Блокировка действует только в случае попыток недоверенных программ получить несанкционированный доступ к буферу обмена. Если вы вручную копируете данные из окна одной программы в окно другой программы (например, из Блокнота в окно текстового редактора), доступ к буферу обмена разрешен. Если источником данных для копирования является браузер Internet Explorer®, открытый в обычном режиме, в буфер обмена могут быть помещены только данные из адресной строки браузера.

Запуск программы защиты паролей Kaspersky Password Manager

Программа Kaspersky Password Manager предназначена для безопасного хранения и синхронизации паролей между всеми вашими устройствами. Kaspersky Password Manager нужно устанавливать независимо от Kaspersky Total Security. После установки вы можете запускать Kaspersky Password Manager из меню **Пуск** (в операционной системе Microsoft Windows 7 и ниже), с начального экрана (в операционной системе Microsoft Windows 8 и выше) или из окна Kaspersky Total Security.

► *Чтобы запустить программу защиты паролей Kaspersky Password Manager, если она уже установлена, выполните следующие действия:*

1. Откройте главное окно программы Kaspersky Total Security.
2. Нажмите на кнопку **Менеджер паролей**.
3. В открывшемся окне нажмите на кнопку **Запустить Kaspersky Password Manager**.

Откроется окно программы защиты паролей Kaspersky Password Manager.

► *Чтобы загрузить и установить программу защиты паролей Kaspersky Password Manager, если она еще не установлена, выполните следующие действия:*

1. Откройте главное окно программы.
2. Нажмите на кнопку **Менеджер паролей**.

   Откроется окно **Менеджер паролей**.
3. Нажмите на кнопку **Загрузить и установить Kaspersky Password Manager**.

   Kaspersky Total Security загрузит установочный пакет Kaspersky Password Manager и установит программу на ваш компьютер.

   Загруженный установочный пакет Kaspersky Password Manager остается на вашем компьютере вне зависимости от того, установлена ли с его помощью на компьютер программа Kaspersky Password Manager.

Информацию о работе с программой Kaspersky Password Manager смотрите в *Руководстве пользователя Kaspersky Password Manager*.

Защита от сбора информации о ваших действиях в интернете

Этот раздел содержит информацию о том, как с помощью Kaspersky Total Security защитить вас от сбора информации о ваших действиях в интернете.

В этом разделе

О защите от сбора данных

Для защиты от сбора информации о ваших действиях в интернете предназначен компонент *Защита от сбора данных*.

Когда вы находитесь в интернете, компонент Защита от сбора данных обнаруживает запросы, отправляемые браузером на сервисы отслеживания при загрузке веб-страниц, которые содержат программные коды и html-разметку, предназначенные для отслеживания. Сервисы отслеживания используют информацию из этих запросов для анализа ваших действий и могут применять результаты анализа, например, для показа вам соответствующей рекламной информации.

В *режиме обнаружения* компонент Защита от сбора данных предоставляет вам возможность просмотреть отчеты об обнаруженных запросах на сервисы отслеживания. Этот режим включен по умолчанию.

В *режиме блокировки* в дополнение к отчетам компонент Защита от сбора данных модифицирует запросы на сервисы отслеживания и ответы от них таким образом, чтобы защитить вас от сбора информации о ваших действиях в интернете. Далее в этом документе под *блокировкой запросов* и под *блокировкой сервисов отслеживания* понимается описанная выше модификация запросов на сервисы отслеживания и ответов от них.

Вы можете управлять компонентом Защита от сбора данных непосредственно в браузере (см. раздел «Управление защитой от сбора данных в браузере» на стр. 99).

Защита от сбора данных имеет следующие ограничения:

- Программа не блокирует сервисы отслеживания из категории «Средства интернет-коммуникации», если вы находитесь на веб-сайте соответствующей социальной сети.
- Если веб-страницу, с которой отправлен запрос на сервис отслеживания, не удалось определить, то Kaspersky Total Security не блокирует этот сервис отслеживания и не отображает информацию о запросе на него.
- Если веб-страницу, с которой отправлен запрос на сервис отслеживания, удалось определить, но не удалось сопоставить ни с одной веб-страницей, открытой в браузере, то Kaspersky Total Security применяет к этому запросу то действие, которое задано в параметрах Защиты от сбора данных (обнаруживает или блокирует). Программа отображает информацию об этом запросе в отчетах, но не включает этот запрос в статистику Защиты от сбора данных, отображаемую в браузере.

Настройка защиты от сбора данных

► *Чтобы настроить защиту от сбора данных, выполните следующие действия:*

1. Откройте главное окно программы.
2. Нажмите на кнопку ⚙ в нижней части окна программы.

   Откроется окно **Настройка**.
3. В левой части окна выберите раздел **Защита**.

   Откроется окно со списком компонентов защиты. По умолчанию компонент Защита от сбора данных включен.

4. Если вы хотите выключить компонент Защита от сбора данных, установите переключатель напротив элемента **Защита от сбора данных** в положение  .

5. Если вы хотите изменить установленные по умолчанию параметры компонента Защита от сбора данных, в правой части окна выберите элемент **Защита от сбора данных**.

   Откроется окно **Параметры Защиты от сбора данных**.

6. Настройте параметры Защиты от сбора данных на вашем компьютере:

   - Если вы хотите, чтобы программа только обнаруживала и подсчитывала запросы на сервисы отслеживания, но не блокировала их, оставьте выбранный по умолчанию вариант **Обнаруживать запросы, не блокируя**.

   - Если вы хотите, чтобы программа блокировала запросы на сервисы отслеживания, выберите вариант **Блокировать обнаруженные запросы**. По ссылке **Категории и исключения** вы можете перейти в окно, где можно указать категории сервисов отслеживания, которые нужно блокировать.

7. Если вы не хотите, чтобы на веб-сайты отправлялся HTTP-заголовок, означающий запрет на сбор данных о ваших действиях, снимите флажок **Отправлять запрет на сбор данных**. По умолчанию этот флажок установлен.

8. Если вы хотите запретить сбор данных о ваших действиях при посещении веб-сайтов «Лаборатории Касперского» и ее партнеров, снимите флажок **Разрешить сбор данных на веб-сайтах «Лаборатории Касперского» и ее партнеров**. По умолчанию Защита от сбора данных не блокирует запросы на сервисы отслеживания на веб-сайтах «Лаборатории Касперского» и ее партнеров.

9. Если вы хотите запретить сбор данных на веб-сайтах, даже если при этом нарушается их работоспособность, снимите флажок **Разрешить сбор данных на несовместимых веб-сайтах**. По умолчанию Защита от сбора данных не блокирует запросы на сервисы отслеживания на веб-сайтах, о которых «Лаборатории Касперского» известно, что их работоспособность может быть нарушена в результате блокировки.

   > «Лаборатория Касперского» обновляет список несовместимых веб-сайтов по мере устранения проблем несовместимости.

Блокировка сервисов отслеживания по категориям

► *Чтобы настроить блокировку сервисов отслеживания по категориям, выполните следующие действия:*

1. Откройте главное окно программы.
2. Нажмите на кнопку в нижней части окна программы.

   Откроется окно **Настройка**.
3. В левой части окна выберите раздел **Защита**.

   Откроется окно со списком компонентов защиты. По умолчанию компонент Защита от сбора данных включен.
4. В правой части окна выберите компонент **Защита от сбора данных**.

   Откроется окно **Параметры Защиты от сбора данных**.
5. Выберите вариант **Блокировать обнаруженные запросы**.
6. По ссылке **Категории и исключения** перейдите в окно **Категории и исключения**.
7. Установите флажки напротив категорий сервисов отслеживания, которые программа должна блокировать.

Разрешение на сбор данных на отдельных веб-сайтах

► *Чтобы разрешить сбор данных на отдельных веб-сайтах, выполните следующие действия:*

1. Откройте главное окно программы.
2. Нажмите на кнопку в нижней части окна программы.

   Откроется окно **Настройка**.
3. В левой части окна выберите раздел **Защита**.

   Откроется окно со списком компонентов защиты. По умолчанию компонент Защита от сбора данных включен.

4. В правой части окна выберите элемент **Защита от сбора данных**.

   Откроется окно **Параметры Защиты от сбора данных**.

5. Выберите вариант **Блокировать обнаруженные запросы**.

6. По ссылке **Категории и исключения** перейдите в окно **Категории и исключения**.

7. По ссылке **Исключения** откройте окно **Исключения Защиты от сбора данных**.

8. Нажмите на кнопку **Добавить**.

9. В открывшемся окне укажите веб-адрес сайта, на котором вы хотите разрешить сбор данных, и нажмите на кнопку **Добавить**.

   Указанный веб-сайт будет добавлен в список исключений.

Вы также можете разрешить сбор данных на веб-сайте при его посещении в браузере (см. раздел «Управление защитой от сбора данных в браузере» на стр. 99).

Просмотр отчета о запросах на сервисы отслеживания

► *Чтобы просмотреть отчет о запросах на сервисы отслеживания, выполните следующие действия:*

1. Откройте главное окно программы.

2. Нажав на кнопку **Больше функций**, откройте окно **Инструменты**.

3. В окне **Инструменты** по ссылке **Защита приватности** откройте окно **Защита приватности**.

   В окне **Защита приватности** в блоке **Защита от сбора данных** отображается сводный отчет с информацией о категориях сервисов отслеживания и количестве отправленных на них запросов.

4. Для получения детального отчета об обнаруженных и заблокированных запросах на сервисы отслеживания откройте окно **Подробные отчеты** по ссылке **Подробнее** в блоке **Защита от сбора данных**.

Вы можете просматривать отчет об обнаруженных запросах на сервисы отслеживания в браузере (см. раздел «Управление защитой от сбора данных в браузере» на стр. 99).

Управление защитой от сбора данных в браузере

Вы можете управлять компонентом Защита от сбора данных непосредственно в браузере:

- включать компонент, если он выключен;
- просматривать статистику обнаруженных запросов на сервисы отслеживания;
- переходить в окно настройки Защиты от сбора данных;
- просматривать информацию о том, блокируются ли те или иные категории сервисов отслеживания;
- просматривать информацию о режиме работы компонента (см. раздел «О защите от сбора данных» на стр. 94) и о том, блокируются ли сервисы отслеживания на веб-сайте, открытом в браузере;
- изменять режим работы компонента, а также разрешать или запрещать блокировку сервисов отслеживания на веб-сайте, открытом в браузере.

► *Чтобы получить доступ к управлению компонентом Защита от сбора данных в браузере,*

нажмите на кнопку **Kaspersky Protection** в панели инструментов браузера.

В открывшемся меню отображается информация о работе компонента и элементы управления им.

Защита от баннеров при посещении веб-сайтов

Для защиты от баннеров в интернете предназначен компонент Анти-Баннер. Если компонент включен, вы можете выключать отображение баннеров непосредственно на веб-странице или же указать адрес веб-сайта и маску, по которой Kaspersky Total Security будет блокировать отображение баннеров на этом веб-сайте. По умолчанию Kaspersky Total Security защищает от наиболее распространенных типов баннеров.

В этом разделе

Включение компонента Анти-Баннер

► *Чтобы включить компонент Анти-Баннер, выполните следующие действия:*

1. Откройте главное окно программы.
2. Нажмите на кнопку  в нижней части окна программы.

   Откроется окно **Настройка**.
3. Выберите раздел **Защита**.
4. В правой части окна выберите компонент Анти-Баннер и включите его с помощью переключателя.

Выключение отображения баннера на веб-сайте

► *Чтобы выключить отображение баннера на веб-сайте, выполните следующие действия:*

1. Находясь на веб-сайте, наведите курсор мыши на баннер, отображение которого вы хотите выключить.
2. Нажмите на клавишу **CTRL** на клавиатуре.
3. В появившемся меню выберите пункт **Добавить в Анти-Баннер**.

   Откроется окно **Запрещенные веб-адреса**.
4. В окне **Запрещенные веб-адреса** нажмите на кнопку **Добавить**.

   Адрес баннера будет добавлен в список запрещенных веб-адресов.
5. Обновите веб-страницу в браузере, чтобы баннер перестал отображаться.

При последующих переходах на эту веб-страницу баннер не будет отображаться.

Выключение отображения всех баннеров на веб-сайте

Вы можете выключить отображение всех баннеров на определенном веб-сайте. Для этого необходимо указать маску этого веб-сайта и добавить ее в список запрещенных веб-адресов.

► *Чтобы выключить отображение всех баннеров на веб-сайте, выполните следующие действия:*

1. Откройте главное окно программы.
2. Нажмите на кнопку  в нижней части окна программы.

   Откроется окно **Настройка**.

3. Выберите раздел **Защита**.
4. Выберите компонент Анти-Баннер.

   Откроется окно **Параметры Анти-Баннера**.
5. Включите компонент Анти-Баннер с помощью переключателя в верхней части окна.
6. В окне **Параметры Анти-Баннера** по ссылке **Настроить запрещенные веб-адреса** откройте окно **Запрещенные веб-адреса**.
7. В окне **Запрещенные веб-адреса** нажмите на кнопку **Добавить**.
8. В открывшемся окне в поле **Маска веб-адреса (URL)** введите маску адреса веб-сайта, на котором вы хотите выключить отображение баннеров. Например: `http://example.com*`.
9. В качестве статуса для этого веб-сайта укажите **Активно**.
10. Нажмите на кнопку **Добавить**.

Kaspersky Total Security будет блокировать баннеры на сайте http://example.com.

Устранение следов работы на компьютере и в интернете

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 конфиденциальные данные, могут оказаться доступными злоумышленникам и посторонним лицам.

В состав Kaspersky Total Security входит мастер устранения следов активности пользователя в операционной системе.

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

1. Откройте главное окно программы.
2. Нажав на кнопку **Больше функций**, расположенную в нижней части главного окна, откройте окно **Инструменты**.
3. В левой части окна **Инструменты** по ссылке **Защита приватности** откройте окно **Защита приватности**.
4. В окне **Защита приватности** по ссылке **Устранение следов активности** запустите мастер устранения следов активности.

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 об обнаруженных следах активности и предлагаемых действиях для их устранения (см. рис. ниже).

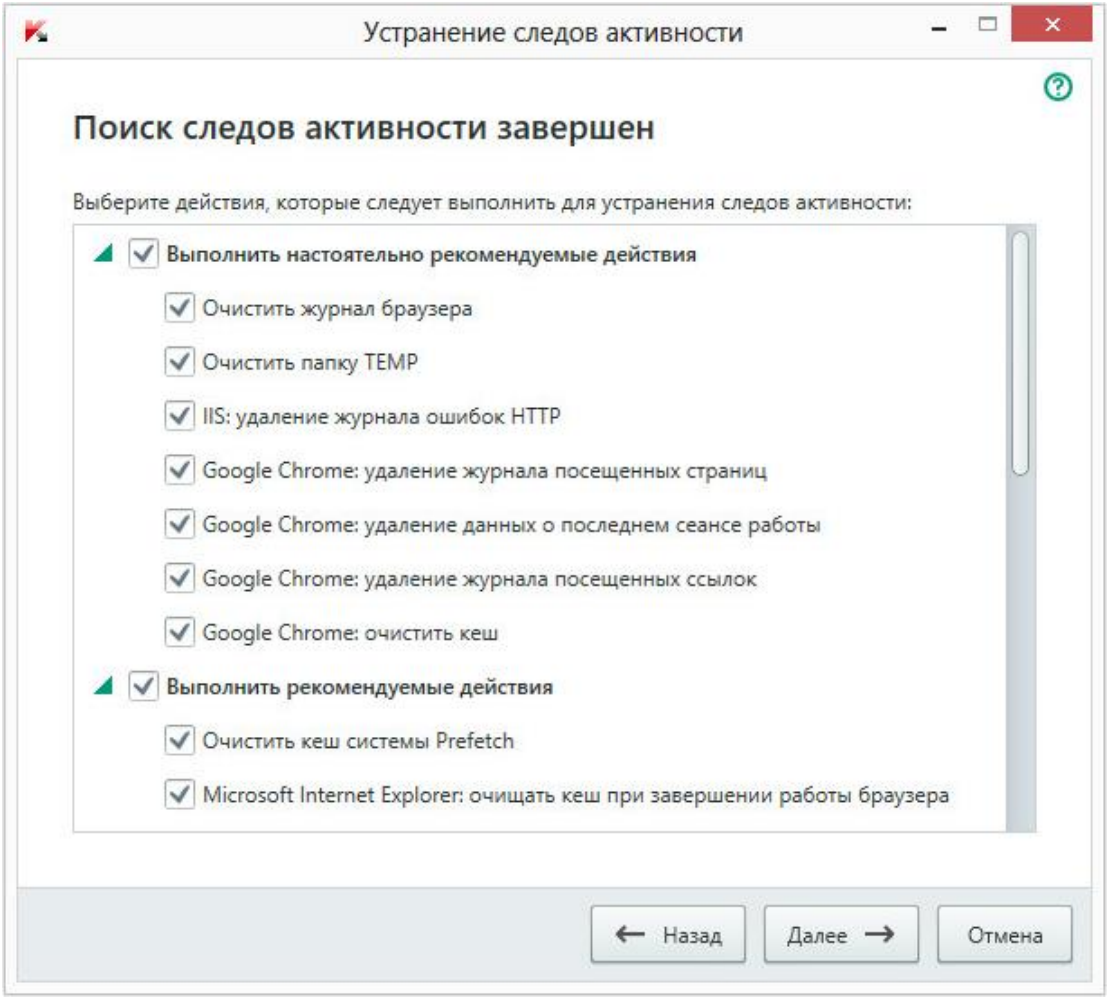

Рисунок 4. Обнаруженные следы активности и рекомендации по их устранению

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.

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 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

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

Контроль работы пользователей на компьютере и в интернете

Этот раздел содержит информацию о том, как с помощью Kaspersky Total Security контролировать действия пользователей на компьютере и в интернете.

В этом разделе

Использование Родительского контроля

Родительский контроль позволяет контролировать действия разных пользователей на компьютере и в сети. С помощью Родительского контроля вы можете ограничивать доступ к интернет-ресурсам и программам, а также просматривать отчеты о действиях пользователей.

В настоящее время доступ к компьютеру и интернет-ресурсам получает все большее количество детей и подростков. При использовании компьютера и интернета дети сталкиваются с целым рядом угроз:

- потеря времени и / или денег при посещении чатов, игровых ресурсов, интернет-магазинов, аукционов;
- доступ к веб-ресурсам, предназначенным для взрослой аудитории (например, содержащим порнографические, экстремистские материалы, затрагивающим темы оружия, наркотиков, насилия);
- загрузка файлов, зараженных вредоносными программами;
- ущерб для здоровья от чрезмерно длительного нахождения за компьютером;
- контакты с незнакомыми людьми, которые под видом сверстников могут получить информацию о ребенке (например, настоящее имя, адрес, время, когда никого нет дома).

Родительский контроль позволяет снизить риски, связанные с работой на компьютере и в интернете. Для этого используются следующие функции:

- ограничение использования компьютера и интернета по времени;
- создание списков разрешенных и запрещенных для запуска игр и приложений, а также временное ограничение запуска разрешенных программ;
- создание списков разрешенных и запрещенных для доступа веб-сайтов, выбор категорий не рекомендованного к просмотру содержимого веб-ресурсов;
- включение режима безопасного поиска с помощью поисковых систем (при этом ссылки на веб-сайты с сомнительным содержимым не отображаются в результатах поиска);
- ограничение загрузки файлов из интернета;
- создание списков контактов, запрещенных или разрешенных для общения в социальных сетях;
- просмотр текста переписки в социальных сетях;

- запрет пересылки определенных персональных данных;
- поиск заданных ключевых слов в тексте переписки.

Вы можете настраивать функции Родительского контроля для каждой учетной записи пользователя на компьютере отдельно. Вы также можете просматривать отчеты Родительского контроля о действиях контролируемых пользователей компьютера.

Переход к настройке параметров Родительского контроля

► *Чтобы перейти к настройке параметров Родительского контроля, выполните следующие действия:*

1. Откройте главное окно программы.
2. В главном окне программы нажмите на кнопку **Родительский контроль**.
3. Если доступ к параметрам Родительского контроля не защищен паролем, программа предложит задать пароль. Выберите один из предложенных вариантов действия:
   - Если вы хотите защитить паролем доступ к параметрам Родительского контроля, выполните следующие действия:
     a. Заполните поля **Пароль** и **Подтверждение пароля** и нажмите на кнопку **Продолжить**.
     b. В окне **Область действия пароля** нажмите на кнопку **Создать пароль**.
     c. В окне **Введите пароль** повторите ввод пароля и нажмите на кнопку **Войти**.
   - Если вы не хотите защищать паролем доступ к параметрам Родительского контроля, по ссылке **Пропустить** перейдите к настройке параметров Родительского контроля.

   Откроется окно **Родительский контроль**.
4. Выберите учетную запись пользователя и по ссылке **Настроить ограничения** перейдите к окну настройки параметров Родительского контроля.

Контроль использования компьютера

Родительский контроль позволяет задать ограничения времени, проводимого пользователем за компьютером. Вы можете указать интервал времени, когда Родительский контроль должен блокировать доступ к компьютеру (время сна), а также общее ограничение времени использования компьютера в течение дня. Можно указать различные ограничения для рабочих и выходных дней.

► *Чтобы настроить ограничения времени использования компьютера, выполните следующие действия:*

1. Перейдите в окно настройки параметров Родительского контроля (см. раздел «Переход к настройке параметров Родительского контроля» на стр. 108).

2. В окне настройки параметров Родительского контроля выберите раздел **Компьютер**.

3. Чтобы указать интервал времени, в течение которого Родительский контроль будет блокировать доступ к компьютеру, в блоках **Рабочие дни** и **Выходные дни** установите флажок **Блокировать доступ с**.

4. В раскрывающемся списке рядом с флажком **Блокировать доступ с** укажите время начала блокировки.

5. В раскрывающемся списке **до** укажите время окончания блокировки.

   Расписание времени использования компьютера также можно задать с помощью таблицы. Таблица отображается при нажатии на кнопку  .

   Родительский контроль будет блокировать пользователю доступ к компьютеру в течение указанного интервала времени.

6. Чтобы ограничить общее время использования компьютера в течение дня, в блоках **Рабочие дни** и **Выходные дни** установите флажок **Разрешить доступ не более** и выберите интервал времени в раскрывающемся списке рядом с флажком.

   Родительский контроль будет блокировать пользователю доступ к компьютеру, когда общее время использования компьютера в течение дня превысит указанный интервал.

7. Чтобы задать перерывы при использовании компьютера пользователем, в блоке **Перерывы в работе** установите флажок **Делать перерыв** и выберите периодичность (например, каждый час) и длительность (например, 10 минут) перерывов в раскрывающихся списках рядом с флажком.

8. Установите переключатель, расположенный в верхней части окна, в положение **Контроль включен**  .

Родительский контроль будет блокировать доступ пользователя к компьютеру в соответствии с указанными параметрами.

Контроль использования интернета

С помощью Родительского контроля вы можете ограничить время использования интернета, а также запретить доступ пользователя к избранным категориям веб-сайтов и отдельным веб-сайтам. Кроме того, вы можете запретить пользователю загрузку из интернета файлов определенных типов (например, архивов, видео).

► *Чтобы настроить ограничения времени использования интернета, выполните следующие действия:*

1. Перейдите в окно настройки параметров Родительского контроля (см. раздел «Переход к настройке параметров Родительского контроля» на стр. 108).

2. В окне настройки параметров Родительского контроля выберите раздел **Интернет**.

3. Если вы хотите ограничить общее время использования интернета по рабочим дням, в блоке **Ограничение доступа в интернет** установите флажок **Ограничивать доступ в рабочие дни до** и выберите ограничение по времени в раскрывающемся списке рядом с флажком.

4. Если вы хотите ограничить общее время использования интернета по выходным дням, установите флажок **Ограничивать доступ в выходные дни до** и выберите ограничение по времени в раскрывающемся списке рядом с флажком.

5. Установите переключатель, расположенный в верхней части окна, в положение **Контроль включен**  .

Родительский контроль будет ограничивать общее время, проводимое пользователем в интернете, в соответствии с указанными значениями.

► *Чтобы ограничить посещение определенных веб-сайтов, выполните следующие действия:*

1. Перейдите в окно настройки параметров Родительского контроля (см. раздел «Переход к настройке параметров Родительского контроля» на стр. 108).

2. В окне настройки параметров Родительского контроля выберите раздел **Интернет**.

3. Чтобы в результатах поиска не отображалось содержимое «для взрослых», в блоке **Контроль посещения веб-сайтов** установите флажок **Включить безопасный поиск**.

   При поиске информации на веб-сайтах, таких как Google™, YouTube™ (только для пользователей, не вошедших на сайт youtube.com под своей учетной записью), Bing®, Yahoo!™, Mail.ru, ВКонтакте, Yandex среди результатов поиска не будет присутствовать содержимое «для взрослых».

4. Чтобы запретить доступ к веб-сайтам определенных категорий, выполните следующие действия:

   a. В блоке **Контроль посещения веб-сайтов** установите флажок **Ограничить доступ к веб-сайтам**.

   b. Выберите вариант **Блокировать доступ к веб-сайтам из выбранных категорий** и по ссылке **Выбрать категории веб-сайтов** откройте окно **Блокировать доступ к категориям веб-сайтов**.

   c. Установите флажки напротив категорий веб-сайтов, открытие которых необходимо блокировать.

      Родительский контроль будет блокировать открытие веб-сайта пользователем, если его содержимое относится к какой-либо из запрещенных категорий.

5. Чтобы запретить доступ к отдельным веб-сайтам, выполните следующие действия:

   a. В блоке **Контроль посещения веб-сайтов** установите флажок **Ограничить доступ к веб-сайтам**.

   b. По ссылке **Настроить исключения** откройте окно **Исключения**.

c. В нижней части окна нажмите на кнопку **Добавить**.

   Откроется окно добавления новой маски веб-адреса.

d. Введите адрес веб-сайта, посещение которого необходимо запретить, в поле **Маска веб-адреса**.

e. Выберите область действия запрета в блоке **Область применения**: весь веб-сайт или только указанная веб-страница.

f. Если вы хотите запретить посещение указанного веб-сайта, в блоке **Действие** выберите вариант **Запретить**.

g. Нажмите на кнопку **Добавить**.

Указанный веб-сайт появится в списке в окне **Исключения**. Закройте окно **Исключения**.

6. Установите переключатель, расположенный в верхней части окна, в положение **Контроль включен**  .

Родительский контроль будет блокировать посещение веб-сайтов в соответствии с указанными параметрами.

► *Чтобы запретить загрузку из интернета файлов определенных типов, выполните следующие действия:*

1. Перейдите в окно настройки параметров Родительского контроля (см. раздел «Переход к настройке параметров Родительского контроля» на стр. 108).

2. В окне настройки параметров Родительского контроля выберите раздел **Интернет**.

3. В блоке **Запрет загрузки файлов** установите флажки напротив типов файлов, загрузку которых необходимо блокировать.

4. Установите переключатель, расположенный в верхней части окна, в положение **Контроль включен**  .

Родительский контроль будет блокировать загрузку файлов указанных типов из интернета.

Контроль запуска игр и программ

С помощью Родительского контроля вы можете разрешать или запрещать пользователю запуск игр в зависимости от их возрастной категории. Также вы можете запретить пользователю запуск определенных программ (например, игр, IM-клиентов) или ограничить время использования программ.

► *Чтобы запретить запуск игр, содержимое которых не соответствует возрасту пользователя, выполните следующие действия:*

1. Перейдите в окно настройки параметров Родительского контроля (см. раздел «Переход к настройке параметров Родительского контроля» на стр. 108).

2. В окне настройки параметров Родительского контроля выберите раздел **Программы**.

3. Если вы хотите заблокировать запуск всех игр, содержимое которых не соответствует возрасту пользователя, установите флажок **Ограничить запуск игр для возраста младше** и выберите возрастное ограничение в раскрывающемся списке рядом с флажком.

4. Если вы хотите заблокировать запуск игр с определенным содержимым, выполните следующие действия:

   a. Установите флажок **Блокировать игры из категорий для взрослых**.

   b. По ссылке **Выбрать категории игр** откройте окно **Блокировать игры по категориям**.

   c. Установите флажки напротив категорий содержимого игр, которые нужно блокировать.

5. Вернитесь в раздел **Программы**.

6. Установите переключатель, расположенный в верхней части окна, в положение **Контроль включен**  .

► *Чтобы ограничить запуск определенной программы, выполните следующие действия:*

1. Перейдите в окно настройки параметров Родительского контроля (см. раздел «Переход к настройке параметров Родительского контроля» на стр. 108).

2. В окне настройки параметров Родительского контроля выберите раздел **Программы**.

3. По кнопке **Добавить программу** откройте окно **Открыть** и выберите исполняемый файл программы.

   Выбранная программа появится в списке **Блокировать указанные программы**. Kaspersky Total Security автоматически добавит эту программу в определенную категорию, например, *Игры*.

4. Если вы хотите заблокировать запуск программы, в раскрывающемся списке справа от названия программы выберите элемент **Блокировать**.

5. Если вы хотите заблокировать запуск всех программ определенной категории, установите флажок напротив названия категории в списке (например, вы можете заблокировать программы категории *Игры*).

6. Если вы хотите установить ограничения на время использования программы, в раскрывающемся списке справа от названия программы выберите элемент **По правилам**.

   Откроется окно **Ограничение использования программы**.

7. Если вы хотите ограничить время использования программы в рабочие и выходные дни, в блоках **Рабочие дни** и **Выходные дни** установите флажок **Разрешить доступ не более** и в раскрывающемся списке укажите количество часов в день, в течение которых пользователю разрешено использовать программу. Также вы можете указать точное время, когда пользователю разрешено / запрещено использовать программу, воспользовавшись таблицей **Точное время использования**.

8. Если вы хотите задать перерывы в использовании программы, в блоке **Перерывы в работе** установите флажок **Делать перерыв** и выберите частоту и длительность перерыва в раскрывающихся списках.

9. Нажмите на кнопку **Сохранить**.

10. Установите переключатель, расположенный в верхней части окна, в положение **Контроль включен**  .

Родительский контроль будет применять заданные ограничения при работе пользователя с программой.

Контроль общения в социальных сетях

С помощью Родительского контроля вы можете просматривать переписку пользователя в социальных сетях и блокировать обмен сообщениями с определенными контактами.

► *Чтобы настроить контроль переписки пользователя, выполните следующие действия:*

1. Перейдите в окно настройки параметров Родительского контроля (см. раздел «Переход к настройке параметров Родительского контроля» на стр. 108).

2. В окне настройки параметров Родительского контроля выберите раздел **Общение**.

3. Чтобы просмотреть переписку и, при необходимости, заблокировать определенные контакты, выполните следующие действия:

   a. Выберите вариант **Запретить общение со всеми, кроме разрешенных известных контактов**.

   b. По ссылке **Известные контакты** откройте окно **Отчет об общении**.

   c. Просмотрите контакты, с которыми переписывался пользователь. Вы можете отобразить в окне определенные контакты одним из следующих способов:

      - Чтобы просмотреть переписку пользователя в определенной социальной сети, выберите нужный элемент в раскрывающемся списке в левой части окна.

      - Чтобы отобразить контакты, с которыми пользователь вел наиболее активную переписку, в раскрывающемся списке в правой части окна выберите элемент **По количеству сообщений**.

- Чтобы отобразить контакты, с которыми пользователь переписывался в определенный день, в раскрывающемся списке в правой части окна выберите элемент **По дате переписки**.

d. Чтобы просмотреть переписку пользователя с определенным контактом, нажмите на контакт в списке.

   Откроется окно с историей переписки с этим контактом.

e. Если вы хотите заблокировать переписку пользователя с выбранным контактом, нажмите на кнопку **Запретить общение**.

4. Установите переключатель, расположенный в верхней части окна, в положение **Контроль включен**  .

Родительский контроль будет блокировать обмен сообщениями между пользователем и выбранным контактом.

Контроль содержимого переписки

С помощью Родительского контроля вы можете отслеживать и запрещать пользователю употребление в переписке указанных персональных данных (например, фамилии, номера телефона, номера банковских карт) и ключевых слов (например, ненормативной лексики).

► *Чтобы настроить контроль пересылки персональных данных, выполните следующие действия:*

1. Перейдите в окно настройки параметров Родительского контроля (см. раздел «Переход к настройке параметров Родительского контроля» на стр. 108).

2. В окне настройки параметров Родительского контроля выберите раздел **Контроль содержимого**.

3. В блоке **Контроль передачи персональных данных** установите флажок **Запретить передачу персональных данных третьим лицам**.

4. По ссылке **Изменить список персональных данных** откройте окно **Список персональных данных**.

5. В нижней части окна нажмите на кнопку **Добавить**.

   Откроется окно добавления персональных данных.

6. Выберите тип персональных данных (например, «номер телефона») по ссылке или введите описание в поле **Название поля**.

7. Укажите персональные данные (например, фамилию, номер телефона) в поле **Значение**.

8. Нажмите на кнопку **Добавить**.

   Персональные данные появятся в списке в окне **Список персональных данных**.

9. Закройте окно **Список персональных данных**.

10. Установите переключатель, расположенный в верхней части окна, в положение **Контроль включен**  .

Родительский контроль будет отслеживать и блокировать употребление указанных персональных данных в переписке через интернет.

► *Чтобы настроить контроль употребления ключевых слов в переписке, выполните следующие действия:*

1. Перейдите в окно настройки параметров Родительского контроля (см. раздел «Переход к настройке параметров Родительского контроля» на стр. 108).

2. В окне настройки параметров Родительского контроля выберите раздел **Контроль содержимого**.

3. В блоке **Контроль употребления ключевых слов** установите флажок **Обнаруживать употребление ключевых слов**.

4. По ссылке **Изменить список ключевых слов** откройте окно **Список ключевых слов**.

5. В нижней части окна нажмите на кнопку **Добавить**.

   Откроется окно для добавления ключевого слова.

6. Введите ключевую фразу в поле **Значение** и нажмите на кнопку **Добавить**.

   Указанная ключевая фраза появится в списке ключевых слов в окне **Список ключевых слов**.

7. Закройте окно **Список ключевых слов**.

8. Установите переключатель, расположенный в верхней части окна, в положение **Контроль включен**  .

Родительский контроль будет обнаруживать передачу сообщений, содержащих указанную ключевую фразу, при переписке через интернет, и включать информацию о таких сообщениях в отчет.

Просмотр отчета о действиях пользователя

Вы можете просмотреть отчеты о действиях каждого пользователя, для которого настроен Родительский контроль, отдельно для каждой категории контролируемых событий.

► *Чтобы просмотреть отчет о действиях контролируемого пользователя, выполните следующие действия:*

1. Перейдите в окно настройки параметров Родительского контроля (см. раздел «Переход к настройке параметров Родительского контроля» на стр. 108).

2. Выберите учетную запись пользователя и по ссылке **Посмотреть отчет** перейдите к окну отчетов.

3. В блоке с нужным типом ограничения (например, **Интернет** или **Общение**) откройте отчет о контролируемых действиях по ссылке **Подробнее**.

В окне отобразится отчет о контролируемых действиях пользователя.

Удаленное управление защитой компьютера

В этом разделе содержится информация о том, как вы можете удаленно управлять защитой вашего компьютера, если на нем установлена программа Kaspersky Total Security.

В этом разделе

Об удаленном управлении защитой компьютера

Если на компьютере установлена программа Kaspersky Total Security, вы можете управлять защитой этого компьютера удаленно. Удаленное управление защитой компьютера выполняется на портале My Kaspersky. Чтобы удаленно управлять защитой компьютера, вам нужно зарегистрироваться на портале My Kaspersky, войти в свою учетную запись на портале My Kaspersky и перейти в раздел **Устройства**.

На портале My Kaspersky вы можете решать следующие задачи по обеспечению безопасности вашего компьютера:

- просматривать список проблем безопасности на компьютере и удаленно устранять их;
- проверять компьютер на вирусы и другие программы, представляющие угрозу;
- обновлять базы и программные модули;
- настраивать компоненты программы Kaspersky Total Security.

Если проверка компьютера запущена из портала My Kaspersky, то Kaspersky Total Security обрабатывает обнаруженные объекты в автоматическом режиме без вашего участия. В случае обнаружения вируса или другой программы, представляющей угрозу, программа Kaspersky Total Security попытается выполнить лечение без перезагрузки компьютера. Если лечение без перезагрузки компьютера невозможно, на портале My Kaspersky в списке проблем защиты компьютера появляется сообщение о том, что для лечения компьютера требуется перезагрузка.

Если на портале My Kaspersky в списке обнаруженных объектов более 10 элементов, то они группируются. В этом случае через портал обнаруженные объекты можно обработать только одновременно, без возможности просмотреть каждый объект. Для просмотра отдельных объектов в этом случае рекомендуется использовать интерфейс программы, установленной на компьютере.

Подробную информацию о работе с порталом вы найдете в Справке портала My Kaspersky (https://help.kaspersky.com/KPC/1.0/ru-RU/index.htm).

Об учетной записи на портале My Kaspersky

Учетная запись на портале My Kaspersky требуется для входа на портал My Kaspersky https://center.kaspersky.com, а также для работы с порталом и некоторыми программами «Лаборатории Касперского».

Если у вас еще нет учетной записи на портале My Kaspersky, вы можете создать ее на портале или из программ, совместимых с порталом. Вы также можете использовать для входа на портал учетные данные других ресурсов «Лаборатории Касперского».

При создании учетной записи на портале My Kaspersky вам нужно указать действующий адрес электронной почты и придумать пароль. Пароль должен состоять не менее чем из 8 символов и содержать хотя бы одну цифру, одну заглавную и одну строчную латинские буквы. Пробелы не допускаются.

> Если введенный пароль слишком простой или распространенный, учетная запись не будет создана.

При создании учетной записи вы можете задать секретный вопрос. Этот вопрос обеспечивает дополнительную защиту при восстановлении забытого пароля.

После создания учетной записи на указанный вами адрес электронной почты будет выслано сообщение, содержащее ссылку для активации вашей учетной записи.

Активируйте учетную запись по ссылке из сообщения в течение 7 дней, иначе ваша учетная запись будет удалена.

Переход к удаленному управлению защитой компьютера

► *Чтобы перейти к удаленному управлению защитой компьютера, выполните следующие действия:*

1. Откройте главное окно программы.
2. Нажмите на кнопку **Управление в интернете**.
3. В окне **Управление в интернете** нажмите на кнопку **Подключить компьютер к My Kaspersky**.

   В окне **Управление в интернете** загрузится форма подключения к порталу My Kaspersky, если подключение не было выполнено ранее. Заполните поля и выполните вход в портал My Kaspersky.

   > Подключение к порталу My Kaspersky может отсутствовать в результате сбоя в работе портала. В этом случае Kaspersky Total Security показывает уведомление о том, что на портале My Kaspersky возникли проблемы, которые решаются специалистами «Лаборатории Касперского». Если вы не можете подключиться к порталу My Kaspersky в результате сбоя в работе портала, повторите попытку подключения позже.

В окне браузера по умолчанию откроется страница портала My Kaspersky на разделе **Устройства**.

Сохранение ресурсов операционной системы для компьютерных игр

При одновременной работе Kaspersky Total Security и некоторых программ (в особенности компьютерных игр) в полноэкранном режиме иногда могут возникать следующие неудобства:

- работа программы или игры замедляется из-за недостатка системных ресурсов;
- окна уведомлений Kaspersky Total Security отвлекают от игры.

Чтобы не изменять параметры Kaspersky Total Security 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 Kaspersky Total Security 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 главное окно программы.
2. Нажмите на кнопку  в нижней части окна программы.

   Откроется окно **Настройка**.
3. В левой части окна выберите раздел **Производительность**.

   В окне отобразятся параметры производительности Kaspersky Total Security.
4. В блоке **Игровой профиль** установите флажок **Использовать игровой профиль**.

Работа с неизвестными программами

С помощью Kaspersky Total Security вы сможете снизить риски, связанные с использованием неизвестных программ (например, риски заражения компьютера вирусами и другими программами, представляющими угрозу, и нежелательного изменения параметров операционной системы).

В состав Kaspersky Total Security входят компоненты и инструменты, позволяющие проверить репутацию программы и контролировать активность программы на вашем компьютере.

В этом разделе

Проверка репутации программы

Kaspersky Total Security 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 Контролем программ или 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 программы 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).

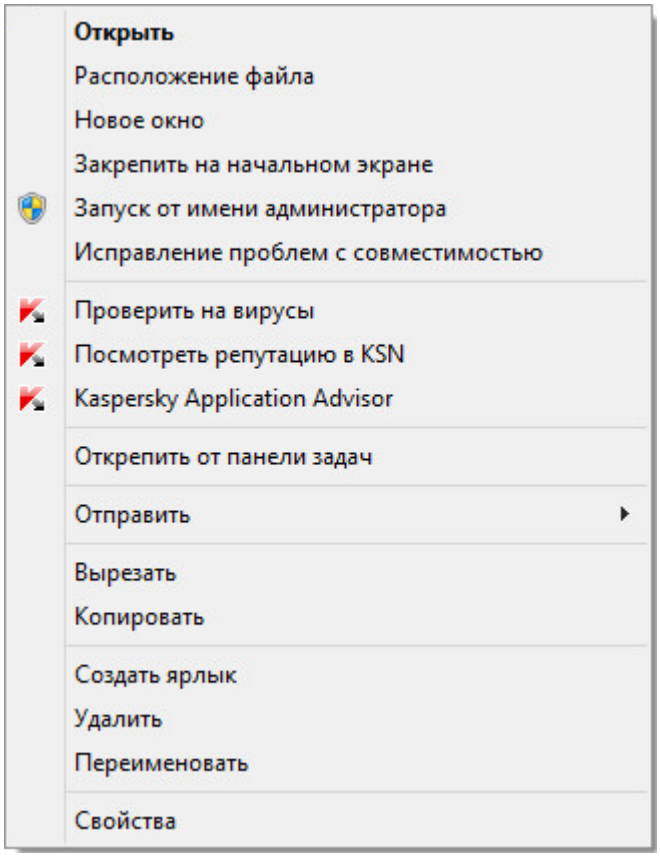

Рисунок 5. Контекстное меню объекта

Откроется окно со сведениями о репутации программы в Kaspersky Security Network.

См. также

Участие в Kaspersky Security Network 167

Контроль действий программы на компьютере и в сети

Компонент Контроль программ предотвращает выполнение программами опасных для операционной системы действий, а также обеспечивает контроль доступа к ресурсам операционной системы и вашим персональным данным.

Контроль программ отслеживает действия, которые совершают в операционной системе программы, установленные на компьютере, и регулирует их на основании правил. Эти правила регламентируют подозрительную активность программ, в том числе доступ программ к защищаемым ресурсам (например, к файлам, папкам, ключам реестра, сетевым адресам).

При работе на 64-разрядных операционных системах недоступны для настройки права программ на выполнение следующих действий:

- прямой доступ к физической памяти;
- управление драйверами принтера;
- создание сервиса;
- открытие сервиса для чтения;
- открытие сервиса для изменения;
- изменение конфигурации сервиса;
- управление сервисом;
- запуск сервиса;
- удаление сервиса;
- доступ к внутренним данным браузера;
- доступ к критическим объектам операционной системы;
- доступ к хранилищу паролей;
- установка прав отладчика;
- использование программных интерфейсов операционной системы;
- использование программных интерфейсов операционной системы (DNS).

При работе на 64-разрядной Microsoft Windows 8 дополнительно недоступны для настройки права программ на выполнение следующих действий:

- отправка оконных сообщений другим процессам;
- подозрительные операции;
- установка перехватчиков;
- перехват входящих событий потока;
- создание снимков экрана.

Сетевую активность программ контролирует компонент Сетевой экран.

При первом запуске программы на компьютере Контроль программ проверяет ее безопасность и помещает в одну из групп (Доверенные, Недоверенные, Сильные ограничения или Слабые ограничения). Группа определяет правила, которые Kaspersky Total Security применяет для контроля активности этой программы.

Kaspersky Total Security помещает программы в группы доверия (Доверенные, Недоверенные, Сильные ограничения или Слабые ограничения), только если включен компонент Контроль программ или Сетевой экран, а также когда включены оба эти компонента. Если оба эти компонента выключены, функциональность распределения программ по группам доверия не работает.

Вы можете изменить правила контроля действий программы вручную.

Настройка параметров Контроля программ

► *Чтобы настроить параметры Контроля программ, выполните следующие действия:*

1. Откройте главное окно Kaspersky Total Security.
2. Нажмите на кнопку **Больше функций**, расположенную в нижней части главного окна.

   Откроется окно **Инструменты**.

3. Выберите блок **Контроль программ**.

   Откроется окно **Контроль программ**.

4. В окне **Контроль программ** в блоке **Программы** по ссылке **Управление программами** откройте окно **Управление программами**.

5. Выберите нужную программу в списке и откройте окно **Правила программы** двойным щелчком мыши.

6. Чтобы настроить правила доступа программы к ресурсам операционной системы, выполните следующие действия:

   a. На закладке **Файлы и системный реестр** выберите нужную категорию ресурсов.

   b. В графе с возможным действием над ресурсом (**Чтение**, **Запись**, **Удаление** или **Создание**) нажатием на значок откройте меню и выберите в нем нужное значение (**Разрешить**, **Запретить**, **Запросить действие** или **Наследовать**).

7. Чтобы настроить права программы на выполнение различных действий в операционной системе, выполните следующие действия:

   a. На закладке **Права** выберите нужную категорию прав.

   b. В графе **Действие** нажатием на значок откройте меню и выберите в нем нужное значение (**Разрешить**, **Запретить**, **Запросить действие** или **Наследовать**).

8. Чтобы настроить права программы на выполнение различных действий в сети, выполните следующие действия:

   a. На закладке **Сетевые правила** нажмите на кнопку **Добавить**.

      Откроется окно **Сетевое правило**.

   b. В открывшемся окне задайте нужные параметры правила и нажмите на кнопку **Сохранить**.

   c. Назначьте приоритет для нового правила. Для этого выделите правило и переместите его вверх или вниз по списку.

9. Чтобы исключить некоторые действия программы из проверки Контролем программ, на закладке **Исключения** установите флажки для действий, которые не нужно контролировать.

10. Нажмите на кнопку **Сохранить**.

    Все исключения, созданные в правилах контроля программ, доступны в окне настройки Kaspersky Total Security в разделе **Угрозы и исключения**.

Компонент Контроль программ будет отслеживать и ограничивать действия программы в соответствии с настроенными параметрами.

О доступе программ к веб-камере

Злоумышленники могут пытаться получить несанкционированный доступ к веб-камере с помощью специальных программ. Kaspersky Total Security блокирует несанкционированный доступ программ к веб-камере и показывает уведомление о том, что доступ заблокирован. По умолчанию Kaspersky Total Security блокирует доступ к веб-камере программам, которые входят в группы доверия «Сильные ограничения» и «Недоверенные».

Вы можете разрешить доступ к веб-камере программам (см. раздел «Разрешение доступа программы к веб-камере» на стр. 131), входящим в группы «Сильные ограничения» и «Недоверенные», в окне настройки Контроля программ. Если к веб-камере пытается подключиться программа, входящая в группу доверия «Слабые ограничения», Kaspersky Total Security показывает уведомление и предлагает вам самостоятельно принять решение о том, предоставлять этой программе доступ к веб-камере или нет.

Если к веб-камере пытается подключиться программа, которой разрешен доступ по умолчанию, Kaspersky Total Security показывает уведомление. В уведомлении содержится информация о том, что установленная на компьютере программа (например, Skype™) сейчас получает изображение с веб-камеры. В раскрывающемся списке уведомления вы можете запретить доступ программы к веб-камере или перейти к настройке параметров доступа программ к веб-камере (см. раздел «Настройка параметров доступа программ к веб-камере» на стр. 130). Это уведомление не отображается, если на вашем компьютере уже есть программы, запущенные в полноэкранном режиме.

Также в раскрывающемся списке уведомления о получении видеоданных программой вы можете выключить показ уведовлений или перейти к настройке отображения уведомлений (см. раздел «Настройка параметров доступа программ к веб-камере» на стр. 130).

Kaspersky Total Security по умолчанию разрешает доступ к веб-камере программам, для которых требуется ваше разрешение, если графический интерфейс программы находится в процессе загрузки, выгрузки или не отвечает, и вы не можете вручную разрешить доступ.

Функциональность защиты доступа к веб-камере имеет следующие особенности и ограничения:

- Программа контролирует видео и статические изображения, полученные в результате обработки данных веб-камеры.
- Программа контролирует аудиосигнал, если он является частью видеопотока, получаемого с веб-камеры.
- Программа Kaspersky Total Security контролирует только веб-камеры, подключаемые по интерфейсу USB или IEEE1394 и отображаемые в Диспетчере устройств Windows как Устройства обработки изображений (Imaging Device).

Ознакомиться со списком поддерживаемых веб-камер вы можете по ссылке (http://support.kaspersky.ru/12004).

Чтобы защита от несанкционированного доступа к веб-камере работала, должен быть включен компонент Контроль программ.

Настройка параметров доступа программ к веб-камере

► *Чтобы настроить параметры доступа программ к веб-камере, выполните следующие действия:*

1. Откройте главное окно программы.
2. Нажмите на кнопку  в нижней части окна программы.

   Откроется окно **Настройка**.

3. В разделе **Защита** в правой части окна выберите **Доступ к веб-камере**.

4. Настройте параметры доступа к веб-камере на вашем компьютере:

   - Если вы хотите запретить доступ всех программ к веб-камере, установите флажок **Запретить всем программам доступ к веб-камере**.

   - Если вы хотите получать уведомление о том, что веб-камеру использует программа, которой это разрешено, установите флажок **Показывать уведомление, когда веб-камеру использует программа, которой это разрешено**.

   - Если вы хотите разрешить доступ к веб-камере всем программам, в окне **Настройка** на закладке **Защита** с помощью переключателя выключите контроль доступа к веб-камере.

Разрешение доступа программы к веб-камере

► *Чтобы разрешить доступ программы к веб-камере, выполните следующие действия:*

1. Откройте главное окно программы.

2. Нажмите на кнопку **Больше функций**.

   Откроется окно **Инструменты**.

3. В окне **Инструменты** в блоке **Контроль программ** нажмите на кнопку **Подробнее**.

   Откроется окно **Контроль программ**.

4. В окне **Контроль программ** в блоке **Программы** по ссылке **Управление программами** откройте окно **Управление программами**.

5. Выберите программу в списке, которой вы хотите разрешить доступ к веб-камере, и откройте окно **Правила программы** двойным щелчком мыши.

6. В окне **Правила программы** перейдите на закладку **Права**.

7. В списке категорий прав выберите пункт **Изменение операционной системы** → **Подозрительные изменения в операционной системе** → **Доступ к веб-камере**.

8. В графе **Действие** нажатием на значок откройте меню и выберите пункт **Разрешить**.

9. Нажмите на кнопку **Сохранить**.

Доступ программы к веб-камере будет разрешен.

О доступе программ к устройствам записи звука

Злоумышленники могут пытаться получить несанкционированный доступ к устройствам записи звука с помощью специальных программ. *Устройства записи звука* – это микрофоны, подключаемые к компьютеру или встроенные в компьютер, способные передавать аудиопоток через интерфейс звуковой карты («на вход»). Kaspersky Total Security контролирует доступ программ к устройствам записи звука и защищает от несанкционированного перехвата аудиосигнала.

По умолчанию Kaspersky Total Security запрещает программам из групп доверия «Недоверенные» и «Сильные ограничения» получать аудиосигнал, поступающий с подключенных к компьютеру устройств записи звука. Вы можете вручную разрешать программам доступ к устройствам записи звука (см. раздел «Настройка параметров доступа программы к устройствам записи звука» на стр. 133).

Если к устройству записи звука обращается программа из группы доверия «Слабые ограничения», Kaspersky Total Security показывает уведомление и предлагает вам самостоятельно решить, разрешать такой программе доступ к устройству записи звука или запрещать. Если Kaspersky Total Security не может показать такое уведомление (например, еще не загрузился графический интерфейс Kaspersky Total Security), программе из группы доверия «Слабые ограничения» разрешен доступ к устройству записи звука.

Для всех программ, входящих в группу «Доверенные», доступ к устройствам записи звука разрешен по умолчанию.

Функциональность защиты доступа программ к устройствам записи звука имеет следующие особенности:

- Для работы функциональности необходимо, чтобы был включен компонент Контроль программ.
- Если программа начала получать аудиосигнал до запуска компонента Контроль программ, Kaspersky Total Security разрешает программе получение аудиосигнала и не показывает никаких уведомлений.
- При изменении параметров доступа программы к устройствам записи звука (например, программе было запрещено получение аудиосигнала в окне параметров Контроля программ), чтобы программа перестала получать аудиосигнал, требуется перезапуск этой программы.
- Контроль доступа к устройствам записи звука не зависит от параметров доступа программ к веб-камере.
- Если графический интерфейс программы еще не загрузился, программам, для которых установлено разрешение «Запросить действие», разрешается получение аудиосигнала.
- Kaspersky Total Security защищает доступ только к встроенным микрофонам и внешним микрофонам. Другие устройства передачи звука не поддерживаются.

Программа не гарантирует защиту аудиосигнала, передаваемого с таких устройств, как DSLR-камеры, портативные видеокамеры, экшн-камеры.

Настройка параметров доступа программы к устройствам записи звука

► *Чтобы настроить параметры доступа программы к устройствам записи звука, выполните следующие действия:*

1. Откройте главное окно программы.
2. Нажмите на кнопку **Больше функций**, расположенную в нижней части главного окна.

   Откроется окно **Инструменты**.

3. Выберите блок **Контроль программ**.

   Откроется окно **Контроль программ**.

4. По ссылке **Управление программами** откройте окно **Управление программами**.

5. Выберите программу в списке, которой вы хотите разрешить доступ к устройствам записи звука, и откройте окно **Правила программы** двойным щелчком мыши.

6. В окне **Правила программы** перейдите на закладку **Права**.

7. В списке категорий прав выберите пункт **Изменение операционной системы** → **Подозрительные изменения в операционной системе** → **Доступ к устройствам записи звука**.

8. В графе **Действие** нажмите на значок и выберите один из пунктов меню:

   - Чтобы разрешить программе получение аудиосигнала, выберите пункт **Разрешить**.
   - Чтобы запретить программе доступ к аудиосигналу, выберите пункт **Запретить**.

9. Если вы хотите получать уведомления о том, что программе был запрещен или разрешен доступ к аудиосигналу, в графе **Действие** нажмите на значок и выберите пункт **Записывать в отчет**.

10. Нажмите на кнопку **Сохранить**.

О контроле изменений в операционной системе

Программа Kaspersky Total Security с помощью компонента Контроль изменений в операционной системе контролирует следующие изменения в операционной системе:

- изменение адреса домашней страницы в браузере;
- изменение поисковой системы в браузере;
- установка плагинов, расширений и панелей инструментов в браузере;
- смена браузера по умолчанию;
- изменение параметров прокси-сервера.

Перечисленный набор контролируемых изменений является минимальным и гарантируется специалистами «Лаборатории Касперского». В результате обновления баз и программных модулей набор контролируемых изменений может быть расширен.

Если какая-либо программа пытается изменить браузер по умолчанию для одного из протоколов (http, ftp, https) и вы разрешаете это изменение в окне уведомления, в дальнейшем Kaspersky Total Security автоматически разрешает этой программе изменение браузера по умолчанию для двух других протоколов и не показывает никаких уведомлений.

Kaspersky Total Security не контролирует изменения операционной системы и не показывает уведомление, если изменения в операционную систему вносят следующие программы:

- браузер;
- стандартное средство изменения параметров браузера;
- стандартное средство операционной системы для изменения контролируемых параметров, например, explorer.exe;
- программа, несовместимая с Kaspersky Total Security, если контроль или отмена изменений, выполненных этой программой, приведет к ошибкам в ее работе;
- мастер установки новой версии Kaspersky Total Security;
- программа, выполняющая те же функции, что и компонент Контроль изменений в операционной системе (например, Менеджер браузеров от Яндекс);
- программы в стиле нового интерфейса Windows.

Настройка параметров контроля изменений в операционной системе

► *Чтобы настроить параметры изменений в операционной системе, выполните следующие действия:*

1. Откройте главное окно программы.
2. Нажмите на кнопку в нижней части окна программы.

   Откроется окно **Настройка**.

3. В левой части окна **Настройка** выберите раздел **Защита**.

4. По ссылке **Контроль изменений в операционной системе** перейдите в окно **Изменения в операционной системе**.

5. Включите переключатель **Контроль изменений в операционной системе**, чтобы изменения вступили в силу и компонент защиты Контроль изменений в операционной системе начал работать.

6. Установите флажок **Использовать помощник по установке**, чтобы запретить установку дополнительного программного обеспечения при установке новых программ.

   Если флажок **Использовать помощник по установке** снят после того, как вы уже запустили установку какой-либо программы, помощник по установке продолжит свою работу в рамках текущей установки. Флажки напротив программ, предлагаемых к дополнительной установке, будут сняты, а сами дополнительные программы не будут устанавливаться. При последующей установке программ эта функциональность работать не будет. Дополнительные программы будут устанавливаться совместно с основной.

   Функциональность помощника по установке недоступна для 64-разрядных программ установки на Microsoft Windows XP (x64). Функциональность помощника по установке может быть недоступна в некоторых программах по установке.

7. Установите флажок **Блокировать рекламные сообщения**, чтобы запретить показ шагов установки, содержащих рекламу, во время установки на компьютер новых программ.

8. Установите флажок **Контролировать изменения**, чтобы программа контролировала параметры операционной системы, браузеров, а также параметры сети.

9. Установите флажок **Автоматически запрещать изменения**, чтобы программа Kaspersky Total Security автоматически запрещала изменение всех контролируемых параметров операционной системы, не показывая уведомления об этом.

Режим Безопасных программ

Этот раздел содержит информацию о режиме Безопасных программ.

В этом разделе

О режиме Безопасных программ

Kaspersky Total Security предоставляет возможность создания на компьютере безопасной среды (режим Безопасных программ), в которой разрешен запуск только доверенных программ. Режим Безопасных программ подходит вам, если вы используете постоянный набор широко известных программ, и у вас нет необходимости часто запускать новые неизвестные программы, загруженные из интернета. Работая в режиме Безопасных программ, Kaspersky Total Security блокирует запуск всех программ, которые не являются доверенными по данным «Лаборатории Касперского». Основаниями о том, доверять или нет программе, может служить информация, полученная из Kaspersky Security Network, данные о цифровой подписи программы, данные о доверии к программе установки и источнику, из которого была загружена программа.

Режим Безопасных программ имеет следующие особенности и ограничения:

- Для работы режима Безопасных программ требуется, чтобы были включены компоненты защиты Контроль программ, Файловый Антивирус и Мониторинг активности. При прекращении работы одного из этих компонентов режим Безопасных программ выключается.
- Режим Безопасных программ может быть недоступен, если системные файлы расположены в разделах жесткого диска с файловой системой, отличной от NTFS.

- Режим Безопасных программ может отсутствовать или быть недоступным в текущей версии Kaspersky Total Security. Наличие в Kaspersky Total Security режима Безопасных программ зависит от вашего региона и поставщика услуг. Рекомендуется уточнять наличие режима Безопасных программ при покупке программы.

- Если наличие режима Безопасных программ предусмотрено в вашей версии Kaspersky Total Security, но в настоящее время режим Безопасных программ недоступен, он может стать доступным после обновления баз и программных модулей (см. раздел «Обновление баз и программных модулей» на стр. 59). После обновления баз и программных модулей могут быть изменены параметры запуска неизвестных программ и модулей.

Режим Безопасных программ может быть включен автоматически или вручную. При включении режима Безопасных программ вручную всем программам, установленным на вашем компьютере, присваивается статус доверенных. Программы, установленные после включения режима Безопасных программ, не получают статус доверенных и обрабатываются по общим правилам Контроля программ.

Также вы можете включить режим Безопасных программ вручную после того, как Kaspersky Total Security выполнит анализ операционной системы и установленных программ. Если по результатам анализа Kaspersky Total Security обнаружил, что на компьютере установлены неизвестные программы, включать режим Безопасных программ не рекомендуется.

Автоматическое включение режима Безопасных программ выполняется, если по результатам анализа операционной системы и установленных программ Kaspersky Total Security обнаружил, что на компьютере используются преимущественно доверенные программы.

После включения режима Безопасных программ Kaspersky Total Security может блокировать программы, не являющиеся доверенными. Вы можете разрешить запуск таких программ (см. раздел «Контроль действий программы на компьютере и в сети» на стр. 125), если вы работаете с ними, а затем включить режим Безопасных программ.

Включение режима Безопасных программ

► *Чтобы включить режим Безопасных программ, выполните следующие действия:*

1. Откройте главное окно программы.
2. Нажмите на кнопку **Больше функций**, расположенную в нижней части главного окна.

   Откроется окно **Инструменты**.
3. В окне **Инструменты** в списке инструментов в левой части окна по ссылке **Режим Безопасных программ** перейдите в окно **Режим Безопасных программ**.
4. Выберите один из вариантов включения режима Безопасных программ:

   - В окне **Режим Безопасных программ** нажмите на кнопку **Включить**.

     Режим Безопасных программ начнет работу. При выборе этого варианта Kaspersky Total Security разрешает запуск программ, установленных на ваш компьютер до включения режима Безопасных программ.
   - По ссылке **Включить и проверить все установленные программы** запустите анализ операционной системы с последующим включением режима Безопасных программ.

     Начнется анализ операционной системы и установленных программ за исключением временных файлов и ресурсных dll-библиотек, содержащих исполняемый код. Информация о процессе анализа отобразится в открывшемся окне **Анализ установленных программ**.

     a. Дождитесь окончания анализа операционной системы и установленных программ. Вы можете свернуть окно **Анализ установленных программ**.

     b. Просмотрите информацию о результатах анализа в окне **Режим Безопасных программ**.

        Если в процессе анализа обнаружены системные файлы, информации о которых недостаточно, включать режим Безопасных программ не рекомендуется. Также не рекомендуется включать режим Безопасных программ, если обнаружено большое количество программ, информации о которых недостаточно, чтобы программа Kaspersky Total Security считала их полностью безопасными.

После окончания анализа вы можете просмотреть информацию о недоверенных системных файлах в окне **Режим Безопасных программ**. При включении Режима безопасных программ эти файлы и программы будут заблокированы.

c. Если вы хотите разрешить запуск недоверенных программ и системных файлов, в окне **Режим Безопасных программ** переведите переключатель в графе **Запуск** напротив недоверенной программ или системного файла в положение **Разрешен**.

d. Нажмите на кнопку **Включить режим Безопасных программ**.

Режим Безопасных программ будет включен. Kaspersky Total Security будет блокировать запуск всех программ и системных файлов, не являющихся доверенными. После включения режима Безопасных программ и первой перезагрузки операционной системы запуск неизвестных программ разрешен до запуска Kaspersky Total Security. После последующих перезагрузок операционной системы Kaspersky Total Security блокирует запуск неизвестных программ.

Выключение режима Безопасных программ

► *Чтобы выключить режим Безопасных программ, выполните следующие действия:*

1. Откройте главное окно программы.
2. Нажмите на кнопку **Больше функций**, расположенную в нижней части главного окна.

   Откроется окно **Инструменты**.
3. В окне **Инструменты** в левой части окна по ссылке **Режим Безопасных программ** откройте окно **Режим Безопасных программ**.
4. В блоке **Режим Безопасных программ включен** в нижней части окна перейдите по ссылке **Выключить**.

Режим Безопасных программ будет выключен.

Удаление данных без возможности восстановления

Дополнительная безопасность персональных данных обеспечивается защитой от несанкционированного восстановления удаленной информации злоумышленниками.

В состав Kaspersky Total Security входит инструмент для удаления данных без возможности восстановления обычными программными средствами.

Kaspersky Total Security позволяет удалять данные без возможности восстановления со следующих носителей информации:

- Локальные и сетевые диски. Удаление возможно, если у вас есть права на запись и удаление информации.
- Съемные диски или другие устройства, которые распознаются как съемные диски (например, дискеты, карты памяти, USB-карты или мобильные телефоны). Удаление данных с карт памяти возможно, если на них механически не включен режим защиты от записи.

Вы можете удалять те данные, доступ к которым разрешен под вашей учетной записью. Перед удалением данных требуется убедиться, что эти данные не используются работающими программами.

► *Чтобы удалить данные без возможности восстановления, выполните следующие действия:*

1. Откройте главное окно программы.
2. Нажав на кнопку **Больше функций**, расположенную в нижней части главного окна, откройте окно **Инструменты**.
3. В левой части окна **Инструменты** по ссылке **Защита приватности** откройте окно **Защита приватности**.

4. В окне **Защита приватности** по ссылке **Необратимое удаление данных** откройте окно **Необратимое удаление данных** (см. рис. ниже).

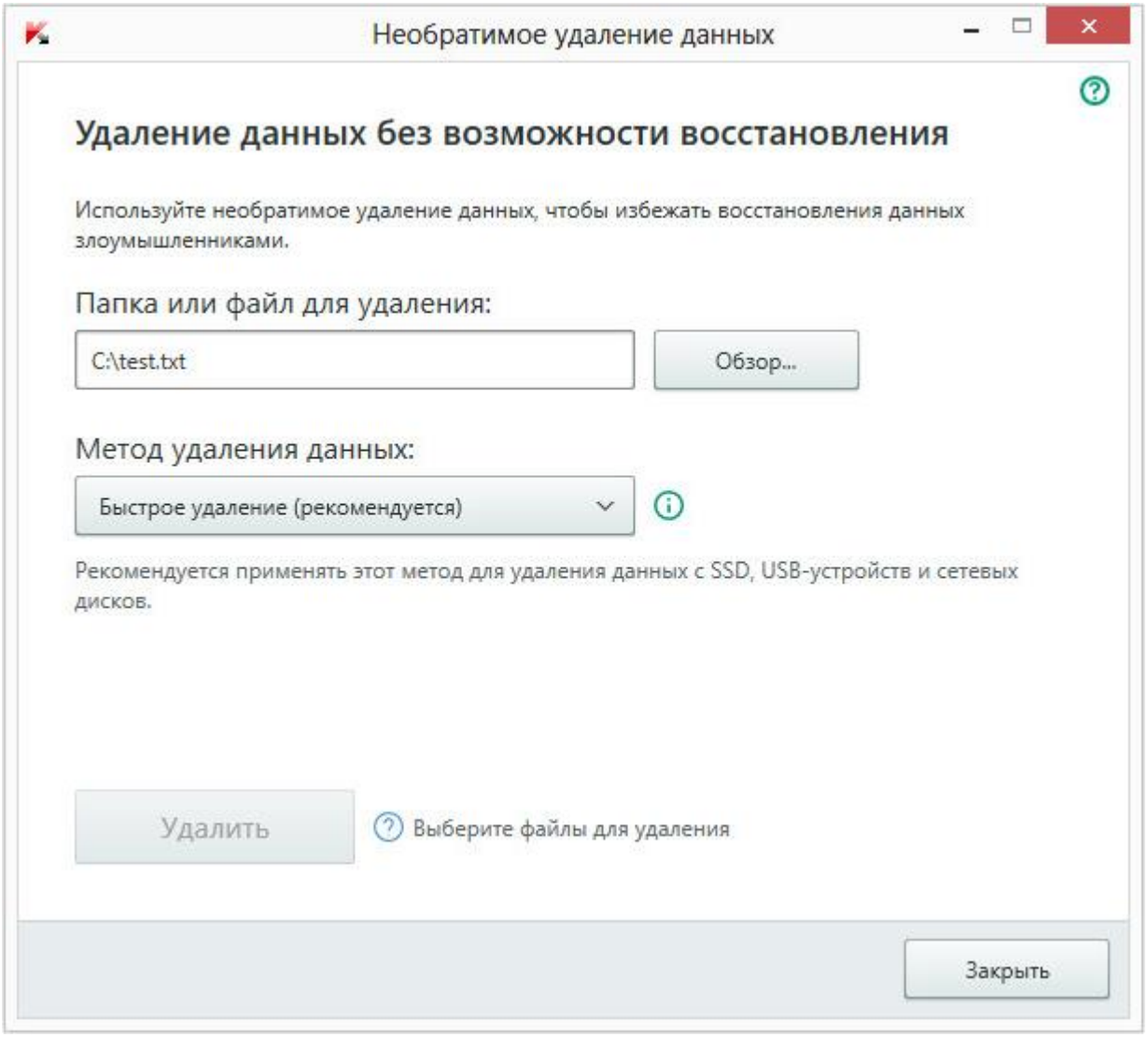

*Рисунок 6. Окно **Необратимое удаление данных***

5. Нажмите на кнопку **Обзор** и в открывшемся окне **Выбор папки** выберите папку или файл для удаления без возможности восстановления.

> Удаление системных файлов может вызвать сбои в работе операционной системы.

6. В раскрывающемся списке **Метод удаления данных** выберите нужный метод удаления данных.

   Для удаления данных с SSD-, USB-устройств и сетевых дисков рекомендуется применять методы **Быстрое удаление** или **ГОСТ Р 50739-95, Россия**. Остальные методы удаления могут нанести вред SSD-, USB-устройству или сетевому диску.

7. Нажмите на кнопку **Удалить**.

8. В открывшемся окне подтверждения удаления нажмите на кнопку **Удалить**. Если некоторые файлы не были удалены, в открывшемся окне повторите удаление по кнопке **Повторить**. Чтобы выбрать другую папку для удаления, нажмите на кнопку **Завершить**.

Удаление неиспользуемых данных

Этот раздел содержит информацию об удалении временных и неиспользуемых файлов.

В этом разделе

Об удалении неиспользуемых данных

Со временем в операционной системе накапливаются временные и неиспользуемые файлы. Эти файлы могут занимать большой объем памяти, что снижает эффективность работы системы, а также могут использоваться вредоносными программами.

Временные файлы создаются при запуске любых программ или операционных систем. По завершении работы не все временные файлы автоматически удаляются. В состав Kaspersky Total Security входит мастер удаления неиспользуемых данных.

Мастер удаления неиспользуемых данных позволяет найти и удалить следующие файлы:

- журналы событий системы, куда записываются названия всех открытых программ;
- журналы событий разных программ или утилит обновления (например, Windows Updater);
- журналы системных соединений;
- временные файлы браузеров (cookies);
- временные файлы, которые остаются после установки / удаления программ;

- содержимое корзины;
- файлы папки TEMP, объем которой иногда достигает нескольких гигабайт.

Помимо удаления из системы ненужных файлов, мастер удаляет те файлы, в которых могли сохраниться конфиденциальные данные (пароли, имена пользователей и информация с регистрационных форм). Тем не менее, для полного удаления таких данных рекомендуется использовать мастер устранения следов активности.

Процедура удаления неиспользуемых данных

► *Чтобы запустить мастер удаления неиспользуемых данных, выполните следующие действия:*

1. Откройте главное окно программы.
2. Нажав на кнопку **Больше функций**, расположенную в нижней части главного окна, откройте окно **Инструменты**.
3. В открывшемся окне по ссылке **Удаление неиспользуемых данных** запустите мастер удаления неиспользуемых данных.

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 шаге следует нажать на кнопку **Отмена**.

Рассмотрим подробнее шаги мастера.

Шаг 1. Начало работы мастера

В первом окне мастера представлена информация об удалении неиспользуемых данных.

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

Шаг 2. Поиск неиспользуемых данных

Мастер осуществляет поиск неиспользуемых данных на вашем компьютере. Поиск может занять некоторое время. По завершении поиска мастер автоматически перейдет к следующему шагу.

Шаг 3. Выбор действий для удаления неиспользуемых данных

По завершении поиска неиспользуемых данных открывается окно, в котором отображается список действий.

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. Удаление неиспользуемой информации

Мастер выполняет действия, выбранные на предыдущем шаге. Удаление неиспользуемой информации может занять некоторое время.

После удаления неиспользуемой информации мастер автоматически перейдет к следующему шагу.

> Во время работы мастера некоторые файлы (например, файл журнала Microsoft Windows, журнал событий Microsoft Office) могут использоваться операционной системой. Чтобы удалить эти файлы, мастер предложит перезагрузить операционную систему.

Шаг 5. Завершение работы мастера

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

Резервное копирование данных

Этот раздел содержит информацию о резервном копировании данных.

В этом разделе

О резервном копировании данных

Резервное копирование данных необходимо для защиты ваших данных от потери в результате выхода из строя или кражи оборудования, случайного удаления или потери в результате действий злоумышленников.

Чтобы выполнить резервное копирование данных, требуется создать (см. раздел «Создание задачи резервного копирования» на стр. 148) и запустить (см. раздел «Запуск задачи резервного копирования» на стр. 153) задачу резервного копирования. Задача может быть запущена автоматически, по заданному расписанию, или вручную. С помощью программы вы можете просматривать информацию о выполнении этих задач.

Сохранять резервные копии данных рекомендуется на съемных дисках или в Онлайн-хранилище.

Для создания резервных копий Kaspersky Total Security позволяет использовать следующие типы хранилищ:

- локальный диск;
- съемный диск (например, внешний жесткий диск);
- сетевой диск;
- FTP-сервер;
- Онлайн-хранилище (см. раздел «Об Онлайн-хранилище» на стр. 154).

Создание задачи резервного копирования

► *Чтобы создать задачу резервного копирования, выполните следующие действия:*

1. Откройте главное окно программы.
2. Нажмите на кнопку **Резервное копирование**.
3. В открывшемся окне **Резервное копирование** выполните следующие действия:
   - нажмите на кнопку **Выбрать файлы для резервного копирования**, если задача резервного копирования еще не создавалась;
   - нажмите на кнопку **Создать резервные копии других файлов**, если у вас есть задача резервного копирования и вы хотите создать новую.

   Будет запущен мастер создания задачи резервного копирования.

   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 шаге следует нажать на кнопку **Отмена**.

   Рассмотрим подробнее шаги мастера.

В этом разделе

Шаг 1. Выбор файлов

На этом шаге мастера выберите тип файлов или укажите папки, для которых вы хотите создать резервные копии:

- Для быстрой настройки выберите один из предустановленных типов файлов (файлы из папок «Мои документы» и «Рабочий стол», фотографии и изображения, фильмы и видео, музыкальные файлы). При подтверждении этого варианта мастер сразу перейдет к шагу 4 «Выбор хранилища резервных копий».

  > Kaspersky Total Security не создает резервные копии файлов, расположенных в папках «Рабочий стол» и «Мои документы», если эти папки находятся на сетевом диске.

- Выберите вариант **Создать резервные копии файлов из указанных папок**, чтобы вручную указать папки, для которых вы хотите создать резервные копии.

Шаг 2. Выбор папок для резервного копирования

Если на предыдущем шаге мастера вы выбрали вариант **Создать резервные копии файлов из указанных папок**, нажмите на кнопку **Добавить папку** и выберите папку в открывшемся окне **Выбор папки для резервного копирования** или перетащите папку в окно программы.

Установите флажок **Дополнительно указать типы файлов**, если вы хотите в указанных папках уточнить типы файлов, для которых требуется создать резервные копии.

Шаг 3. Выбор типов файлов для резервного копирования

Если на предыдущем шаге мастера вы установили флажок **Дополнительно указать типы файлов**, на этом шаге мастера установите флажки напротив типов файлов, для которых вы хотите создать резервные копии.

Шаг 4. Выбор хранилища резервных копий

На этом шаге выберите хранилище резервных копий:

- **Онлайн-хранилище**. Выберите этот вариант, если вы хотите хранить резервные копии в Онлайн-хранилище Dropbox. Перед использованием требуется активировать Онлайн-хранилище (см. раздел «Активация Онлайн-хранилища» на стр. 155). При создании резервной копии с использованием Онлайн-хранилища Kaspersky Total Security не создает резервные копии тех типов данных, на которые наложены ограничения правилами использования Dropbox.
- **Локальный диск**. Если вы хотите хранить резервные копии на локальном диске, выберите нужный локальный диск в списке.
- **Сетевой диск**. Если вы хотите хранить резервные копии на сетевом диске, выберите нужный сетевой диск в списке.
- **Съемный диск**. Если вы хотите хранить резервные копии на съемном диске, выберите нужный съемный диск в списке.

Для безопасности данных рекомендуется использовать Онлайн-хранилище или создавать хранилища резервных копий на съемных дисках.

► *Чтобы добавить сетевое хранилище, выполните следующие действия:*

1. По ссылке **Добавить сетевое хранилище** откройте окно **Добавление сетевого хранилища** и выберите тип сетевого хранилища: сетевой диск или FTP-сервер.
2. Укажите данные, необходимые для подключения к сетевому хранилищу.
3. Нажмите на кнопку **ОК**.

► *Чтобы добавить съемный диск в качестве хранилища резервных копий, выполните следующие действия:*

1. По ссылке **Подключить имеющееся хранилище** откройте окно **Подключение хранилища**.
2. Выберите раздел **Съемный диск**.
3. Нажмите на кнопку **Обзор** и в открывшемся окне укажите съемный диск, на который вы хотите сохранять резервные копии файлов.

Установите флажок **Использовать расширенную настройку хранилища**, если вы хотите настроить параметры хранения файлов, такие как количество хранимых версий резервных копий и время хранения версий резервных копий.

Шаг 5. Создание расписания резервного копирования

На этом шаге мастера выполните одно из следующих действий:

- Задайте расписание запуска задачи резервного копирования, если хотите, чтобы задача запускалась автоматически.
- В раскрывающемся списке **Запускать резервное копирование** выберите вариант **по требованию**, если хотите запускать задачу самостоятельно.

Шаг 6. Ввод пароля для защиты резервных копий

Установите флажок **Включить защиту паролем** и заполните поля **Пароль для доступа к резервным копиям** и **Подтверждение пароля**, если вы хотите защитить паролем доступ к резервным копиям.

Шаг 7. Параметры хранения резервных копий файлов

Этот шаг доступен, если на шаге 4 «Выбор хранилища резервных копий» вы установили флажок **Использовать расширенную настройку хранилища**.

Настройте параметры хранения файлов:

- Установите флажок **Ограничить количество версий резервных копий** и в поле **Количество хранимых версий резервных копий** укажите количество версий резервных копий одного файла, которые необходимо сохранять.
- Установите флажок **Ограничить время хранения версий резервных копий** и в поле **Период хранения версии резервной копии** укажите количество дней, которые должна храниться каждая версия резервной копии.

Шаг 8. Ввод имени задачи резервного копирования

На этом шаге выполните следующие действия:

- Введите имя задачи резервного копирования.
- Установите флажок **Запустить резервное копирование по завершении работы мастера**, если вы хотите, чтобы резервное копирование началось автоматически после завершения работы мастера.

Шаг 9. Завершение работы мастера

Нажмите на кнопку **Завершить**.

Будет создана задача резервного копирования. Созданная задача отображается в окне **Резервное копирование**.

Запуск задачи резервного копирования

► *Чтобы запустить задачу резервного копирования, выполните следующие действия:*

1. Откройте главное окно программы.
2. Нажмите на кнопку **Резервное копирование**.
3. В открывшемся окне **Резервное копирование** выберите задачу резервного копирования и нажмите на кнопку **Начать копирование**.

Запустится задача резервного копирования.

Восстановление данных из резервной копии

► *Чтобы восстановить данные из резервной копии, выполните следующие действия:*

1. Откройте главное окно программ.
2. Нажмите на кнопку **Резервное копирование**.
3. Выполните одно из следующих действий:
   - Нажмите на кнопку **Восстановить файлы** напротив нужной задачи резервного копирования.
   - По ссылке **Управление хранилищами** откройте окно, где напротив нужного хранилища резервных копий нажмите на кнопку **Восстановить файлы**.

4. Если при создании резервной копии был задан пароль, укажите этот пароль в окне **Введите пароль для доступа к хранилищу**.

5. В раскрывающем списке **Дата / время копирования** выберите дату и время создания резервной копии.

6. Установите флажки напротив папок, которые вы хотите восстановить.

7. Если вы хотите восстановить только определенные типы файлов, в раскрывающемся списке **Тип файлов** выберите эти типы файлов.

8. Нажмите на кнопку **Восстановить выбранные файлы**.

   Откроется окно **Восстановление файлов из резервных копий**.

9. Выберите один из двух вариантов:

   - **В исходную папку**. Если выбран этот вариант, программа восстанавливает данные в исходную папку.

   - **В указанную папку**. Если выбран этот вариант, программа восстанавливает данные в указанную папку. Нажмите на кнопку **Обзор**, чтобы выбрать папку, в которую вы хотите восстановить данные.

10. В раскрывающемся списке **При совпадении имен файлов** выберите действие, которое должна выполнять программа, если имя восстанавливаемого файла совпадает с именем файла, находящегося в указанной для восстановления папке.

11. Нажмите на кнопку **Восстановить**.

    Выбранные для восстановления файлы будут восстановлены из резервной копии и сохранены в указанной папке.

Об Онлайн-хранилище

Программа Kaspersky Total Security позволяет сохранять резервные копии ваших данных в Онлайн-хранилище на удаленном сервере, используя веб-сервис Dropbox.

Для использования Онлайн-хранилища требуется:

- Убедиться, что компьютер подключен к интернету.
- Создать учетную запись на веб-сайте поставщика услуг хранения данных онлайн.
- Активировать Онлайн-хранилище.

Вы можете использовать одну и ту же учетную запись Dropbox для сохранения в единое Онлайн-хранилище резервных копий данных с разных устройств, на которых установлена программа Kaspersky Total Security.

Объем Онлайн-хранилища определяется поставщиком услуг хранения данных онлайн, веб-сервисом Dropbox. Более подробную информацию об условиях использовании веб-сервиса вы можете получить на сайте Dropbox https://www.dropbox.com/.

Активация Онлайн-хранилища

► *Чтобы активировать Онлайн-хранилище, выполните следующие действия:*

1. Откройте главное окно программы.
2. Нажмите на кнопку **Резервное копирование**.
3. В открывшемся окне **Резервное копирование** выполните следующие действия:
   - нажмите на кнопку **Выбрать файлы для резервного копирования**, если задача резервного копирования не создавалась;
   - нажмите на кнопку **Создать резервные копии других файлов**, если у вас уже есть задача резервного копирования.

   Будет запущен мастер создания задачи резервного копирования (см. раздел «Создание задачи резервного копирования» на стр. 148).
4. В окне выбора типа данных выберите категорию данных или вручную укажите файлы, для которых нужно создавать резервные копии.

5. В окне выбора хранилища выберите Онлайн-хранилище и нажмите на кнопку **Активировать**.

   > Для создания Онлайн-хранилища требуется подключение к интернету.

   Откроется окно входа в учетную запись Dropbox.

6. В открывшемся окне выполните одно из следующих действий:

   - Если вы не зарегистрированы на веб-сайте Dropbox, пройдите процедуру регистрации.
   - Если вы зарегистрированы на веб-сайте Dropbox, войдите в учетную запись Dropbox.

7. Для завершения активации Онлайн-хранилища подтвердите, что Kaspersky Total Security может использовать вашу учетную запись Dropbox для резервного копирования данных и восстановления данных из резервной копии. Kaspersky Total Security будет помещать резервные копии данных в отдельную папку, которая создается в папке хранения приложений Dropbox.

   После завершения активации Онлайн-хранилища откроется окно выбора хранилища. Онлайн-хранилище будет доступно для выбора. Для активированного Онлайн-хранилища отображается объем занятого пространства и объем свободного пространства, доступного для записи информации.

Хранение данных в сейфах

Этот раздел содержит информацию о том, как вы можете защитить данные с помощью сейфов.

В этом разделе

О сейфе

Для защиты ваших конфиденциальных данных от несанкционированного доступа предназначены сейфы. *Сейф* – это хранилище данных на вашем компьютере, которое вы можете открывать или закрывать с помощью известного только вам пароля. Для изменения файлов, хранящихся в закрытом сейфе, требуется ввести пароль. Если вы ввели неверный пароль 10 раз подряд, доступ к сейфу блокируется на один час.

Если вы потеряете или забудете пароль, восстановить данные будет невозможно.

Для создания сейфов в Kaspersky Total Security используются следующие алгоритмы шифрования данных: AES XTS 256 с эффективной длинной ключа 56 бит.

Помещение файлов в сейф

► *Чтобы поместить файлы в сейф, выполните следующие действия:*

1. Откройте главное окно программы.
2. Нажмите на кнопку **Виртуальные сейфы**.

3. В открывшемся окне **Виртуальные сейфы** выполните одно из следующих действий:

   - Нажмите на кнопку **Создать новый сейф**, если у вас еще нет сейфа.
   - Нажмите на кнопку **Создать сейф**, если ранее вы создавали сейфы.

4. По ссылке **Добавить файлы и папки в сейф** откройте Проводник и укажите файлы, которые вы хотите поместить в сейф.

   Выбранные файлы отобразятся в окне **Виртуальные сейфы**.

5. Нажмите на кнопку **Продолжить**.
6. Введите название сейфа и укажите его расположение или используйте значения этих параметров по умолчанию.
7. Для получения быстрого доступа к сейфу установите флажок **Создать ярлык сейфа на рабочем столе**.
8. Нажмите на кнопку **Продолжить**.
9. Заполните поля **Пароль** и **Подтверждение пароля** и нажмите на кнопку **Продолжить**.
10. Выберите действие с исходными копиями файлов вне сейфа:

    - Чтобы удалить исходные копии файлов вне сейфа, нажмите на кнопку **Удалить**.
    - Чтобы сохранить исходные копии файлов вне сейфа, нажмите на кнопку **Пропустить**.

11. Нажмите на кнопку **Завершить**.

    В списке сейфов отобразится созданный вами сейф.

12. Чтобы закрыть сейф, нажмите на кнопку **Закрыть**.

    Данные в закрытом сейфе будут доступны только после ввода пароля.

Получение доступа к файлам, хранящимся в сейфе

► *Чтобы получить доступ к файлам, хранящимся в сейфе, выполните следующие действия:*

1. Откройте главное окно программы
2. Нажмите на кнопку **Виртуальные сейфы**.
3. В открывшемся окне **Виртуальные сейфы** нажмите на кнопку **Открыть** рядом с нужным сейфом.
4. Введите пароль и нажмите на кнопку **Открыть сейф в Проводнике**.

Файлы, сохраненные в сейфе, отобразятся в окне Проводника. Вы можете внести необходимые изменения в файлы и снова закрыть сейф.

Чтобы открыть сейфы, созданные в предыдущей версии программы, вам нужно выполнить конвертацию старого формата сейфов в новый формат. Программа сама предложит вам выполнить конвертацию при попытке открыть сейф в Kaspersky Total Security.

Конвертация сейфов в новый формат зависит от размера сейфа и может занимать значительное время.

Защита доступа к управлению Kaspersky Total Security с помощью пароля

На одном компьютере могут работать несколько пользователей с разным опытом и уровнем компьютерной грамотности. Неограниченный доступ разных пользователей к управлению Kaspersky Total Security 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;
- завершение работы программы;
- удаление программы.

► *Чтобы защитить доступ к Kaspersky Total Security с помощью пароля, выполните следующие действия:*

1. Откройте главное окно программы.
2. Нажмите на кнопку ⚙ в нижней части окна программы.

   Откроется окно **Настройка**.
3. В левой части окна выберите раздел **Общие** и по ссылке **Установить защиту паролем** откройте окно **Защита паролем**.
4. В открывшемся окне заполните поля **Новый пароль** и **Подтверждение пароля**.
5. В блоке параметров **Область действия пароля** укажите действия с программой, доступ к которым нужно защитить паролем.

Забытый пароль восстановить нельзя. Если пароль забыт, для восстановления доступа к параметрам Kaspersky Total Security потребуется обращение в Службу технической поддержки.

Приостановка и возобновление защиты компьютера

Приостановка защиты означает выключение на некоторое время всех ее компонентов.

Во время приостановки защиты или выключения Kaspersky Total Security действует функция контроля активности программ, запущенных на вашем компьютере. Информация о результатах контроля активности программ сохраняется в операционной системе. При следующем запуске или возобновлении защиты Kaspersky Total Security использует эту информацию для защиты вашего компьютера от вредоносных действий, которые могли быть выполнены во время приостановки защиты или выключения Kaspersky Total Security. Хранение информации о результатах контроля активности программ не ограничено по времени. Эта информация удаляется в случае удаления Kaspersky Total Security с вашего компьютера.

► *Чтобы приостановить защиту компьютера, выполните следующие действия:*

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

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

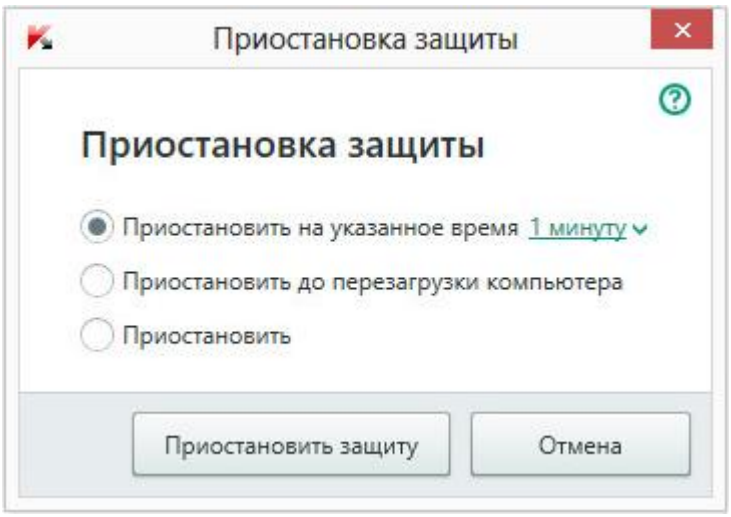

Рисунок 7. Окно Приостановка защиты

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 компьютера** – защита будет включена после перезапуска программы или перезагрузки операционной системы (при условии, что включен автоматический запуск программы).
   - **Приостановить** – защита будет включена тогда, когда вы решите возобновить ее.

3. Нажмите на кнопку **Приостановить защиту** и подтвердите действие в открывшемся окне.

► *Чтобы возобновить защиту компьютера,*

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

Восстановление стандартных параметров работы программы

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

В результате работы мастера для всех компонентов защиты будет установлен уровень безопасности **Рекомендуемый**.

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

1. Откройте главное окно программы.
2. Нажмите на кнопку  в нижней части окна программы.

   Откроется окно **Настройка**.
3. Выберите раздел **Общие**.

   В окне отобразятся параметры настройки Kaspersky Total Security.
4. В нижней части окна в раскрывающемся списке **Управление параметрами** выберите элемент **Восстановить параметры**.

Рассмотрим подробнее шаги мастера.

Шаг 1. Начало работы мастера

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

Шаг 2. Восстановление параметров

На этом шаге выполняется восстановление параметров работы программы до тех, которые заданы специалистами «Лаборатории Касперского» по умолчанию.

Шаг 3. Завершение восстановления

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

Просмотр отчета о работе программы

Kaspersky Total Security 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 обновлялись базы и программные модули, сколько обнаружено спам-сообщений и многое другое).

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

1. Откройте главное окно программы.

2. Нажав на кнопку **Больше функций**, расположенную в нижней части главного окна, откройте окно **Инструменты**.

3. В окне **Инструменты** выберите блок **Отчет**, чтобы открыть окно **Отчеты**.

   В окне **Отчеты** отображаются отчеты о работе программы за текущий день (в левой части окна) и за период (в правой части окна).

4. Если вам нужно просмотреть подробный отчет о работе программы, откройте окно **Подробные отчеты** по ссылке **Подробные отчеты**, расположенной в верхней части окна **Отчеты**.

   В окне **Подробные отчеты** данные представлены в табличном виде. Для удобства просмотра отчетов вы можете выбирать различные варианты фильтрации записей.

Применение параметров программы на другом компьютере

Настроив программу, вы можете применить параметры ее работы к программе Kaspersky Total Security, установленной на другом компьютере. В результате программа на обоих компьютерах будет настроена одинаково.

Параметры работы программы сохраняются в конфигурационном файле, который вы можете перенести с одного компьютера на другой.

Перенос параметров Kaspersky Total Security с одного компьютера на другой производится в три этапа:

1. Сохранение параметров программы в конфигурационном файле.
2. Перенос конфигурационного файла на другой компьютер (например, по электронной почте или на съемном диске).
3. Импорт параметров из конфигурационного файла в программу, установленную на другом компьютере.

► *Чтобы экспортировать параметры программы, выполните следующие действия:*

1. Откройте главное окно программы.
2. Нажмите на кнопку в нижней части окна программы.

   Откроется окно **Настройка**.
3. В окне **Настройка** выберите раздел **Общие**.
4. В раскрывающемся списке **Управление параметрами** выберите элемент **Экспортировать параметры**.

   Откроется окно **Сохранить как**.
5. Задайте имя конфигурационного файла и нажмите на кнопку **Сохранить**.

Параметры программы будут сохранены в конфигурационный файл.

Вы также можете экспортировать параметры работы программы при помощи командной строки, используя команду: `avp.com EXPORT <имя_файла>`.

► *Чтобы импортировать параметры в программу, установленную на другом компьютере, выполните следующие действия:*

1. Откройте главное окно программы Kaspersky Total Security, установленной на другом компьютере.
2. Нажмите на кнопку в нижней части окна.

   Откроется окно **Настройка**.
3. В окне **Настройка** выберите раздел **Общие**.
4. В раскрывающемся списке **Управление параметрами** выберите элемент **Импортировать параметры**.

   Откроется окно **Открыть**.
5. Укажите конфигурационный файл и нажмите на кнопку **Открыть**.

Параметры будут импортированы в программу, установленную на другом компьютере.

Участие в Kaspersky Security Network

Чтобы повысить эффективность защиты вашего компьютера, Kaspersky Total Security использует облачную защиту. Облачная защита реализуется с помощью инфраструктуры Kaspersky Security Network, использующей данные, полученных от пользователей во всем мире.

Kaspersky Security Network (KSN) – это инфраструктура облачных служб, 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 Kaspersky Total Security на неизвестные угрозы, повышает эффективность работы некоторых компонентов защиты, а также снижает вероятность ложных срабатываний.

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

Если вы участвуете в Kaspersky Security Network, вы в автоматическом режиме отправляете в «Лабораторию Касперского» информацию о конфигурации вашей операционной системы и времени запуска и завершения процессов Kaspersky Total Security.

В этом разделе

Включение и выключение участия в Kaspersky Security Network

Участие в Kaspersky Security Network является добровольным. Вы можете включить или выключить использование Kaspersky Security Network (KSN) во время установки Kaspersky Total Security 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. Нажмите на кнопку  в нижней части окна программы.

   Откроется окно **Настройка**.
3. В разделе **Дополнительно** выберите блок **Дополнительные средства защиты и управления**.

   В окне отобразятся сведения о Kaspersky Security Network и параметры участия в Kaspersky Security Network.
4. Включите или выключите участие в Kaspersky Security Network по кнопкам **Включить** / **Выключить**:

   - Если вы хотите участвовать в Kaspersky Security Network, нажмите на кнопку **Включить**.

     Откроется окно с текстом Положения о Kaspersky Security Network. Если вы согласны с условиями положения, нажмите на кнопку **Я согласен**.
   - Если вы не хотите участвовать в Kaspersky Security Network, нажмите на кнопку **Выключить**.

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**.

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

1. Откройте главное окно программы.
2. Нажав на кнопку **Больше функций**, расположенную в нижней части главного окна, откройте окно **Инструменты**.
3. В левой части окна **Инструменты** по ссылке **Облачная защита** откройте окно **Облачная защита**.

В окне **Облачная защита** отобразится статус подключения к Kaspersky Security Network.

Работа с программой из командной строки

Вы можете работать с Kaspersky Total Security с помощью командной строки.

Синтаксис командной строки:

```
avp.com <команда> [параметры]
```

Для просмотра справочной информации о синтаксисе командной строки предусмотрена команда:

```
avp.com [ /? | HELP ]
```

Эта команда позволяет получить полный список команд, доступных для работы с Kaspersky Total Security через командную строку.

Для получения справочной информации о синтаксисе конкретной команды вы можете воспользоваться одной из следующих команд:

```
avp.com <команда> /?
avp.com HELP <команда>
```

Обращаться к программе через командную строку следует из папки установки программы либо с указанием полного пути к avp.com.

Обращение в Службу технической поддержки

Этот раздел содержит информацию о способах и условиях получения технической поддержки.

В этом разделе

Способы получения технической поддержки

Если вы не нашли решения вашей проблемы в документации к программе или в одном из источников информации о программе, 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 с портала My Kaspersky. Этот способ позволяет вам связаться со специалистами Службы технической поддержки через форму запроса.

Техническая поддержка предоставляется только пользователям, которые приобрели лицензию на использование программы. Техническая поддержка для пользователей пробных версий не осуществляется.

Техническая поддержка по телефону

В большинстве регионов по всему миру вы можете позвонить специалистам Службы технической поддержки. Вы можете найти информацию о способах получения технической поддержки в вашем регионе и контакты Службы технической поддержки на веб-сайте Службы технической поддержки «Лаборатории Касперского» (http://support.kaspersky.ru/support/contacts).

Перед обращением в Службу технической поддержки ознакомьтесь с правилами предоставления технической поддержки (http://support.kaspersky.ru/support/rules).

Получение технической поддержки на портале My Kaspersky

My Kaspersky (https://my.kaspersky.ru) – это единый онлайн-ресурс для управления защитой ваших устройств и кодами активации программ «Лаборатории Касперского», а также для получения технической поддержки.

Для доступа к порталу My Kaspersky вам нужно зарегистрироваться. Для этого вам нужно указать адрес электронной почты и задать пароль.

Для получения технической поддержки вы можете выполнять следующие действия на портале My Kaspersky:

- отправлять запросы в Службу технической поддержки;
- обмениваться сообщениями со Службой технической поддержки без использования электронной почты;
- отслеживать состояние ваших запросов в реальном времени.

Вы также можете просматривать полную историю ваших запросов в Службу технической поддержки.

Электронный запрос в Службу технической поддержки

В электронном запросе в Службу технической поддержки вам нужно указать следующую информацию:

- тему вашего запроса;
- название и номер версии программы;
- название и номер версии операционной системы;
- описание проблемы.

Специалист Службы технической поддержки направляет ответ на ваш вопрос на портал My Kaspersky и на адрес электронной почты, который вы указали при регистрации.

Сбор информации для Службы технической поддержки

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.

Для более эффективного оказания поддержки в случае возникновения вопросов по работе программы специалисты Службы технической поддержки могут попросить вас в отладочных целях на время проведения работ по диагностике изменить параметры программы. Для этого может потребоваться выполнение следующих действий:

- Активировать функциональность сбора расширенной диагностической информации.
- Выполнить более тонкую настройку работы отдельных компонентов программы, недоступную через стандартные средства пользовательского интерфейса.

- Изменить параметры хранения и отправки собираемой диагностической информации.
- Настроить перехват и сохранение в файл сетевого трафика.

Вся необходимая для выполнения перечисленных действий информация (описание последовательности шагов, изменяемые параметры, конфигурационные файлы, скрипты, дополнительные возможности командной строки, отладочные модули, специализированные утилиты и т. д.), а также состав собираемых в отладочных целях данных будут сообщены вам специалистами Службы технической поддержки. Собранная расширенная диагностическая информация сохраняется на компьютере пользователя. Автоматическая пересылка собранных данных в «Лабораторию Касперского» не выполняется.

Перечисленные выше действия должны выполняться только под руководством специалистов Службы технической поддержки по полученным от них инструкциям. Самостоятельное изменение параметров работы программы способами, не описанными в Руководстве администратора или в рекомендациях специалистов Службы технической поддержки, может привести к замедлению и сбоям в работе операционной системы, снижению уровня защиты компьютера, а также к нарушению доступности и целостности обрабатываемой информации.

В этом разделе

Создание отчета о состоянии операционной системы

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

1. Откройте главное окно программы.
2. Нажмите на кнопку  в нижней части окна.

   Откроется окно **Поддержка**.

3. В открывшемся окне по ссылке **Мониторинг проблем** откройте окно **Мониторинг проблем**.
4. В открывшемся окне по ссылке **Как создать отчет об операционной системе** откройте в браузере статью в Базе знаний о том, как создать отчет об операционной системе.
5. Следуйте инструкции, приведенной в статье Базы знаний.

Отправка файлов данных

После создания файлов трассировки и отчета о состоянии операционной 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 на портале My Kaspersky» на стр. 172). Этот номер доступен на портале My Kaspersky при наличии активного запроса.

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

1. Откройте главное окно программы.
2. Нажмите на кнопку в нижней части окна.

   Откроется окно **Поддержка**.
3. По ссылке **Мониторинг проблем** откройте окно **Мониторинг проблем**.
4. В открывшемся окне по ссылке **Отправить отчет в Службу технической поддержки** откройте окно **Отправка отчета**.
5. Установите флажки рядом с теми данными, которые вы хотите отправить в Службу технической поддержки.
6. Введите номер запроса, назначенный Службой технической поддержки.
7. Нажмите на кнопку **Отправить отчет**.

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

Если отправить файлы по какой-либо причине невозможно, вы можете сохранить файлы данных на вашем компьютере и впоследствии отправить их с портала My Kaspersky.

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

1. Откройте главное окно программы.
2. Нажмите на кнопку в нижней части окна.

   Откроется окно **Поддержка**.
3. В открывшемся окне по ссылке **Мониторинг проблем** откройте окно **Мониторинг проблем**.
4. В открывшемся окне по ссылке **Отправить отчет в Службу технической поддержки** откройте окно **Отправка отчета**.
5. Выберите типы данных, которые вы хотите сохранить на диске:
   - **Информация об операционной системе**. Установите этот флажок, если вы хотите сохранить на диске информацию об операционной системе вашего компьютера.
   - **Полученные для анализа данные**. Установите этот флажок, если вы хотите сохранить файлы трассировки программы. По ссылке **<количество файлов>, <объем данных>** откройте окно **Полученные для анализа данные**. Установите флажки напротив тех файлов трассировки, которые вы хотите сохранить.
6. По ссылке **Сохранить отчет** откройте окно для сохранения архива с файлами данных.
7. Задайте имя архива и подтвердите сохранение.

Созданный архив вы можете отправить в Службу технической поддержки через портал My Kaspersky.

О составе и хранении файлов трассировки

Файлы трассировки хранятся на вашем компьютере в открытом виде в течение семи дней с момента выключения записи данных. По истечении семи дней файлы трассировки безвозвратно удаляются.

Файлы трассировки хранятся в папке ProgramData\Kaspersky Lab.

Файлы трассировки имеют следующие названия: `KAV<номер версии_dateXX.XX_timeXX.XX_pidXXX.><тип файла трассировки>.log`.

Файлы трассировки могут содержать конфиденциальные данные. Ознакомиться с содержимым файла трассировки вы можете, открыв его в текстовом редакторе (например, «Блокнот»).

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.

► *Чтобы выполнить скрипт AVZ, выполните следующие действия:*

1. Откройте главное окно программы.
2. Нажмите на кнопку  в нижней части окна.

   Откроется окно **Поддержка**.
3. В открывшемся окне перейдите по ссылке **Мониторинг проблем**.

   Откроется окно **Мониторинг проблем**.
4. В открывшемся окне по ссылке **Выполнить скрипт** откройте окно **Выполнение скрипта**.
5. Скопируйте текст скрипта, полученного от специалистов Службы технической поддержки, вставьте его в поле ввода в открывшемся окне и нажмите на кнопку **Выполнить**.

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.

Ограничения и предупреждения

Kaspersky Total Security имеет ряд некритичных для работы программы ограничений.

Ограничения при обновлении предыдущей версии программы

Программа может быть обновлена, если на вашем компьютере установлены следующие версии Kaspersky Total Security:

- Kaspersky CRYSTAL 2.0;
- Kaspersky CRYSTAL 3.0;
- Kaspersky Total Security 4.0.

Обновление более ранних версий программы не поддерживается.

При удалении версии программы ниже Kaspersky CRYSTAL 2.0 резервные копии файлов и объекты, находящиеся на карантине, будут потеряны, так как их формат не поддерживается и не может быть преобразован в новый формат. При обновлении Kaspersky CRYSTAL 2.0 возможно выполнить преобразование резервных копий файлов и объектов, находящихся на карантине, в новый формат. Хранилище резервных копий в формате Kaspersky CRYSTAL 3.0 поддерживается и не требует преобразования в новый формат.

Функциональность обновления программы Kaspersky Total Security имеет следующие ограничения:

- При обновлении предыдущей версии Kaspersky Total Security следующие параметры программы заменяются параметрами по умолчанию:
  - параметры отображения Kaspersky Total Security;
  - расписание проверки;
  - участие в Kaspersky Security Network;
  - уровень защиты Файлового Антивируса;
  - уровень защиты Почтового Антивируса;
  - источники обновлений;
  - список доверенных веб-адресов;

- параметры Проверки ссылок.

- После обновления предыдущей версии программы Kaspersky Total Security запускается автоматически, даже если в сохраненных параметрах автозапуск программы выключен. При последующих перезагрузках операционной системы Kaspersky Total Security не запускается автоматически, если в сохраненных параметрах автозапуск программы выключен.

Ограничения работы некоторых компонентов и обработки файлов в автоматическом режиме

Обработка зараженных файлов выполняется в автоматическом режиме по правилам, сформированным специалистами «Лаборатории Касперского». Вы не можете вручную изменять эти правила. Правила могут обновиться в результате обновления баз и программных модулей. Также в автоматическом режиме обновляются правила Сетевого экрана, Контроля программ и режима Безопасных программ.

Ограничения проверки файлов и сертификатов веб-сайтов

При проверке файла и сертификата веб-сайта программа может обращаться за информацией в Kaspersky Security Network. Если данные из Kaspersky Security Network получить не удалось, программа принимает решение о том, является ли файл зараженным, а сертификат недоверенным, на основании локальных антивирусных баз.

Ограничения функциональности Мониторинга активности

Функциональность противодействия программам-крипторам (шифрование файлов пользователя вредоносной программой) имеет следующие ограничения:

- Для обеспечения функциональности используется системная папка Temp. Если на системном диске, на котором расположена папка Temp, недостаточно свободного места для создания временных файлов, защита от программ-крипторов не предоставляется. При этом уведомление о невыполнении копирования (непредоставлении защиты) не выводится.

- Временные файлы удаляются автоматически при завершении работы Kaspersky Total Security или отключении компонента Мониторинг активности.

- В случае нештатного завершения работы Kaspersky Total Security временные файлы автоматически не удаляются. Чтобы удалить временные файлы, необходимо вручную очистить папку Temp. Для этого откройте окно **Выполнить** (**Запуск программы** в Windows XP) и в поле **Открыть** введите `%TEMP%`. Нажмите на кнопку **ОК**.

Ограничения функциональности проверки защищенных соединений

В связи с техническими ограничениями реализации алгоритмов проверки проверка защищенных соединений не поддерживает некоторые расширения протокола TLS 1.0 и выше (в частности NPN и ALPN). Подключение по этим протоколам может быть ограничено. Браузеры с поддержкой протокола SPDY используют вместо SPDY протокол HTTP поверх TLS, даже если сервер, к которому выполняется подключение, поддерживает SPDY. При этом уровень защиты соединения не снижается. Если сервер поддерживает только протокол SPDY, и возможность установить соединение с помощью протокола HTTPS отсутствует, программа не будет контролировать установленное соединение.

Программа Kaspersky Total Security не поддерживает обработку трафика, передаваемого через HTTPS/2 Proxy. Также программа не обрабатывает трафик, передаваемый через расширения протокола HTTP/2.

Программа Kaspersky Total Security контролирует только те защищенные соединения, которые она может расшифровать. Программа не контролирует соединения, добавленные в список исключений (ссылка **Веб-сайты** в окне **Параметры сети**). Проверка и расшифровка зашифрованного трафика по умолчанию выполняется следующими компонентами:

- Веб-Антивирус.
- Безопасные платежи.
- Проверка ссылок.
- Родительский контроль.

Kaspersky Total Security расшифровывает зашифрованный трафик при работе пользователя в браузере Google Chrome, если в этом браузере отсутствует или выключено расширение Kaspersky Protection.

Предупреждение о работе компонента Анти-Спам

Функциональность компонента защиты Анти-Спам может быть изменена в результате изменения файла настройки компонента Анти-Спам.

Ограничения Резервного копирования

Резервное копирование имеет следующие ограничения:

- Онлайн-хранилище резервных копий становится недоступным при смене жесткого диска или при переходе на новый компьютер. Информацию о том, как восстановить подключение к Онлайн-хранилищу при смене оборудования, смотрите на веб-сайте Службы технической поддержки «Лаборатории Касперского».

- Изменение служебных файлов хранилища резервных копий может привести к тому, что вы потеряете доступ к хранилищу резервных копий и не сможете восстановить свои данные.

Ограничение функциональности Виртуальные сейфы

При создании сейфа в файловой системе FAT32 размер файла сейфа на диске не должен превышать 4 ГБ.

Особенности проверки памяти ядра на наличие руткитов во время работы в Защищенном браузере

В случае обнаружения недоверенного модуля во время работы Защищенного браузера открывается новая закладка браузера с уведомлением о том, что была обнаружена вредоносная программа. В этом случае рекомендуется закрыть браузер и выполнить полную проверку компьютера.

Особенности защиты данных буфера обмена

Kaspersky Total Security разрешает программе обращаться к буферу обмена в следующих случаях:

- Программа с активным окном пытается поместить данные в буфер обмена. Активным считается окно, с которым вы работаете в настоящий момент.

- Защищенный процесс программы пытается поместить данные в буфер обмена.

- Защищенный процесс программы или процесс с активным окном пытается получить данные из буфера обмена.

- Данные из буфера обмена пытается получить процесс программы, который ранее сам поместил эти данные в буфер обмена.

Предупреждение о совместимости с программами «Лаборатории Касперского»

Программа Kaspersky Total Security совместима со следующими программами «Лаборатории Касперского»:

- Kaspersky Fraud Prevention 2.0.
- Kaspersky Fraud Prevention 2.5.
- Kaspersky Fraud Prevention 3.0.
- Kaspersky Fraud Prevention 3.5.
- Kaspersky Fraud Prevention 4.0.
- Kaspersky Fraud Prevention 5.0.
- Kaspersky Password Manager 2.0.
- Kaspersky Password Manager 5.0.
- Kaspersky Password Manager 7.0.
- Kaspersky Password Manager 8.0.

Особенности обработки зараженных файлов компонентами программы

Программа по умолчанию может удалять зараженные файлы, если их лечение невозможно. Удаление по умолчанию может выполняться при обработке файлов такими компонентами, как Контроль программ, Почтовый Антивирус, Файловый Антивирус, при выполнении задач проверки, а также при обнаружении опасной активности программ компонентом Мониторинг активности.

Ограничения работы некоторых компонентов при совместной установке программы с Kaspersky Fraud Prevention for Endpoints

Работа следующих компонентов Kaspersky Total Security ограничивается в Защищенном браузере, если программа установлена совместно с Kaspersky Fraud Prevention for Endpoints:

- Веб-Антивирус, кроме Анти-Фишинга;
- Родительский контроль;
- Проверка ссылок;
- Анти-Баннер.

Предупреждение об изменении функциональности IM-Антивируса и Родительского контроля

Начиная с версии Kaspersky Total Security 2016 компонент IM-Антивирус не проверяет сообщения, переданные по протоколу IRC.

Начиная с версии Kaspersky Total Security 2016 компонент Родительский контроль не проверяет сообщения, переданные через IM-клиенты.

О содержании персональных данных в файлах отчетов

Файлы отчетов хранятся локально на вашем компьютере.

Путь к файлам отчетов: %allusersprofile%\Kaspersky Lab\AVP16.0.0\Report\Database.

Отчеты содержатся в следующих файлах:

- reports.db;
- reports.db-wal;
- reports.db-shm (не содержит персональных данных).

Файлы отчетов защищены от несанкционированного доступа, если в программе Kaspersky Total Security включена самозащита. Если самозащита выключена, файлы отчетов не защищаются.

Файлы отчетов могут содержать персональные данные, полученные в результате работы компонентов защиты, таких как Файловый Антивирус, Почтовый Антивирус, Анти-Спам, Родительский контроль.

Файлы отчетов могут содержать следующие персональные данные:

- IP-адрес устройства пользователя;
- история посещения веб-сайтов;
- версия браузера и операционной системы;
- имена и пути расположения файлов cookie и других файлов;
- адрес электронной почты, отправитель, тема письма, текст сообщений, имена пользователей, список контактов.

Особенности работы процесса Autorun

Процесс autorun выполняет запись результатов своей работы. Данные сохраняются в текстовые файлы с названием вида «kl-autorun-<date><time>.log». Чтобы просмотреть данные, требуется открыть окно **Выполнить** (**Запуск программы** в Windows XP), в поле **Открыть** ввести %TEMP% и нажать на кнопку **ОК**.

В файлы трассировки сохраняются пути к файлам установки, загруженным в ходе использования autorun. Данные хранятся в течение работы процесса autorun и безвозвратно удаляются при завершении этого процесса. Данные никуда не отправляются.

Ограничения работы Kaspersky Total Security при включенном режиме Device Guard на Microsoft Windows 10:

Недоступно включение компонента Защита от сетевых атак в интерфейсе программы.

Частично ограничена работа следующей функциональности:

- Поиск и лечение руткитов (отложенное лечение файлов при перезагрузке компьютера, обнаружение вредоносных программ, прописывающихся в системном реестре на автозапуск).
- Эвристический анализ (эмуляция запуска подозрительных программ).

О записи событий, касающихся Лицензионного соглашения и Kaspersky Security Network, в журнал событий Windows

События принятия или отказа от условий Лицензионного соглашения, а также принятия или отказа от участия в Kaspersky Security Network записываются в журнал Windows.

Ограничения проверки репутации локальных адресов в Kaspersky Security Network

Ссылки, ведущие на локальные ресурсы, не проверяются в Kaspersky Security Network.

Глоссарий

К

Kaspersky Security Network (KSN)

Инфраструктура облачных служб, 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 угрозы, 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.

Антивирусные базы

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

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».

Блокирование объекта

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

В

Виртуальный сейф

Специальное хранилище данных, в котором файлы хранятся в зашифрованном виде. Для получения доступа к таким файлам требуется ввод пароля. Виртуальные сейфы служат для предотвращения несанкционированного доступа к данным пользователей.

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.

Возможно зараженный объект

Объект, код которого содержит модифицированный участок кода известной программы, представляющей угрозу, или объект, напоминающий такую программу 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).

Г

Гипервизор

Программа, обеспечивающая параллельную работу нескольких операционных систем на одном компьютере.

Группа доверия

Группа, в которую Kaspersky Total Security помещает программу или процесс в зависимости от наличия электронной цифровой подписи программы, репутации программы в Kaspersky Security Network, доверия к источнику программы и потенциальной опасности действий, которые выполняет программа или процесс. На основании принадлежности программы к группе доверия Kaspersky Total Security может накладывать ограничения на действия этой программы в операционной системе.

В Kaspersky Total Security используются следующие группы доверия: «Доверенные», «Слабые ограничения», «Сильные ограничения», «Недоверенные».

Д

Доверенный процесс

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

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: задача полной проверки, задача обновления.

Зараженный объект

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

Защищенный браузер

Специальный режим работы обычного браузера, предназначенный для финансовых операций и покупок в интернете. С помощью Защищенного браузера программа защищает конфиденциальные данные, которые вы вводите на веб-сайтах банков и платежных систем (например, номера банковской карты, пароли для доступа к сервисам интернет-банкинга), а также предотвращает кражу платежных средств при проведении платежей онлайн. При этом в обычном браузере, использованном для обращения к веб-сайту, отображается сообщение о запуске Защищенного браузера.

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 кейлоггерами.

Код активации

Код, который вы получаете, приобретая лицензию на использование Kaspersky Total Security. Этот код необходим для активации программы.

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

Компоненты защиты

Части Kaspersky Total Security, 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 из-за 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. Таким объектам присваивается статус возможно зараженных.

Несовместимая программа

Антивирусная программа стороннего производителя или программа «Лаборатории Касперского», не поддерживающая управление через Kaspersky Total Security.

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 операционной системы и программного обеспечения вашего компьютера. Каждый раз при старте операционная система запускает эти объекты. Существуют вирусы, способные поражать именно объекты автозапуска, что может привести, например, к блокированию запуска операционной системы.

П

Пакет обновлений

Пакет файлов для обновления баз и программных модулей. 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.

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 установочного пакета программы «Лаборатории Касперского» и отвечающие за реализацию его основных задач. Каждому типу задач, реализуемых программой (защита, проверка, обновление баз и программных модулей), соответствует свой программный модуль.

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

Резервное копирование данных

Создание резервных копий данных, хранящихся на компьютере. Резервные копии создаются с целью предотвращения потери данных в результате кражи, поломки оборудования или действий злоумышленников.

Руткит

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

В операционных системах Windows под руткитом принято подразумевать программу, которая внедряется в операционную 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 операционной системе. Кроме того, как правило, руткит может маскировать присутствие в операционной системе любых описанных в его конфигурации процессов, каталогов и файлов на диске, ключей в реестре. Многие руткиты устанавливают в операционную 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 программных модулей.

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 сообщений электронной почты, чаще всего рекламного характера.

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 операционной 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

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 операционную систему или программу и нарушения ее целостности. Большое количество уязвимостей в операционной системе делает ее работу ненадежной, так как внедрившиеся в операционную систему вирусы могут вызывать сбои в работе как самой операционной системы, так и установленных программ.

Ф

Фишинг

Вид интернет-мошенничества, целью которого является получение неправомерного доступа к конфиденциальным данным пользователей.

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 операционной системе может представлять угрозу безопасности. 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).

АО «Лаборатория Касперского»

«Лаборатория Касперского» – известный в мире производитель систем компьютерной защиты от различных видов угроз, включая защиту от 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 конечных пользователей (рейтинг «IDC Worldwide Endpoint Security Revenue by Vendor»). В России, по данным IDC, «Лаборатория Касперского» – самый предпочитаемый производитель систем компьютерной защиты для домашних пользователей («IDC Endpoint Tracker 2014»).

«Лаборатория Касперского» основана в России в 1997 году. Сегодня «Лаборатория Касперского» – это международная группа компаний с 34 офисами в 31 стране мира. В компании работает более 3000 квалифицированных специалистов.

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

Линейка персональных продуктов включает программы, обеспечивающие информационную безопасность настольных компьютеров и ноутбуков, планшетных компьютеров, смартфонов и других мобильных устройств.

Компания предлагает решения и технологии для защиты и контроля рабочих станций и мобильных устройств, виртуальных машин, файловых и веб-серверов, почтовых шлюзов, сетевых экранов. Также в портфеле компании есть специализированные продукты для защиты от DDoS-атак, защиты сред под управлением АСУТП и предотвращения финансового мошенничества. Использование этих решений в сочетании с централизованными средствами управления позволяет построить и эксплуатировать эффективную автоматизированную защиту организации любого размера 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 тысяч новых компьютерных угроз, создают средства их обнаружения и лечения и включают сигнатуры этих угроз в базы, используемые программами «Лаборатории Касперского».

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 программного обеспечения, среди них: Alcatel-Lucent, Alt-N, Asus, BAE Systems, Blue Coat, Check Point, Cisco Meraki, Clearswift, D-Link, Facebook, General Dynamics, H3C, Juniper Networks, Lenovo, Microsoft, NETGEAR, Openwave Messaging, Parallels, Qualcomm, Samsung, Stormshield, Toshiba, Trustwave, Vertu, ZyXEL. Многие из инновационных технологий компании подтверждены патентами.

ДОСТИЖЕНИЯ. За годы борьбы с компьютерными угрозами «Лаборатория Касперского» завоевала сотни наград. Например, в 2014 году по итогам испытаний и исследований, проведенных авторитетной австрийской антивирусной лабораторией AV-Comparatives, «Лаборатория Касперского» стала одним из двух лидеров по количеству полученных сертификатов Advanced+, в результате компания была удостоена сертификата Top Rated. Но главная награда «Лаборатории Касперского» – это приверженность пользователей по всему миру. Продукты и технологии компании защищают более 400 миллионов пользователей. Количество организаций, являющихся ее клиентами, превышает 270 тысяч.

Веб-сайт «Лаборатории Касперского»:	http://www.kaspersky.ru
Вирусная энциклопедия:	http://www.securelist.ru/
Вирусная лаборатория:	http://newvirus.kaspersky.ru (для проверки подозрительных файлов и веб-сайтов)
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.

Dropbox – товарный знак Dropbox, Inc.

Google, Google Chrome, Chrome, YouTube – товарные знаки Google, Inc.

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

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

Mozilla, Firefox – товарные знаки Mozilla Foundation.

Skype – товарный знак компании Skype.

VMware – товарный знак VMware, Inc. или зарегистрированный в США или других юрисдикциях товарный знак VMware, Inc.

Mail.ru – зарегистрированный товарный знак, правообладателем которого является ООО «Мэйл.Ру».

Предметный указатель

K

A

Б

В

Д

И

К

Л

Н

О

П

Р

С

Т

У

Э