Kaspersky Internet Security

Руководство пользователя

ВЕРСИЯ ПРОГРАММЫ: 15.0 MAINTENANCE RELEASE 2

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 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: 29.04.2015

http://www.kaspersky.ru
http://support.kaspersky.ru

СОДЕРЖАНИЕ

ОБ ЭТОМ РУКОВОДСТВЕ

Этот документ представляет собой Руководство пользователя Kaspersky Internet Security 2015 Maintenance Release 2 (далее Kaspersky Internet Security).

Для успешного использования Kaspersky Internet 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 Internet Security, активировать и использовать программу.
- Обеспечить быстрый поиск информации для решения вопросов, связанных с работой Kaspersky Internet 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. 11)

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

Kaspersky Internet Security (см. стр. 13)

Этот раздел содержит описание возможностей программы, а также краткую информацию о функциях и компонентах программы. Вы узнаете о том, из чего состоит комплект поставки и какие услуги доступны зарегистрированным пользователям программы. В разделе приведена информация о том, каким программным и аппаратным требованиям должен отвечать компьютер, чтобы на него можно было установить программу.

Установка и удаление программы (см. стр. 18)

Этот раздел содержит пошаговые инструкции по установке и удалению программы.

Лицензирование программы (см. стр. 29)

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

Работа с уведомлениями программы (см. стр. 34)

Этот раздел содержит информацию о работе с уведомлениями программы.

Анализ состояния защиты компьютера и устранение проблем безопасности (см. стр. 35)

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

Обновление баз и программных модулей (см. стр. 36)

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

Проверка компьютера (см. стр. 37)

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

Восстановление удаленного или вылеченного программой объекта (см. стр. 40)

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

Восстановление операционной системы после заражения (см. стр. 41)

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

Защита электронной почты (см. стр. 43)

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

Защита личных данных в интернете (см. стр. 45)

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

Защита от баннеров при посещении веб-сайтов (см. стр. 57)

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

Устранение следов работы на компьютере и в интернете (см. стр. 59)

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

Контроль работы пользователей на компьютере и в интернете (см. стр. 62)

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

Сохранение ресурсов операционной системы для компьютерных игр (см. стр. 70)

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

Глоссарий (см. стр. 105)

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

ЗАО «Лаборатория Касперского» (см. стр. 111)

Этот раздел содержит информацию о ЗАО «Лаборатория Касперского».

Информация о стороннем коде (см. стр. 112)

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

Уведомления о товарных знаках (см. стр. 113)

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

Предметный указатель

Этот раздел позволяет быстро найти необходимые сведения в документе.

Условные обозначения

Текст документа сопровождается смысловыми элементами, на которые мы рекомендуем вам обращать особое внимание, – предупреждениями, советами, примерами.

Для выделения смысловых элементов используются условные обозначения. Условные обозначения и примеры их использования приведены в таблице ниже.

Таблица 1. Условные обозначения

Пример текста	Описание условного обозначения
Обратите внимание на то, что...	Предупреждения выделены красным цветом и заключены в рамку. В предупреждениях содержится информация о возможных нежелательных действиях, которые могут привести к потере информации, сбоям в работе оборудования или операционной системы.
Рекомендуется использовать...	Примечания заключены в рамку. Примечания могут содержать полезные советы, рекомендации, особые значения параметров или важные частные случаи в работе программы.
Пример: ...	Примеры приведены в блоках на желтом фоне под заголовком «Пример».

Пример текста	Описание условного обозначения
Обновление – это... Возникает событие *Базы устарели*.	Курсивом выделены следующие смысловые элементы текста: • новые термины; • названия статусов и событий программы.
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 нужно 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 пользователю.
<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 и сведения о веб-сайтах, которые вы можете использовать, чтобы обсудить работу программы.

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

В ЭТОМ РАЗДЕЛЕ

Источники информации для самостоятельного поиска

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

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

Если вы не нашли решения возникшей проблемы самостоятельно, рекомендуем вам обратиться в Службу технической поддержки «Лаборатории Касперского» (см. раздел «Техническая поддержка по телефону» на стр. 95).

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

Страница на веб-сайте «Лаборатории Касперского»

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

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

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

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

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

На странице программы в Базе знаний (http://support.kaspersky.ru/kis2015) вы найдете статьи, которые содержат полезную информацию, рекомендации и ответы на часто задаваемые вопросы о приобретении, установке и использовании программы.

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

Электронная справка

В состав электронной справки программы входят файлы справки.

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

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

Документация

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

Обсуждение программ «Лаборатории Касперского» на форуме

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

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

KASPERSKY INTERNET SECURITY

Этот раздел содержит описание возможностей программы, а также краткую информацию о функциях и компонентах программы. Вы узнаете о том, из чего состоит комплект поставки и какие услуги доступны зарегистрированным пользователям программы. В разделе приведена информация о том, каким программным и аппаратным требованиям должен отвечать компьютер, чтобы на него можно было установить программу.

В ЭТОМ РАЗДЕЛЕ

Что нового

В Kaspersky Internet Security появились следующие новые возможности:

- Добавлена поддержка последних версий популярных веб-браузеров: теперь компоненты защиты (например, Виртуальная клавиатура) поддерживают веб-браузеры Mozilla™ Firefox™ 32.x, 33.x, 34.x, Google Chrome™ 37.x, 38.x.
- Добавлена поддержка работы браузера Google Chrome для 64-х разрядной операционной системы.
- Повышено быстродействие программы и оптимизировано потребление ресурсов компьютера.
- Значительно сокращено время запуска программы.
- Улучшен процесс обновления программы на новые версии.
- Улучшена работа компонента Мониторинг активности: реализована защита от программ-крипторов. Если программа-криптор пытается выполнить шифрование файла, Kaspersky Internet Security автоматически создает резервную копию такого файла до того, как он будет зашифрован вредоносной программой-криптором. Резервные копии сохраняются в системной папке хранения временных файлов. Если программа-криптор зашифровала файл, Kaspersky Internet Security автоматически восстановит его из резервной копии. Функциональность имеет ограничения (см. раздел «Ограничения и предупреждения» на стр. 102).
- Улучшена работа компонента Безопасные платежи: добавлена запись событий, связанных с ослаблением защиты во время работы Защищенного браузера, в журнал событий. Также добавлена проверка доверенного защищенного соединения с сервисами «Лаборатории Касперского» и с веб-сайтами интернет-банков и платежных систем с помощью проверки сертификатов соответствующих веб-ресурсов.

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 Internet 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 Internet Security

Kaspersky Internet Security обеспечивает комплексную защиту вашего компьютера от известных и новых угроз, сетевых и мошеннических атак, а также спама. Для решения задач комплексной защиты в составе Kaspersky Internet Security предусмотрены различные функции и компоненты защиты.

Защита компьютера

Компоненты защиты предназначены для защиты компьютера от известных и новых 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 Internet 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 Internet 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 Internet 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 интернет-пейджерами. Компонент защищает информацию, поступающую на ваш компьютер по протоколам интернет-пейджеров. IM-Антивирус обеспечивает безопасную работу со многими программами, предназначенными для быстрого обмена сообщениями.

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.

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

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 Internet 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.

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 персональной информации, вводимой на веб-сайтах, от клавиатурных перехватчиков. Виртуальная 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 Internet 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.

Участие в программе «Защити друга»

Участие в программе «Защити друга» позволяет делиться с друзьями ссылками на Kaspersky Internet Security и получать за это бонусные баллы. Накопленные бонусные баллы вы можете обменять на бонусный код активации для Kaspersky Internet Security.

Сервис для пользователей

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

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

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

АППАРАТНЫЕ И ПРОГРАММНЫЕ ТРЕБОВАНИЯ

Общие требования:

- 480 МБ свободного места на жестком диске.
- CD- / DVD-ROM (для установки с установочного CD-диска).
- Подключение к интернету (для активации программы, а также обновления баз и программных модулей).
- Internet Explorer® 8.0 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/10978.

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:

- 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).

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.

УСТАНОВКА И УДАЛЕНИЕ ПРОГРАММЫ

Этот раздел содержит пошаговые инструкции по установке и удалению программы.

В ЭТОМ РАЗДЕЛЕ

СТАНДАРТНАЯ ПРОЦЕДУРА УСТАНОВКИ

Kaspersky Internet 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 этапе 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 Internet Security на ваш компьютер,*

  на установочном CD-диске запустите файл установочного пакета (файл с расширением exe).

Для установки Kaspersky Internet Security вы также можете использовать установочный пакет, полученный через интернет. При этом для некоторых языков локализации мастер установки отображает несколько дополнительных шагов установки.

Вместе с программой будут установлены расширения для веб-браузеров, обеспечивающие безопасную работу в интернете.

В ЭТОМ РАЗДЕЛЕ

Шаг 1. Поиск более новой версии программы

Перед началом установки мастер проверяет наличие более актуальной версии Kaspersky Internet 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 Internet 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 этапе мастер установки предлагает вам установить программу.

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

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

Шаг 3. Просмотр Лицензионного соглашения

Этот шаг мастера установки отображается для некоторых языков локализации при установке Kaspersky Internet Security с установочного пакета, полученного через интернет.

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

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

Если условия Лицензионного соглашения не приняты, установка программы не производится.

Шаг 4. Положение о Kaspersky Security Network

На этом этапе мастер установки предлагает вам принять участие в программе Kaspersky Security Network. Участие в программе предусматривает отправку в ЗАО «Лаборатория Касперского» информации о новых угрозах, обнаруженных на вашем компьютере, о запускаемых программах и о загружаемых подписанных программах, а также информации 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 Internet 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 Internet 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.

  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 Internet Security не может удалить автоматически, необходимо удалить вручную. Во время удаления несовместимых программ потребуется перезагрузка операционной системы, после чего установка Kaspersky Internet 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 этапе мастер информирует вас о завершении установки программы. Чтобы начать работу с Kaspersky Internet Security немедленно, убедитесь, что флажок **Запустить Kaspersky Internet Security** установлен, и нажмите на кнопку **Завершить**.

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

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

Шаг 7. Активация программы

При первом запуске Kaspersky Internet Security запускается мастер активации программы.

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

Вам предлагаются следующие варианты активации Kaspersky Internet Security:

- **Активировать программу**. Выберите этот вариант и введите код активации, если вы приобрели лицензию на использование программы.

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

- **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 Internet 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 **Далее**.

В некоторых случаях регистрация пользователя необходима для использования программы.

Шаг 9. Завершение активации

Мастер информирует вас об успешном завершении активации Kaspersky Internet Security. Кроме того, в окне приводится информация о действующей лицензии: дата окончания срока действия лицензии, а также количество компьютеров, на которые эта лицензия распространяется.

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

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

Установка программы из командной строки

Вы можете установить Kaspersky Internet 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/11173#block2).

Обновление предыдущей версии программы

Установка новой версии Kaspersky Internet Security поверх Kaspersky Internet Security предыдущей версии

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

Установка новой версии Kaspersky Internet Security поверх Kaspersky Anti-Virus предыдущей версии

Если вы устанавливаете новую версию Kaspersky Internet Security на компьютер, на котором уже установлена программа Kaspersky Anti-Virus одной из предыдущих версий с действующей лицензией, мастер активации предложит вам выбрать вариант дальнейших действий:

- Продолжить использовать Kaspersky Anti-Virus по действующей лицензии. В этом случае будет запущен мастер миграции, в результате работы которого на ваш компьютер будет установлена новая версия Kaspersky Anti-Virus. Вы сможете использовать Kaspersky Anti-Virus в течение срока действия лицензии на использование Kaspersky Anti-Virus предыдущей версии.

- Продолжить установку новой версии Kaspersky Internet Security. В этом случае программа будет установлена и активирована согласно стандартному сценарию.

Kaspersky Internet 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 этапе 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 Internet Security на ваш компьютер,

на установочном CD-диске запустите файл установочного пакета (файл с расширением exe).

Для установки Kaspersky Internet Security вы также можете использовать установочный пакет, полученный через интернет. При этом для некоторых языков локализации мастер установки отображает несколько дополнительных шагов установки.

Вместе с программой будут установлены расширения для веб-браузеров, обеспечивающие безопасную работу в интернете.

Обновление предыдущей версии программы имеет ограничения (см. раздел «Ограничения и предупреждения» на стр. 102).

В этом разделе

Шаг 1. Поиск более новой версии программы

Перед началом установки мастер проверяет наличие более актуальной версии Kaspersky Internet 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 Internet 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 этапе мастер установки предлагает вам установить программу.

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

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

Шаг 3. Просмотр Лицензионного соглашения

Этот шаг мастера установки отображается для некоторых языков локализации при установке Kaspersky Internet Security с установочного пакета, полученного через интернет.

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

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

Если условия Лицензионного соглашения не приняты, установка программы не производится.

Шаг 4. Положение о Kaspersky Security Network

На этом этапе мастер установки предлагает вам принять участие в программе Kaspersky Security Network. Участие в программе предусматривает отправку в ЗАО «Лаборатория Касперского» информации о новых угрозах, обнаруженных на вашем компьютере, о запускаемых программах и о загружаемых подписанных программах, а также информации 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 Internet 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 Internet 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.

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

Это окно мастера информирует вас о завершении установки программы.

По завершении установки необходимо перезагрузить операционную систему.

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

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

Переход с Kaspersky Internet Security к использованию Kaspersky Total Security

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

По сравнению с Kaspersky Internet Security программа Kaspersky Total Security обладает рядом дополнительных возможностей:

- Резервное копирование. С помощью автоматического резервного копирования по расписанию вы можете сохранять свои данные на съемных и сетевых дисках, а также в Онлайн-хранилище.
- Защита личной информации. Для защиты ваших личных данных используются Виртуальные сейфы. Вы можете положить файлы в сейф и закрыть его, чтобы никто, кроме вас, не мог получить доступ к этим файлам.
- Защита паролей. Для защиты данных, которые вы вводите в интернете, используется программа Kaspersky Password Manager. С ее помощью вы можете сохранять логины и пароли в хранилище и автоматически заполнять поля ввода в интернете.
- Удаленное управление. С помощью функции Удаленного управления вы можете удаленно управлять защитой ваших компьютеров.

Вы можете временно перейти на пробную версию Kaspersky Total Security, чтобы изучить ее возможности, или приобрести лицензию и перейти к использованию Kaspersky Total Security.

В этом разделе

Временное использование Kaspersky Total Security

Вы можете временно перейти на пробную версию Kaspersky Total Security, чтобы оценить ее возможности. При желании вы можете приобрести лицензию для постоянной работы с программой.

Чтобы временно перейти на пробную версию Kaspersky Total Security, выполните следующие действия:

1. Откройте главное окно программы.
2. По ссылке **Показать дополнительные инструменты** перейдите в окно **Дополнительные инструменты**.
3. В окне **Дополнительные инструменты** по ссылке **Перейти к использованию Kaspersky Total Security** запустите мастер миграции.

4. В открывшемся окне мастера миграции нажмите на кнопку **Пробная версия**.

5. Следуйте указаниям мастера.

Шаг 1. Начало расширения защиты

На этом шаге мастер выводит на экран сообщение о готовности к переходу на пробную версию Kaspersky Total Security. Для продолжения работы мастера нажмите на кнопку **Продолжить**.

Шаг 2. Удаление несовместимых программ

На этом шаге мастер проверяет, нет ли на вашем компьютере программ, несовместимых с Kaspersky Total Security. Если таких программ нет, мастер автоматически переходит к следующему шагу. Если такие программы найдены, мастер выводит их список в окне и предлагает вам удалить их.

После удаления несовместимых программ может потребоваться перезагрузка операционной системы. После перезагрузки мастер запускается автоматически, и процесс перехода на пробную версию Kaspersky Total Security продолжается.

Шаг 3. Переход к использованию пробной версии Kaspersky Total Security

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

Шаг 4. Перезапуск программы

На этом шаге перехода к пробной версии Kaspersky Total Security требуется перезапустить программу. Для этого нажмите на кнопку **Завершить** в окне мастера.

Шаг 5. Завершение активации

После перезапуска программы открывается окно **Лицензирование** программы Kaspersky Total Security, где отображается информация о сроке, в течение которого вы можете использовать пробную версию.

Если при переходе на Kaspersky Total Security срок действия лицензии на программу Kaspersky Internet Security не истек, вы можете продолжить использование Kaspersky Internet Security по этой лицензии на другом комьютере.

Переход к постоянному использованию Kaspersky Total Security

Если вы хотите перейти к постоянному использованию Kaspersky Total Security, вам необходимо приобрести лицензию на использование Kaspersky Total Security и затем активировать программу.

Чтобы приобрести лицензию на использование Kaspersky Internet Security, выполните следующие действия:

1. Откройте главное окно программы.

2. В раскрывающемся списке **Показать дополнительные инструменты** откройте окно **Дополнительные инструменты**.

3. По ссылке **Переход к использованию Kaspersky Total Security** запустите мастер миграции.

4. По ссылке **Купить код активации** перейдите на веб-сайт интернет-магазина «Лаборатории Касперского» или компании-партнера, где вы можете приобрести лицензию на Kaspersky Total Security.

При использовании программы по подписке, а также при работе с программой в некоторых регионах переход на использование Kaspersky Total Security не предусмотрен. В этих случаях элемент **Переход к использованию Kaspersky Total Security** отсутствует.

Удаление программы

В результате удаления Kaspersky Internet Security компьютер и ваши личные данные окажутся незащищенными.

Удаление Kaspersky Internet Security выполняется с помощью мастера установки.

Чтобы запустить мастер,

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

В этом разделе

Шаг 1. Ввод пароля для удаления программы

Чтобы удалить Kaspersky Internet 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 Internet Security с компьютера файлы на карантине будут недоступны. Для работы с этими файлами нужно установить Kaspersky Internet 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 личных 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 Internet 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 активацией программы. Из этого раздела вы узнаете о назначении Лицензионного соглашения, способах активации программы, а также о продлении срока действия лицензии.

В ЭТОМ РАЗДЕЛЕ

О Лицензионном соглашении

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

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

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

О лицензии

Лицензия – это ограниченное по времени право на использование программы, предоставляемое вам на основе Лицензионного соглашения. С лицензией связан уникальный код активации вашего экземпляра Kaspersky Internet 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 (см. раздел «Сервис для пользователей» на стр. 16).

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

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

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 Internet Security без выплаты вознаграждения. Пробная версия Kaspersky Internet Security выполняет свои функции в течение короткого ознакомительного периода. После окончания ознакомительного периода Kaspersky Internet Security прекращает выполнять все свои функции. Для продолжения использования программы требуется приобрести лицензию.

О коде активации

Код активации – это код, который вы получаете, приобретая лицензию на использование Kaspersky Internet 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 Internet Security, код активации указан в документации или на коробке, в которой находится установочный компакт-диск.
- Если вы приобрели Kaspersky Internet Security в интернет-магазине, код активации высылается по адресу электронной почты, указанному вами при заказе.
- Если вы участвуете в программе «Защити друга» (см. раздел «Участие в программе “Защити друга”» на стр. 89), вы можете получить бонусный код активации в обмен на бонусные баллы.

Отсчет срока действия лицензии начинается с даты активации программы. Если вы приобрели лицензию, допускающую использование Kaspersky Internet 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 Internet Security – это использование программы с выбранными параметрами (дата окончания, количество защищаемых устройств). Подписку на Kaspersky Internet 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 Internet 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 Internet 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 будет предоставлен льготный период для продления подписки, в течение которого функциональность программы будет сохранена.

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

Чтобы использовать Kaspersky Internet 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 будет возможно только после окончания подписки.

Если на момент регистрации подписки, Kaspersky Internet Security уже используется по действующей лицензии, то после регистрации подписки Kaspersky Internet 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 Internet 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

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

- информацию о контрольных суммах обрабатываемых файлов (MD5, sha256);
- информацию для определения репутации веб-адресов;
- статистику использования уведомлений программы;
- статистические данные для защиты от спама;
- данные об активации и используемой версии Kaspersky Internet Security;
- информацию о лицензировании установленной версии Kaspersky Internet Security;
- информацию о типах обнаруженных угроз;
- информацию об используемых цифровых сертификатах и информацию, необходимую для проверки их подлинности;
- данные о работе программы и лицензии, необходимые для настройки отображения содержимого доверенных сайтов.

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

Если вы участвуете в программе Kaspersky Security Network (см. раздел «Участие в Kaspersky Security Network (KSN)» на стр. 87), вы соглашаетесь в автоматическом режиме передавать в «Лабораторию Касперского» следующую информацию, полученную в результате работы Kaspersky Internet Security на компьютере:

- информация об установленном аппаратном и программном обеспечении;
- информация о состоянии антивирусной защиты компьютера, а также обо всех возможно зараженных объектах и решениях, принятых относительно этих объектов;

- информация о загружаемых и запускаемых программах;
- информация об ошибках и использовании пользовательского интерфейса Kaspersky Internet Security;
- информация о программе, включая версию программы, информацию о файлах загружаемых программных модулей, версии используемых баз программы;
- статистика обновлений и соединений с серверами «Лаборатории Касперского»;
- информация об используемом беспроводном подключении компьютера;
- статистика задержек, вызванных Kaspersky Internet Security, при работе пользователя с установленными на компьютере программами;
- файлы, которые могут быть использованы злоумышленником для нанесения вреда компьютеру, или их части, в том числе файлы, обнаруженные по вредоносным ссылкам.

Информация для передачи в «Лабораторию Касперского» может храниться на вашем компьютере не более 30 дней с момента создания. Хранение происходит во внутреннем защищенном хранилище. Максимальный объем сохраняемой информации 30 МБ.

Также вы соглашаетесь в автоматическом режиме передавать в «Лабораторию Касперского» для дополнительной проверки файлы (или их части), в отношении которых существует риск использования их злоумышленником для нанесения вреда компьютеру или данным.

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

Приобретение лицензии

Если вы установили Kaspersky Internet Security, не приобретя лицензию заранее, вы можете приобрести лицензию после установки программы. При приобретении лицензии вы получите код активации, с помощью которого нужно активировать программу (см. раздел «Активация программы» на стр. 32).

Чтобы приобрести лицензию, 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 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 Internet Security, появляющиеся в области уведомлений панели задач.

Чтобы активировать программу Kaspersky Internet 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 Internet 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 Internet 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 Internet 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 Internet Security или в режиме Connected Standby в Windows 8. При автоматическом закрытии уведомления Kaspersky Internet Security выполнит действие, рекомендованное по умолчанию.

Уведомления не отображаются в течение первого часа работы программы в случае приобретения компьютера с предустановленной программой Kaspersky Internet 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.

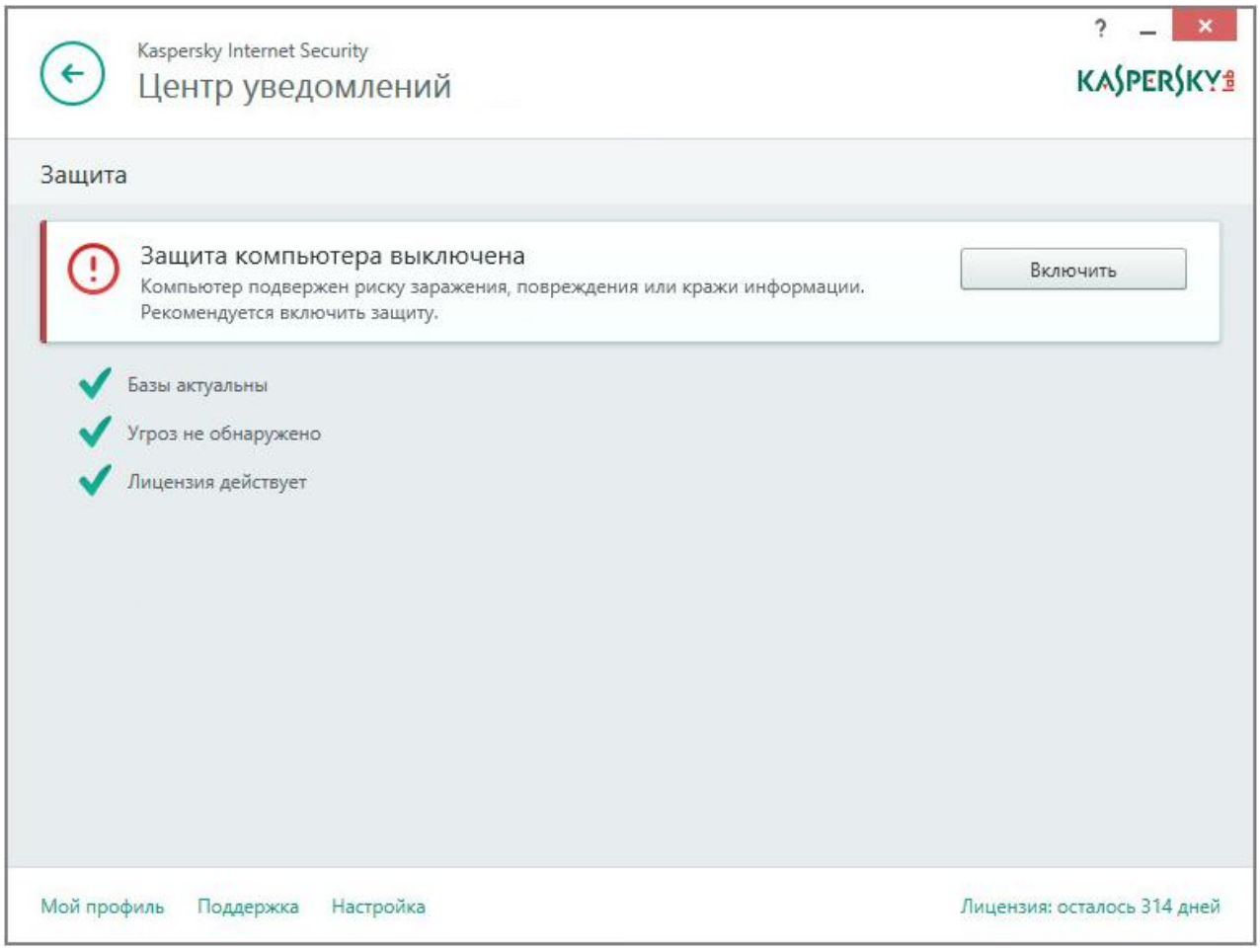

Рисунок 1. Окно Центр уведомлений

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

По умолчанию Kaspersky Internet Security автоматически проверяет наличие пакета обновлений на серверах обновлений «Лаборатории Касперского». Если на сервере содержится новый пакет обновлений, Kaspersky Internet Security загружает и устанавливает его в фоновом режиме. Вы можете в любой момент запустить обновление Kaspersky Internet Security вручную из главного окна программы или из контекстного меню значка программы в области уведомлений панели задач.

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

При работе в операционной системе Microsoft Windows 8 загрузка пакетов обновлений не производится, если используется высокоскоростное мобильное подключение к интернету и в программе настроено ограничение трафика при этом типе подключения. Чтобы выполнить загрузку пакета обновлений, необходимо вручную отключить ограничение в подразделе **Сеть** окна настройки программы.

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

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

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

  1. Откройте главное окно программы и 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 Internet Security проверяет следующие объекты:

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

Рекомендуется выполнить полную проверку сразу после установки Kaspersky Internet 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 Internet 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**.

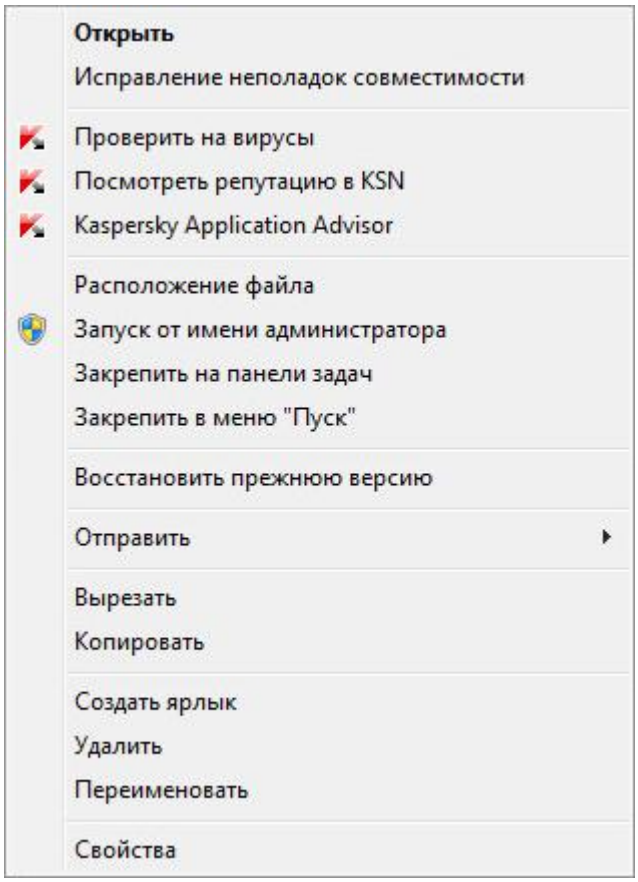

Рисунок 2. Контекстное меню объекта

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 по умолчанию Kaspersky Internet Security проверяет следующие объекты:

- объектов, которые загружаются при запуске операционной системы;
- системной памяти;
- загрузочных секторов 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 Internet 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. По ссылке **Показать дополнительные инструменты**, расположенной 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 Internet 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 Internet 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 Internet 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. По ссылке **Показать дополнительные инструменты**, расположенной 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. По ссылке **Показать дополнительные инструменты**, расположенной 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 с точки зрения опасности, которую они представляют. Для каждой группы повреждений специалисты «Лаборатории Касперского» предлагают набор действий, выполнение которых поможет устранить повреждения. Всего выделено три группы действий:

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

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

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

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

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

Шаг 4. Устранение 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.

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 Internet 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. В нижней части окна перейдите по ссылке **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 как входящие, так и исходящие сообщения, а также проверяет вложенные архивы.
   - **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, а также вложенные архивы. При выборе высокого уровня безопасности применяется глубокий уровень эвристического анализа.
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 Internet Security. В случае удаления объекта Kaspersky Internet Security создает его резервную копию и помещает на карантин (см. раздел «Восстановление удаленного или вылеченного программой объекта» на стр. 40).

Блокирование нежелательной почты (спама)

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

Чтобы включить Анти-Спам и установить рекомендуемый уровень безопасности, выполните следующие действия:

1. Откройте главное окно программы.
2. По ссылке **Настройка** в нижней части окна перейдите в раздел **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**.

ЗАЩИТА ЛИЧНЫХ 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 ЛИЧНЫХ ДАННЫХ В ИНТЕРНЕТЕ

С помощью Kaspersky Internet Security вы можете защитить от кражи свои личные данные:

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

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

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

Для защиты от перехвата данных с клавиатуры предназначена Виртуальная 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 личных данных через интернет предназначен один из инструментов Родительского контроля (см. раздел «Использование Родительского контроля» на стр. 62).

О Виртуальной 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 персональной информации с помощью аппаратных перехватчиков или клавиатурных перехватчиков – программ, регистрирующих нажатие клавиш. Виртуальная 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. Виртуальная клавиатура защищает вводимые персональные данные от перехвата посредством снятия снимков экрана.

Виртуальная клавиатура имеет следующие особенности:

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

Для защиты данных, вводимых с помощью Виртуальной клавиатуры, после установки Kaspersky Internet Security необходимо перезагрузить компьютер.

Использование Виртуальной клавиатуры имеет следующие ограничения:

- Виртуальная клавиатура защищает от перехвата персональной информации только при работе с браузерами Microsoft Internet Explorer, Mozilla Firefox и Google Chrome. При работе с другими браузерами Виртуальная клавиатура не защищает вводимые персональные данные от перехвата.
- Виртуальная клавиатура недоступна в браузере Microsoft Internet Explorer (версии 10 и 11) в стиле нового интерфейса Windows, а также в браузере Microsoft Internet Explorer (версии 10 и 11), если в параметрах браузера установлен флажок **Включить расширенный защищенный режим** (Enhanced Protected Mode). В этом случае рекомендуется вызывать виртуальную клавиатуру из интерфейса Kaspersky Internet Security.
- Виртуальная клавиатура не может защитить ваши персональные данные в случае взлома веб-сайта, требующего ввода таких данных, поскольку в этом случае информация попадет непосредственно в руки злоумышленников.
- Виртуальная клавиатура не предотвращает снятие снимков экрана с помощью нажатия клавиши **PRINT SCREEN** и других комбинаций клавиш, заданных в параметрах операционной системы.
- При запуске Виртуальной клавиатуры в браузере Microsoft Internet Explorer перестает работать функция автозаполнения полей ввода, так как реализация системы автозаполнения позволяет злоумышленникам перехватывать вводимые данные.
- Kaspersky Internet Security не защищает от создания снимков экрана в операционной системе Microsoft Windows 8 и 8.1 (только 64-разрядные), если открыто окно Виртуальной клавиатуры, но не запущен процесс Защищенного браузера.
- В некоторых браузерах (например, Google Chrome) может не работать защита ввода данных определенного типа (например, адресов электронной почты или чисел).

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/11047.

Запуск виртуальной клавиатуры

Открыть Виртуальную клавиатуру можно следующими способами:

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

  Отображение значка быстрого вызова в полях ввода на веб-сайтах можно настроить (см. раздел «Настройка отображения значка Виртуальной клавиатуры» на стр. 48).

  При использовании Виртуальной клавиатуры Kaspersky Internet Security отключает функцию автозаполнения полей ввода на веб-сайтах.

- с помощью комбинации клавиш аппаратной клавиатуры.

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

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

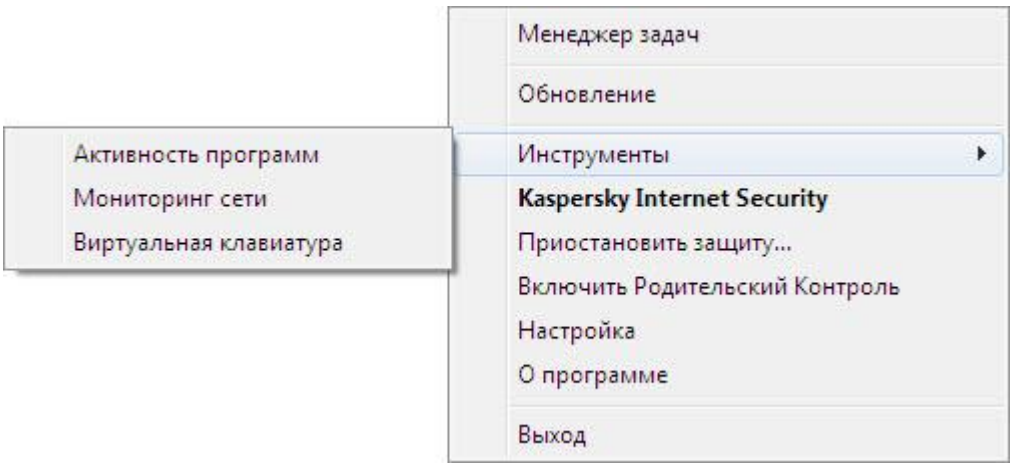

Рисунок 3. Контекстное меню Kaspersky Internet Security

Чтобы открыть Виртуальную клавиатуру из главного окна программы, выполните следующие действия:

1. Откройте главное окно программы.
2. По ссылке **Показать дополнительные инструменты**, расположенной в нижней части главного окна, откройте окно **Инструменты**.
3. В левой части окна **Инструменты** по ссылке **Виртуальная клавиатура** откройте Виртуальную клавиатуру.

- *Чтобы открыть Виртуальную клавиатуру из окна браузера Microsoft Internet Explorer или Mozilla Firefox,*

  нажмите на кнопку  **Виртуальная клавиатура** в панели инструментов браузера.

- *Чтобы открыть Виртуальную клавиатуру из окна браузера Google Chrome,*

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

- *Чтобы открыть Виртуальную клавиатуру с помощью аппаратной клавиатуры,*

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

Настройка отображения значка Виртуальной клавиатуры

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

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

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

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

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

        Значок вызова Виртуальной клавиатуры будет отображаться при открытии веб-сайта, относящегося к какой-либо из выбранных категорий.

     c. Если вы хотите включить или выключить отображение значка вызова Виртуальной клавиатуры на определенном веб-сайте, выполните следующие действия:

        a. По ссылке **Настройка исключений** откройте окно **Исключения для Виртуальной клавиатуры**.

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

           Откроется окно для добавления исключения для Виртуальной клавиатуры.

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

d. Если вы хотите, чтобы значок вызова Виртуальной клавиатуры отображался (или не отображался) только на указанной веб-странице, в блоке **Область применения** выберите **Применить к указанной странице**.

e. В блоке **Значок Виртуальной клавиатуры** укажите, должен ли значок вызова Виртуальной клавиатуры отображаться на указанной веб-странице.

f. Нажмите на кнопку **Добавить**.

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

При открытии указанного веб-сайта значок вызова Виртуальной 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 в интернет-браузерах Microsoft Internet Explorer, Mozilla Firefox и Google Chrome. При работе с другими интернет-браузерами данные, вводимые с аппаратной клавиатуры, не защищаются от перехвата.
- Защита ввода данных 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 некоторых браузерах (например, Google Chrome) может не работать защита ввода данных определенного типа (например, адресов электронной почты или чисел).

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/11047.

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. По ссылке **Настройка** в нижней части окна перейдите в раздел **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. Задайте область защиты ввода данных с аппаратной клавиатуры:

   a. Откройте окно **Параметры Безопасного ввода данных** по ссылке **Изменить категории** в нижней части блока **Защита ввода данных с аппаратной клавиатуры**.

   b. Установите флажки для категорий веб-сайтов, на которых нужно защищать данные, вводимые с клавиатуры.

c. Если вы хотите включить 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**.

      Откроется окно для добавления исключения для аппаратной клавиатуры.

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

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

   e. Выберите действие защиты ввода данных на этом веб-сайте (**Защищать** или **Не защищать**).

   f. 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 Internet 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. По ссылке **Настройка** в нижней части окна перейдите в раздел **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.

Защита 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 Internet 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.

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 правильной работы Защищенного браузера необходимо, чтобы в нем были активированы плагины компонента Безопасные платежи. Плагины автоматически активируются в браузере при его первом перезапуске после установки Kaspersky Internet Security. Если браузер не перезапускался после установки Kaspersky Internet Security, плагины не активируются.

Автоматическая активация плагинов имеет следующие ограничения:

- Плагины встраиваются и активируются только в браузерах, поддерживаемых программой.

  Следующие браузеры поддерживают плагины Безопасных платежей:

  - 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 19.x, 20.x, 21.x, 22.x, 23.x, 24.x, 25.x, 26.x, 27.x, 28.x, 29.x, 30.x, 31.x, 32.x, 33.x, 34.x, 35.x.

  - Google Chrome версий 33.x, 34.x, 35.x, 36.x, 37.x, 38.x.

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

    В Mozilla Firefox плагины не активируются автоматически, если в браузере не был создан профиль пользователя. Для создания профиля пользователя необходимо перезапустить браузер.

    При первом запуске Google Chrome в защищенном режиме веб-браузер предложит вам установить расширение Kaspersky Protection Plugin, которое активирует плагины компонента Безопасные платежи. В случае отказа от установки расширения Kaspersky Protection Plugin вы можете установить его позднее по ссылке http://support.kaspersky.com/interactive/google/ru/kisplugin.

- При обновлении браузера плагины не активируются автоматически, если новая версия браузера не поддерживает ту же технологию активации плагинов, что и предыдущая версия браузера. Если новая версия браузера поддерживает ту же технологию активации плагинов, что и предыдущая версия браузера, плагины активируются автоматически.

Если плагины не активировались автоматически при перезапуске браузера, требуется активировать их вручную. Посмотреть, активированы ли плагины, и активировать их вручную можно в параметрах браузера. Информацию об активации плагинов можно посмотреть в справке используемого браузера.

Вы можете включить или выключить автоматическую активацию плагинов (см. раздел «Включение автоматической активации плагинов Безопасных платежей» на стр. 54) в окне настройки программы.

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

В этом разделе

Настройка параметров Безопасных платежей

Чтобы настроить Безопасные платежи, выполните следующие действия:

1. Откройте главное окно программы.
2. По ссылке **Настройка** в нижней части главного окна перейдите в раздел **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. В нижней части главного окна нажмите на кнопку **Безопасные платежи**.

   Откроется окно **Безопасные платежи**.
3. Нажмите на кнопку **Добавить веб-сайт в Безопасные платежи**.

   В правой части окна отобразятся 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://, по умолчанию используемый Защищенным браузером.
5. При необходимости в поле **Описание** 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 Internet 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 плагинов Безопасных платежей

Чтобы включить активацию плагинов Безопасных платежей в браузерах, выполните следующие действия:

1. Откройте главное окно программы.
2. По ссылке **Настройка** в нижней части главного окна перейдите в раздел **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 **Расширения веб-браузеров** установите флажок **Автоматически активировать плагины программы во всех веб-браузерах**.

О защите от создания снимков экрана

Kaspersky Internet 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. 54).

Kaspersky Internet Security использует технологию гипервизора для защиты от создания снимков экрана. Функциональность защиты от создания снимков экрана с помощью гипервизора Kaspersky Internet Security имеет следующие ограничения в операционной системе Microsoft Windows 8 x64:

- 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. По ссылке **Настройка** в нижней части окна перейдите в раздел **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**.

О защите данных буфера обмена

Kaspersky Internet 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.

Проверка безопасности веб-сайта

Kaspersky Internet Security позволяет проверить безопасность веб-сайта, прежде чем перейти по ссылке на этот веб-сайт. Для проверки веб-сайтов используется *модуль проверки ссылок*, входящий в состав компонента Веб-Антивирус.

Модуль проверки ссылок недоступен в браузере Microsoft Internet Explorer (версии 10 и 11) в стиле Windows 8.

Модуль проверки ссылок встраивается в браузеры Microsoft Internet Explorer, Google Chrome и Mozilla Firefox и проверяет ссылки на открытой в браузере веб-странице. Рядом с каждой ссылкой Kaspersky Internet 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 Internet 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. По ссылке **Настройка** в нижней части главного окна откройте 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 **Модуль проверки ссылок** установите флажок **Проверять ссылки**.
6. Чтобы Веб-Антивирус проверял содержимое всех веб-сайтов, выберите вариант **На всех веб-сайтах, кроме указанных**.

   Если необходимо, укажите веб-страницы, которым вы доверяете, по ссылке **Настроить исключения**. Веб-Антивирус не будет проверять содержимое указанных веб-страниц, а также зашифрованные соединения с указанными веб-сайтами.

7. Чтобы Веб-Антивирус проверял содержимое только определенных веб-страниц, выполните следующие действия:

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

   b. Пройдите по ссылке **Настроить проверяемые веб-сайты**.

   c. В открывшемся окне **Настроить проверяемые веб-сайты** нажмите на кнопку **Добавить**.

   d. В открывшемся окне **Добавить URL** введите адрес веб-страницы, содержимое которой необходимо проверять.

   e. Выберите статус проверки веб-страницы (*Активно* – Веб-Антивирус будет проверять содержимое веб-страницы).

   f. Нажмите на кнопку **Добавить**.

      Указанная веб-страница появится в списке в окне **Проверяемые адреса**. Веб-Антивирус будет проверять ссылки на этой веб-странице.

8. Если вы хотите настроить дополнительные параметры проверки ссылок, в окне **Дополнительные параметры Веб-Антивируса** в блоке **Модуль проверки ссылок** пройдите по ссылке **Настроить модуль проверки ссылок**.

   Откроется окно **Настроить модуль проверки ссылок**.

9. Чтобы Веб-Антивирус предупреждал о безопасности ссылок на всех веб-страницах, в блоке **Проверяемые ссылки** выберите вариант **Любые ссылки**.

10. Чтобы Веб-Антивирус 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.

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

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 Internet Security будет блокировать отображение баннеров на этом веб-сайте. По умолчанию Kaspersky Internet 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. По ссылке **Настройка** перейдите в окно **Настройка**.
3. Выберите раздел **Защита**.
4. Включите компонент **Анти-Баннер**.

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. По ссылке **Настройка** перейдите в окно **Настройка**.
3. Выберите раздел **Защита**.
4. Выберите компонент **Анти-Баннер**.

   Откроется окно **Параметры Анти-Баннера**.
5. В окне **Параметры Анти-Баннера** по ссылке **Настроить запрещенные веб-адреса** откройте окно **Запрещенные веб-адреса**.
6. В окне **Запрещенные веб-адреса** нажмите на кнопку **Добавить**.
7. 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*`.
8. В качестве статуса для этого веб-сайта укажите **Активно**.
9. Нажмите на кнопку **Добавить**.

Kaspersky Internet 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 конфиденциальную информацию, могут оказаться доступными злоумышленникам и посторонним лицам.

В состав Kaspersky Internet 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. По ссылке **Показать дополнительные инструменты**, расположенной в нижней части главного окна, откройте окно **Инструменты**.
3. В левой части окна **Инструменты** 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).

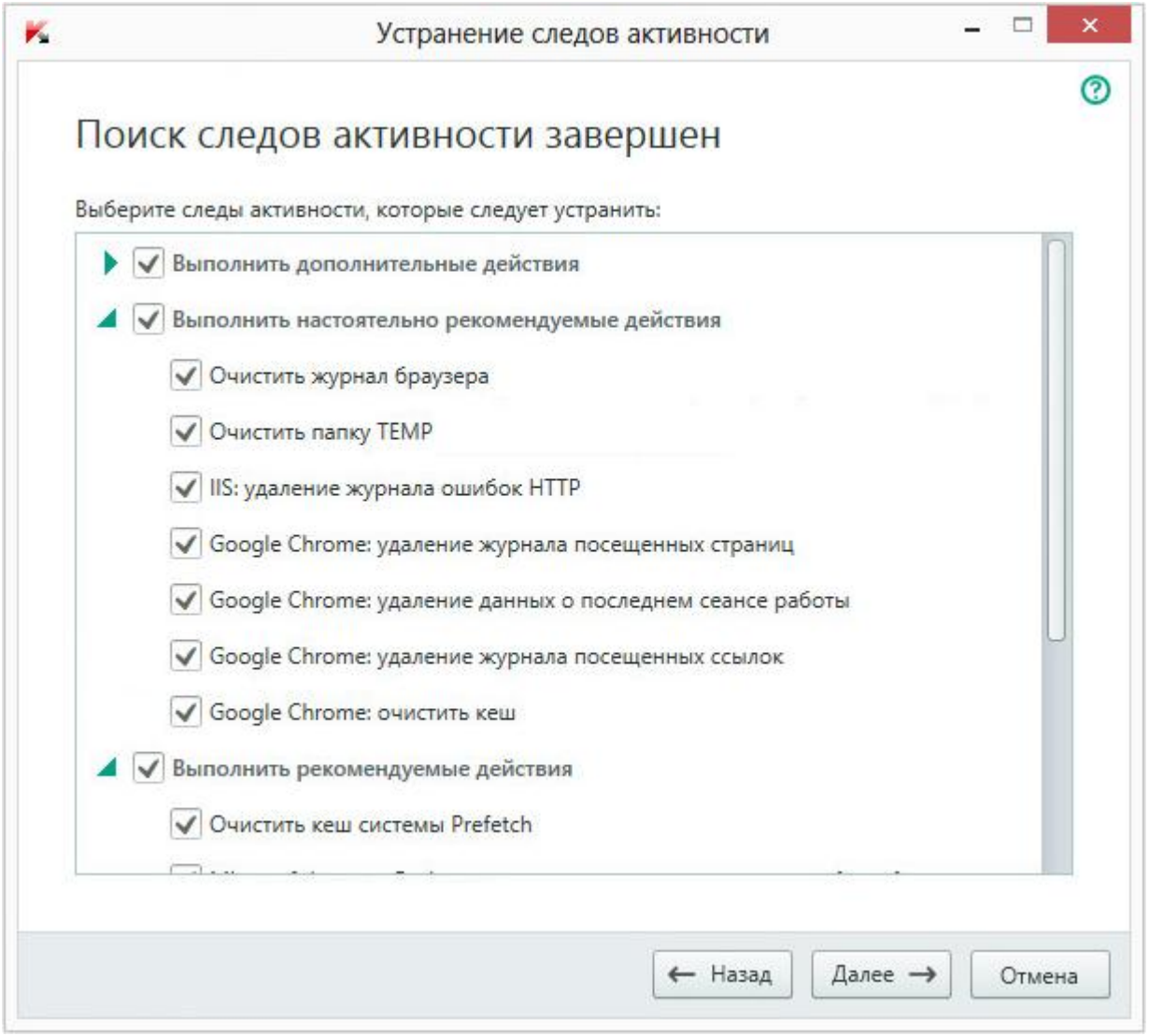

Рисунок 4. Обнаруженные следы активности и рекомендации по их устранению

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 Internet 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 личную 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 программах мгновенного обмена сообщениями и в социальных сетях;
- просмотр текста переписки в программах мгновенного обмена сообщениями и 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. При первом входе в окно **Родительский контроль** программа предложит задать пароль для защиты параметров Родительского контроля. Выберите один из предложенных вариантов действия:
   - Если вы хотите защитить паролем доступ к параметрам Родительского контроля, заполните поля **Пароль** и **Подтверждение** и нажмите на кнопку **Продолжить**.
   - 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. 63).
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 каждые** и выберите периодичность (например, каждый час) и длительность (например, 10 минут) перерывов в раскрывающихся списках рядом с флажком.

8. В окне **Родительский контроль** включите переключатель **Родительский контроль**, расположенный напротив учетной записи пользователя.

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. 63).

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 <ЧЧ:ММ> часов в день** 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 <ЧЧ:ММ> часов в день** и выберите ограничение по времени в раскрывающемся списке рядом с флажком.

5. В окне **Родительский контроль** включите переключатель **Родительский контроль**, расположенный напротив учетной записи пользователя.

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. 63).

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

3. Чтобы в результатах поиска не отображалось содержание «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 содержание «для взрослых».

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

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

   b. Выберите вариант **Веб-сайты для взрослых** 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 **Блокировать доступ к следующим веб-сайтам**.

   b. Выберите вариант **Все веб-сайты, кроме разрешенных в списке исключений** и по ссылке **Добавить исключения** откройте окно **Исключения**.

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

      Откроется окно **Добавить новый веб-сайт**.

   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**.

6. В окне **Родительский контроль** включите переключатель **Родительский контроль**, расположенный напротив учетной записи пользователя.

Родительский контроль будет блокировать посещение веб-сайтов, указанных в списке, в соответствии с настроенными 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. 63).

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. В окне **Родительский контроль** включите переключатель **Родительский контроль**, расположенный напротив учетной записи пользователя.

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, программ мгновенного обмена сообщениями) или ограничить время использования программ.

- *Чтобы запретить запуск игр, содержание 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. 63).

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

3. В блоке **Блокировать игры по содержанию** запретите запуск игр, которые не предназначены для выбранного пользователя по возрасту и / или по содержанию:

   a. Если вы хотите заблокировать запуск всех игр, содержание которых не соответствует возрасту пользователя, установите флажок **Блокировать игры по возрастному рейтингу** и выберите возрастное ограничение в раскрывающемся списке рядом с флажком.

   b. Если вы хотите заблокировать запуск игр с определенным содержанием, 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 содержания игр, которые нужно блокировать.

4. В окне **Родительский контроль** включите переключатель **Родительский контроль**, расположенный напротив учетной записи пользователя.

- *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. 63).

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

3. В нижней части окна по ссылке **Добавить программу в список** откройте окно **Открыть** и выберите исполняемый файл программы.

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

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

5. Если вы хотите установить ограничения на время использования программы, выберите в списке программу или категорию программ и по ссылке **Настроить правила** откройте окно **Ограничение использования программы**.

6. 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. Таблица отображается при нажатии на кнопку  .

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

8. Нажмите на кнопку **Сохранить**.

9. В окне **Родительский контроль** включите переключатель **Родительский контроль**, расположенный напротив учетной записи пользователя.

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 программах мгновенного обмена сообщениями 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. 63).

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 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 или программе мгновенного обмена сообщениями, 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 **История переписки**.

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

4. В окне **Родительский контроль** включите переключатель **Родительский контроль**, расположенный напротив учетной записи пользователя.

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

Контроль содержания переписки

С помощью Родительского контроля вы можете отслеживать и запрещать пользователю употребление в переписке указанных личных данных (например, фамилии, номера телефона, номера кредитной карты) и ключевых фраз (например, ненормативной лексики).

Чтобы настроить контроль пересылки личных данных, выполните следующие действия:

1. Перейдите в окно настройки параметров Родительского контроля (см. раздел «Переход к настройке параметров Родительского контроля» на стр. 63).
2. В окне настройки параметров Родительского контроля выберите раздел **Контроль содержания**.
3. В блоке **Контроль передачи личных данных** установите флажок **Запретить передачу личных данных третьим лицам**.
4. По ссылке **Редактировать перечень личных данных** откройте окно **Перечень личных данных**.
5. В нижней части окна нажмите на кнопку **Добавить**.

   Откроется окно добавления личных данных.
6. Выберите тип личных данных (например, «номер телефона»), по ссылке или введите описание в поле **Название поля**.
7. Укажите личные данные (например, фамилию, номер телефона) в поле **Значение**.
8. Нажмите на кнопку **Добавить**.

   Личные данные появятся в списке в окне **Перечень личных данных**.
9. В окне **Родительский контроль** включите переключатель **Родительский контроль**, расположенный напротив учетной записи пользователя.

Родительский контроль будет отслеживать и блокировать употребление указанных личных данных в переписке в программах мгновенного обмена сообщениями или через веб-сайты.

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. 63).
2. В окне настройки параметров Родительского контроля выберите раздел **Контроль содержания**.
3. В блоке **Контроль употребления ключевых слов** установите флажок **Включить контроль употребления ключевых слов**.
4. По ссылке **Редактировать перечень ключевых слов** откройте окно **Контроль употребления 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 **Контроль употребления ключевых слов**.
7. В окне **Родительский контроль** включите переключатель **Родительский контроль**, расположенный напротив учетной записи пользователя.

Родительский контроль будет блокировать передачу сообщений, содержащих указанную ключевую фразу, при переписке через интернет и программы мгновенного обмена сообщениями.

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. 63).

2. Выберите учетную запись пользователя и по ссылке **Просмотреть 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.

СОХРАНЕНИЕ РЕСУРСОВ ОПЕРАЦИОННОЙ СИСТЕМЫ ДЛЯ КОМПЬЮТЕРНЫХ ИГР

При одновременной работе Kaspersky Internet 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 Internet Security отвлекают от игры.

Чтобы не изменять параметры Kaspersky Internet 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 Internet 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. По ссылке **Настройка** в нижней части главного окна перейдите в раздел **Настройка**.
3. В левой части окна выберите раздел **Производительность**.

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

РАБОТА С НЕИЗВЕСТНЫМИ ПРОГРАММАМИ

С помощью Kaspersky Internet 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 Internet Security входят компоненты и инструменты, позволяющие проверить репутацию программы и контролировать активность программы на вашем компьютере.

В ЭТОМ РАЗДЕЛЕ

ПРОВЕРКА РЕПУТАЦИИ ПРОГРАММЫ

Kaspersky Internet 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).

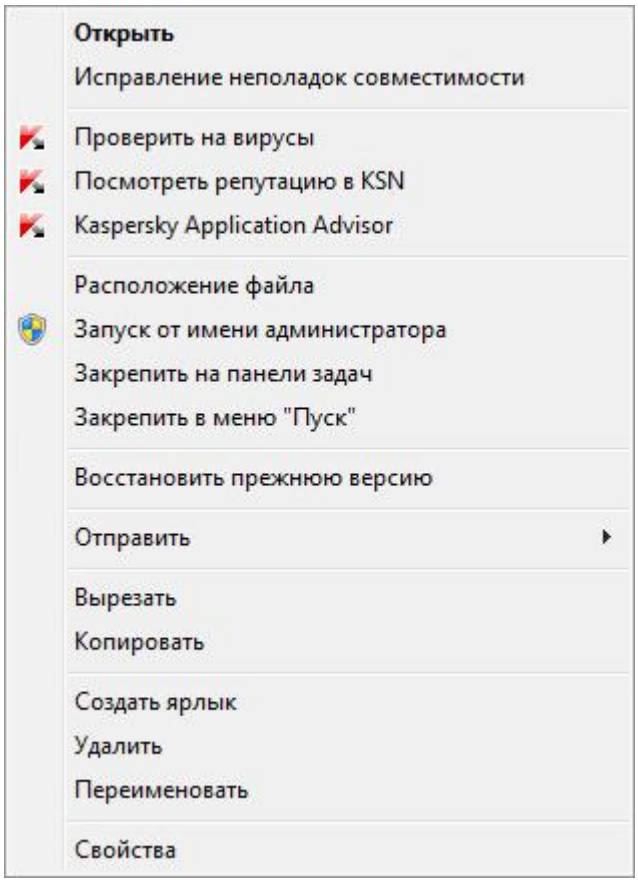

Рисунок 5. Контекстное меню объекта

Откроется окно со сведениями о репутации программы в KSN.

См. также

Участие в Kaspersky Security Network (KSN).....87

Контроль действий программы на компьютере и в сети

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 Internet Security будет применять для контроля активности этой программы.

Kaspersky Internet 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 Internet Security.
2. По ссылке **Показать дополнительные инструменты**, расположенной в нижней части главного окна, откройте окно **Инструменты**.
3. В окне **Инструменты** по ссылке **Контроль программ** откройте 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.

   Откроется окно **Правила программы**.
6. Задайте правила контроля программы:

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

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

     b. По правой клавише мыши в графе с возможным действием над ресурсом (**Чтение**, **Запись**, **Удаление** или **Создание**) откройте контекстное меню и выберите в нем нужное значение (**Разрешить**, **Запретить**, **Действие** или **Наследовать**).

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

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

     b. По правой клавише мыши в графе **Разрешение** откройте контекстное меню и выберите в нем нужное значение (**Разрешить**, **Запретить**, **Действие** или **Наследовать**).

   - 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 нового правила, переместив его вверх или вниз по списку с помощью кнопок **Вверх** и **Вниз**.

   - Чтобы исключить некоторые действия из проверки Контролем программ, на закладке **Исключения** установите флажки для действий, которые не нужно контролировать.
7. Нажмите на кнопку **Сохранить**.

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

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 Internet Security блокирует несанкционированный доступ программ к веб-камере и показывает уведомление о том, что доступ заблокирован. По умолчанию Kaspersky Internet 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. 76), 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 Internet 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 Internet 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. 75). 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 выбрать вариант **Не показывать это уведомление** или перейти к настройке отображения уведомлений (см. раздел «Настройка параметров доступа программ к веб-камере» на стр. 75).

Kaspersky Internet 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 веб-камеры имеет следующие особенности и ограничения:

- Программа контролирует видео и статические изображения, полученные в результате обработки данных веб-камеры.
- Программа Kaspersky Internet 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/10978.

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. По ссылке **Настройка** в нижней части главного окна откройте окно **Настройка**.
3. В разделе **Защита** в правой части окна выберите компонент **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 закладе **Защита** выключите **Доступ 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. По ссылке **Показать дополнительные инструменты**, расположенной в нижней части главного окна, откройте окно **Инструменты**.

3. В окне **Инструменты** по ссылке **Контроль программ** откройте 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 системы** → **Подозрительные изменения в системе** → **Доступ к веб-камере**.

8. По правой клавише мыши в графе **Разрешение** откройте контекстное меню и выберите пункт **Разрешить**.

9. Нажмите на кнопку **Сохранить**.

Доступ программы к веб-камере будет разрешен.

РЕЖИМ БЕЗОПАСНЫХ ПРОГРАММ

Этот раздел содержит информацию о режиме Безопасных программ.

В ЭТОМ РАЗДЕЛЕ

О РЕЖИМЕ БЕЗОПАСНЫХ ПРОГРАММ

Kaspersky Internet 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 Internet 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 Internet Security. Наличие в Kaspersky Internet 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 Internet 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. 36). После обновления баз и программных модулей могут быть изменены параметры запуска неизвестных программ и модулей.

Перед включением режима Безопасных программ Kaspersky Internet Security проводит анализ операционной системы и программ, установленных на вашем компьютере. Анализ может занимать длительное время (до нескольких часов). Если в результате анализа обнаружено программное обеспечение, которое не является доверенным, включать режим Безопасных программ не рекомендуется. После включения режима Безопасных программ Kaspersky Internet 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. 72), если вы работаете с ними, а затем включить режим Безопасных программ.

Kaspersky Internet Security может проводить анализ операционной системы и установленных программ автоматически в фоновом режиме. Если по результатам анализа Kaspersky Internet Security обнаружил, что на компьютере используются преимущественно доверенные программы, режим Безопасных программ может быть включен автоматически.

Включение режима Безопасных программ

Чтобы включить режим Безопасных программ, выполните следующие действия:

1. Откройте главное окно программы.

2. По ссылке **Показать дополнительные инструменты**, расположенной в нижней части главного окна, откройте окно **Инструменты**.

3. В окне **Инструменты** по ссылке **Контроль программ** откройте окно **Контроль программ**.

4. В блоке **Режим Безопасных программ выключен** в нижней части окна **Контроль программ** перейдите по ссылке **Включить**.

   Если необходимые компоненты защиты выключены, откроется окно, содержащее информацию о компонентах защиты, которые требуется включить для работы режима Безопасных программ.

5. Нажмите на кнопку **Продолжить**.

   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**.

   Дождитесь окончания анализа операционной системы и установленных программ. Вы можете свернуть окно **Анализ установленных программ**. При этом анализ будет выполняться в фоновом режиме. Информация о процессе выполнения анализа будет отображаться по ссылке **Анализ установленных программ (<N> %)** в окне **Контроль программ**.

6. Просмотрите информацию о результатах анализа в окне **Анализ установленных программ и исполняемых файлов завершен**.

   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 Internet Security считала их полностью безопасными.

   Вы можете просмотреть информацию о недоверенных системных файлах по ссылке **Перейти к списку неизвестных системных файлов**. Список недоверенных системных файлов отображается в окне **Неизвестные системные файлы**. Вы также можете отменить использование режима Безопасных программ, нажав на кнопку **Не включать режим Безопасных программ**.

7. Если вы хотите разрешить запуск недоверенных программ и системных файлов, в окне **Анализ установленных программ и исполняемых файлов завершен** перейдите по ссылке **Разрешить запуск неизвестных системных файлов и продолжить**.

8. Нажмите на кнопку **Включить режим Безопасных программ по умолчанию**.

Режим Безопасных программ будет включен. Kaspersky Internet Security будет блокировать запуск всех программ и системных файлов, не являющихся доверенными. Будет выполнен переход к окну **Контроль программ**.

После включения режима Безопасных программ и первой перезагрузки операционной системы запуск неизвестных программ разрешен до запуска Kaspersky Internet Security. После последующих перезагрузок операционной системы Kaspersky Internet Security блокирует запуск неизвестных программ.

Выключение режима Безопасных программ

Чтобы выключить режим Безопасных программ, выполните следующие действия:

1. Откройте главное окно программы.
2. По ссылке **Показать дополнительные инструменты**, расположенной в нижней части главного окна, откройте окно **Инструменты**.
3. В окне **Инструменты** по ссылке **Контроль программ** откройте окно **Контроль программ**.
4. В блоке **Режим безопасных программ включен** в нижней части окна перейдите по ссылке **Выключить**.

Режим Безопасных программ будет выключен.

ЗАЩИТА ДОСТУПА К УПРАВЛЕНИЮ KASPERSKY INTERNET 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 Internet 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 Internet Security с помощью пароля, выполните следующие действия:

1. Откройте главное окно программы.
2. По ссылке **Настройка** в нижней части главного окна перейдите в раздел **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 Internet 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 Internet 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 Internet Security использует эту информацию для защиты вашего компьютера от вредоносных действий, которые могли быть выполнены во время приостановки защиты или выключения Kaspersky Internet Security. Хранение информации о результатах контроля активности программ не ограничено по времени. Эта информация удаляется в случае удаления Kaspersky Internet Security с вашего компьютера.

Чтобы приостановить защиту компьютера, выполните следующие действия:

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

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

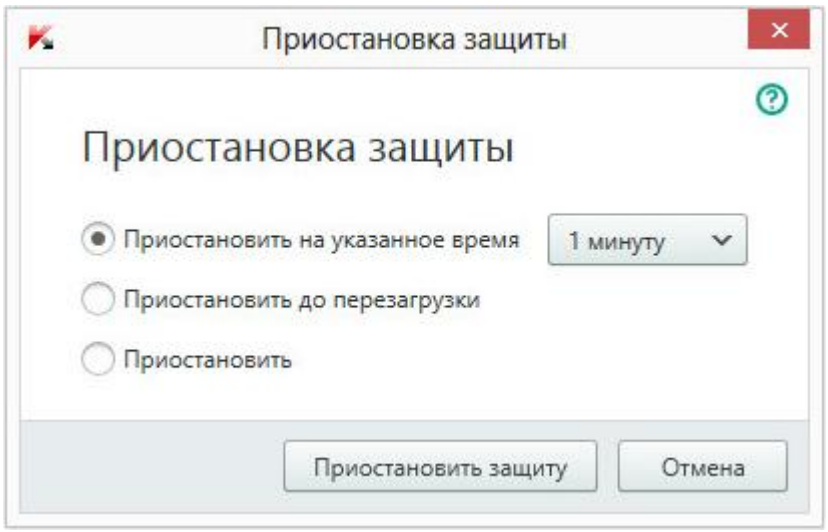

Рисунок 6. Окно Приостановка защиты

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

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

Чтобы возобновить защиту компьютера,

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

ВОССТАНОВЛЕНИЕ СТАНДАРТНЫХ ПАРАМЕТРОВ РАБОТЫ ПРОГРАММЫ

Вы в любое время можете восстановить параметры Kaspersky Internet 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*. При восстановлении рекомендуемого уровня безопасности вы можете выборочно сохранять значения ранее настроенных параметров для компонентов программы.

Чтобы запустить мастер настройки программы, выполните следующие действия:

1. Откройте главное окно программы.
2. В нижней части окна перейдите по ссылке **Настройка**.

   В окне отобразится раздел **Настройка**.
3. Выберите раздел **Общие**.

   В окне отобразятся параметры настройки Kaspersky Internet 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

В этом окне мастера представлены компоненты защиты Kaspersky Internet Security, параметры которых были изменены пользователем или накоплены Kaspersky Internet Security в результате обучения компонентов защиты Сетевой экран и Анти-Спам. Если для какого-либо компонента были сформированы уникальные параметры, они также будут представлены в окне (см. рис. ниже).

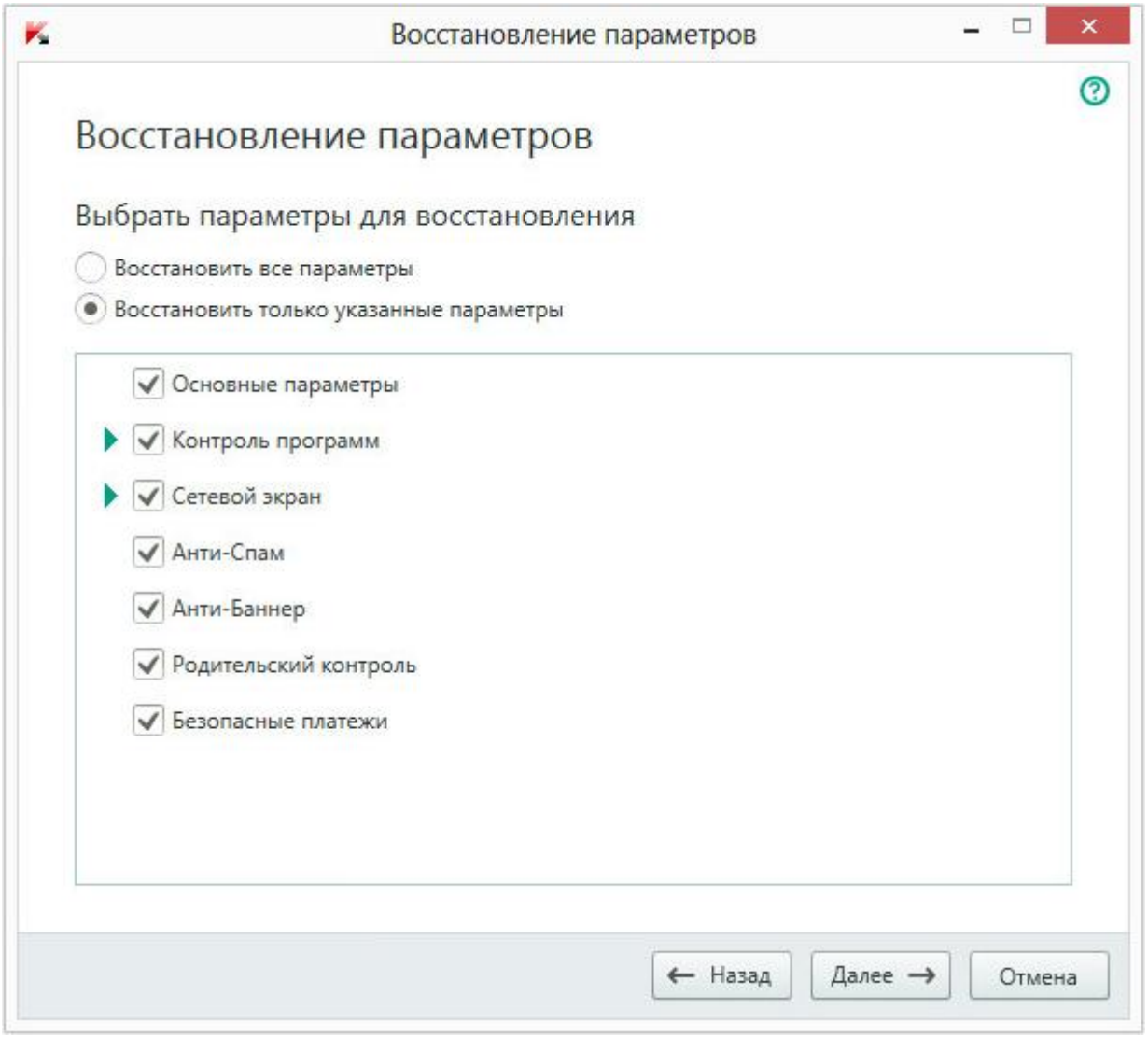

Рисунок 7. Окно Восстановление параметров

В число уникальных параметров входят списки разрешенных и запрещенных фраз и адресов, используемых Анти-Спамом, списки доверенных интернет-адресов и телефонных номеров интернет-провайдеров, правила исключений защиты для компонентов программы, правила фильтрации пакетов и программ Сетевого экрана.

Уникальные параметры формируются во время работы с Kaspersky Internet Security с учетом индивидуальных задач и требований безопасности. «Лаборатория Касперского» рекомендует сохранять уникальные параметры при восстановлении первоначальных параметров программы.

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

Шаг 3. Анализ операционной системы

На данном этапе выполняется поиск информации о программах, входящих в состав Microsoft Windows. Эти программы попадают в список доверенных программ, которые не имеют ограничений на действия, совершаемые в операционной системе.

По завершении анализа мастер автоматически переходит к следующему шагу.

Шаг 4. Завершение восстановления

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

ПРОСМОТР ОТЧЕТА О РАБОТЕ ПРОГРАММЫ

Kaspersky Internet 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 программа обновлялась, сколько обнаружено спам-сообщений и многое другое). Отчеты ведутся с использованием шифрования.

Чтобы просмотреть отчет о работе программы, выполните следующие действия:

1. Откройте главное окно программы.

2. По ссылке **Показать дополнительные инструменты**, расположенной в нижней части главного окна, откройте окно **Инструменты**.

3. В окне **Инструменты** по ссылке **Отчет** откройте 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 отчет** данные представлены в табличном виде. Для удобства просмотра отчетов вы можете выбирать различные варианты группировки записей.

ПРИМЕНЕНИЕ ПАРАМЕТРОВ ПРОГРАММЫ НА ДРУГОМ КОМПЬЮТЕРЕ

Настроив программу, вы можете применить параметры ее работы к программе Kaspersky Internet 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 Internet 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 носителе).
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. В нижней части окна по ссылке **Настройка** откройте 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 Internet Security, установленной на другом компьютере.
2. В нижней части окна по ссылке **Настройка** откройте 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 (KSN)

Чтобы повысить эффективность защиты вашего компьютера, Kaspersky Internet Security использует защиту из облака. Защита из облака реализуется с помощью инфраструктуры Kaspersky Security Network, использующей данные, полученных от пользователей во всем мире.

Kaspersky Security Network (KSN) – это инфраструктура онлайн-служб и сервисов, предоставляющая доступ к оперативной базе знаний «Лаборатории Касперского» о репутации файлов, интернет-ресурсов и программного обеспечения. Использование данных Kaspersky Security Network обеспечивает более высокую скорость реакции Kaspersky Internet 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 Internet Security (см. раздел «О предоставлении данных» на стр. 31).

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 во время установки Kaspersky Internet 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. По ссылке **Настройка** в нижней части главного окна откройте окно **Настройка**.
3. В разделе **Дополнительно** выберите блок **Обратная связь**.

   В окне отобразятся сведения о Kaspersky Security Network (KSN) и параметры участия в KSN.
4. Включите или выключите участие в Kaspersky Security Network по кнопкам **Включить** / **Выключить**:
   - если вы хотите участвовать в KSN, нажмите на кнопку **Включить**;
   - если вы не хотите участвовать в KSN, 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. По ссылке **Настройка** в нижней части главного окна откройте окно **Настройка**.
3. В разделе **Дополнительно** выберите подраздел **Обратная связь**.

В окне отобразится статус подключения к Kaspersky Security Network.

УЧАСТИЕ В ПРОГРАММЕ «ЗАЩИТИ ДРУГА»

Программа «Защити друга» позволяет опубликовать в Твиттере и на страницах в социальных сетях ссылку на загрузку установочного пакета Kaspersky Internet Security с увеличенным ознакомительным периодом. Если ваш друг в социальной сети или в Твиттере загрузит установочный пакет Kaspersky Internet Security по опубликованной вами ссылке и активирует программу, вам будут начислены бонусные баллы. Накопленные бонусные баллы вы можете обменять на бонусный код активации Kaspersky Internet Security.

Возможность участия в программе «Защити друга» может быть доступна не для всех пользователей.

Количество бонусных баллов зависит от версии программы.

Чтобы принять участие в программе «Защити друга», необходимо открыть веб-страницу вашего профиля в программе «Защити друга». Веб-страница вашего профиля доступна по ссылке **Личный кабинет** в нижней части главного окна Kaspersky Internet Security. Ваш профиль создается автоматически при первом входе.

Для входа в ваш профиль в программе «Защити друга» необходимо авторизоваться с помощью учетной записи My Kaspersky. Если у вас еще нет учетной записи My Kaspersky, вы можете создать ее при первом открытии вашего профиля в программе «Защити друга».

На веб-странице вашего профиля в программе «Защити друга» вы можете выполнять следующие действия:

- просматривать количество накопленных бонусных баллов;
- публиковать ссылки на загрузку установочного пакета Kaspersky Internet Security;
- изменять свойства вашего профиля (изображение и имя, которые будут публиковаться в Твиттере, социальных сетях и блоге вместе со ссылкой на загрузку установочного пакета Kaspersky Internet Security).

При переходе с Kaspersky Internet Security к использованию Kaspersky Total Security вы можете продолжить участвовать в программе «Защити друга». В этом случае вы предлагаете друзьям ссылку на загрузку установочного пакета Kaspersky Internet Security. При переходе к использованию Kaspersky Total Security история участия в программе «Защити друга» и накопленные баллы сохраняются, и вы можете обменять накопленные баллы на бонусный код активации Kaspersky Internet Security. При повторной установке Kaspersky Total Security или переходе на более новую версию Kaspersky Total Security участие в программе «Защити друга» прекращается.

В ЭТОМ РАЗДЕЛЕ

Вход в ваш профиль в программе «Защити друга»

Для входа в ваш профиль в программе «Защити друга» нужно авторизоваться с помощью учетной записи My Kaspersky. Если у вас еще нет учетной записи My Kaspersky, при первом входе на веб-страницу программы «Защити друга» вам нужно создать учетную запись My Kaspersky.

Учетная запись My Kaspersky представляет собой адрес вашей электронной почты и пароль (не менее восьми символов), которые вы указали при регистрации.

После создания учетной записи на указанный вами адрес электронной почты будет прислано письмо, содержащее ссылку для активации вашей учетной записи My Kaspersky.

После активации вы можете использовать вашу учетную запись My Kaspersky для входа на страницу вашего профиля в программе «Защити друга».

- *Чтобы создать учетную запись My Kaspersky, выполните следующие действия:*

1. Откройте главное окно программы и в нижней части окна перейдите по ссылке **Личный кабинет**.

   Откроется веб-страница программы «Защити друга», содержащая поля для регистрации или авторизации с помощью учетной записи My Kaspersky.

2. Создайте и активируйте учетную запись My Kaspersky:

   a. В левой части веб-страницы введите адрес электронной почты в поле **E-mail**.

   b. Введите пароль и подтверждение пароля в поля **Пароль** и **Подтверждение пароля**. Пароль должен содержать не менее восьми символов.

   c. Нажмите на кнопку **Зарегистрироваться**.

      На веб-странице отобразится сообщение об успешной регистрации учетной записи My Kaspersky. На указанный вами адрес электронной почты будет отправлено письмо со ссылкой, по которой необходимо перейти для активации учетной записи My Kaspersky.

   d. Перейдите по ссылке для активации учетной записи My Kaspersky в полученном письме.

      На веб-странице отобразится сообщение об успешной активации учетной записи My Kaspersky. Вы можете использовать созданную учетную запись My Kaspersky для входа в ваш профиль в программе «Защити друга».

Если у вас уже есть учетная запись My Kaspersky, вы можете использовать ее для входа на страницу вашего профиля.

- *Чтобы войти на страницу профиля программы «Защити друга», выполните следующие действия:*

1. Откройте главное окно программы и в нижней части окна перейдите по ссылке **Личный кабинет**.

   Откроется веб-страница программы «Защити друга», содержащая поля для регистрации или авторизации с помощью учетной записи My Kaspersky.

2. В правой части веб-страницы введите в поля адрес электронной почты и пароль, указанные при регистрации учетной записи My Kaspersky.

3. Нажмите на кнопку **Войти**.

На веб-странице отобразится ваш профиль в программе «Защити друга».

Как поделиться ссылкой на Kaspersky Internet Security с друзьями

С веб-страницы своего профиля в программе «Защити друга» вы можете опубликовать ссылку на скачивание установочного пакета Kaspersky Internet Security в Твиттере, а также в социальных сетях. Кроме того, вы можете вставить на страницу своего веб-сайта или блога информацию о вашем профиле в программе «Защити друга» со ссылкой на установочный пакет. Также вы можете отправить ссылку на загрузку установочного пакета Kaspersky Internet Security по электронной почте или с помощью программ мгновенного обмена сообщениями (например, ICQ).

- *Чтобы опубликовать ссылку на загрузку установочного пакета Kaspersky Internet Security в Твиттере или социальных сетях, выполните следующие действия:*

1. Откройте главное окно Kaspersky Internet Security и перейдите по ссылке **Личный кабинет** в нижней части окна.

   Откроется веб-страница авторизации в программе «Защити друга».

2. Выполните авторизацию на веб-странице с помощью вашей учетной записи My Kaspersky.

   На веб-странице отобразится информация вашего профиля в программе «Защити друга».

3. В левой части веб-страницы нажмите на кнопку с логотипом нужной социальной сети (Facebook или ВКонтакте) или Твиттера.

Откроется веб-сайт выбранной социальной сети или Твиттер. В ленте новостей ваших друзей будет опубликована ссылка на загрузку установочного пакета Kaspersky Internet Security с продленным периодом бесплатного использования. При необходимости вы можете ввести дополнительный текст в форме публикации.

Если вход на вашу страницу в социальной сети или Твиттере не выполнен, откроется веб-страница авторизации.

- *Чтобы разместить на своем веб-сайте веб-виджет со ссылкой на загрузку установочного пакета Kaspersky Internet Security, выполните следующие действия:*

1. Откройте главное окно Kaspersky Internet Security и перейдите по ссылке **Личный кабинет** в нижней части окна.

   Откроется веб-страница авторизации в программе «Защити друга».

2. Выполните авторизацию на веб-странице с помощью вашей учетной записи My Kaspersky.

   На веб-странице отобразится информация вашего профиля в программе «Защити друга».

3. В верхней части веб-страницы в раскрывающемся списке **Поделиться** выберите элемент **Получить код веб-виджета**.

   Откроется окно **Код веб-виджета**, содержащее код веб-виджета для вставки на страницу вашего веб-сайта.

Вы можете скопировать код веб-виджета в буфер обмена и вставить его в html-код страницы вашего веб-сайта или блога.

- *Чтобы получить ссылку для скачивания установочного пакета Kaspersky Internet Security для пересылки по почте или с помощью программы мгновенного обмена сообщениями, выполните следующие действия:*

1. Откройте главное окно Kaspersky Internet Security и перейдите по ссылке **Личный кабинет** в нижней части окна.

   Откроется веб-страница авторизации в программе «Защити друга».

2. Выполните авторизацию на веб-странице с помощью вашей учетной записи My Kaspersky.

   На веб-странице отобразится информация вашего профиля в программе «Защити друга».

3. В левой части веб-страницы перейдите по ссылке **Получить ссылку**.

   Откроется окно **Ссылка на установочный пакет**, содержащее ссылку для загрузки установочного пакета Kaspersky Internet Security.

Вы можете скопировать ссылку в буфер обмена и отправить ее по почте или с помощью программ мгновенного обмена сообщениями.

Обмен баллов на бонусный код активации

При участии в программе «Защити друга» вы можете получить бонусный код активации Kaspersky Internet Security, накопив определенное количество бонусных баллов. Вам начисляются бонусные баллы, когда пользователи активируют Kaspersky Internet Security, если программа загружена по ссылке, которой вы поделились с ними из своего профиля.

Бонусные коды активации предоставляются в следующих случаях:

- при однократной активации пользователем, с которым вы поделились ссылкой, пробной версии Kaspersky Internet Security;

- при активации пользователем, с которым вы поделились ссылкой, программы Kaspersky Internet Security.

На веб-странице своего профиля вы можете просмотреть историю начисления бонусных баллов и информацию о бонусных кодах активации, которые вам предоставлены. Также предоставленный бонусный код активации будет отправлен на вашу электронную почту.

Бонусный код активации может быть указан в программе в качестве резервного кода активации.

Бонусный код активации может быть применен для активации программы на другом компьютере (например, вы можете подарить его другому пользователю).

Применение бонусного кода активации невозможно в следующих случаях:

- Программа используется по подписке. В этом случае вы можете применить бонусный код активации после окончания подписки. Также вы можете применить бонусный код активации на другом компьютере.

- В программе уже указан резервный код активации. В этом случае вы можете применить бонусный код активации по истечении срока действия лицензии.

- *Чтобы получить бонусный код активации и активировать программу с помощью него, выполните следующие действия:*

1. Откройте главное окно Kaspersky Internet Security и перейдите по ссылке **Личный кабинет** в нижней части окна.

   Откроется веб-страница вашего профиля в программе «Защити друга».

2. Выполните авторизацию на веб-странице с помощью вашей учетной записи My Kaspersky.

   На веб-странице отобразится информация вашего профиля в программе «Защити друга».

Вы можете просмотреть информацию о начисленных вам бонусных баллах в блоке **Мои бонусные баллы**. Если количества накопленных вами бонусных баллов достаточно для получения бонусного кода активации, рядом с кнопкой **Получить бонусный код активации** в правой части веб-страницы отображается уведомление 1.

3. Чтобы получить бонусный код активации и активировать программу с помощью него, выполните следующие действия:

   a. Нажмите на кнопку **Получить бонусный код активации**.

      Дождитесь получения кода активации. Полученный бонусный код активации отобразится в открывшемся окне.

   b. Нажмите на кнопку **Активировать**.

Откроется окно **Активация** с сообщением о проверке кода активации. После проверки кода активации откроется окно с сообщением об успешной активации Kaspersky Internet Security.

Чтобы просмотреть историю предоставления бонусных кодов активации и активировать программу с помощью бонусного кода активации, предоставленного ранее, выполните следующие действия:

1. Откройте главное окно Kaspersky Internet Security и перейдите по ссылке **Личный кабинет** в нижней части окна.

   Откроется веб-страница вашего профиля в программе «Защити друга».

2. Выполните авторизацию на веб-странице с помощью вашей учетной записи My Kaspersky.

   На веб-странице отобразится информация вашего профиля в программе «Защити друга».

3. В нижней части веб-страницы перейдите по ссылке **Бонусные коды активации**.

   Откроется окно **Бонусные баллы** на закладке **Бонусные коды активации**.

4. В списке полученных бонусных кодов активации нажмите на код активации, с помощью которого вы хотите активировать программу.

   Откроется окно, содержащее бонусный код активации.

5. Нажмите на кнопку **Активировать**.

Откроется окно **Активация** с сообщением о проверке кода активации. После проверки кода активации откроется окно с сообщением об успешной активации Kaspersky Internet Security.

РАБОТА С ПРОГРАММОЙ ИЗ КОМАНДНОЙ СТРОКИ

Вы можете работать с Kaspersky Internet 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 Internet 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 получения технической поддержки и о том, какие условия требуются для получения помощи от Службы 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 (см. раздел «Источники информации о программе» на стр. 11), 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

Если возникла неотложная проблема, вы можете позвонить специалистам русскоязычной или международной технической поддержки http://support.kaspersky.ru/support/contacts.

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

Получение технической поддержки на портале My Kaspersky

My Kaspersky (https://my.kaspersky.ru) – это сервис, предназначенный для отправки запросов в Службу технической поддержки и для управления кодами активации программ «Лаборатории Касперского».

Для доступа к порталу My Kaspersky вам требуется зарегистрироваться на странице регистрации (https://my.kaspersky.com/ru/). Вам нужно указать адрес электронной почты и пароль для доступа к порталу My Kaspersky.

На портале My Kaspersky вы можете выполнять следующие действия:

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

Электронный запрос в Службу технической поддержки

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

В полях формы электронного запроса вам нужно указать следующие сведения:

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

Специалист Службы технической поддержки направляет ответ на ваш вопрос через портал My Kaspersky и по адресу электронной почты, который вы указали в электронном запросе.

Электронный запрос в Вирусную лабораторию

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

Вы можете отправлять в Вирусную лабораторию запросы на исследование подозрительных файлов или веб-ресурсов. Вы также можете обращаться туда в случаях ложных срабатываний Kaspersky Internet Security на файлы или веб-ресурсы, которые вы не считаете опасными.

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. По ссылке **Поддержка** в нижней части окна откройте окно **Поддержка**.
3. В открывшемся окне перейдите по ссылке **Мониторинг проблем**.

   Откроется окно **Мониторинг проблем**.
4. В открывшемся окне перейдите по ссылке **Создать отчет об операционной системе**.

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

Чтобы просмотреть отчет, выполните следующие действия:

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

   Откроется окно **Мониторинг проблем**.
4. В открывшемся окне перейдите по ссылке **Просмотреть отчет**.

   Откроется окно Проводника Microsoft Windows.
5. В открывшемся окне откройте архив sysinfo.zip, содержащий файлы отчета.

Отправка файлов данных

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

Чтобы загрузить файлы на сервер Службы технической поддержки, вам понадобится номер запроса. 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. По ссылке **Поддержка** в нижней части окна откройте окно **Поддержка**.
3. В открывшемся окне перейдите по ссылке **Мониторинг проблем**.

   Откроется окно **Мониторинг проблем**.
4. В открывшемся окне перейдите по ссылке **Отправить отчет в Службу технической поддержки**.

   Откроется окно **Отправка отчета**.
5. Установите флажки рядом с теми данными, которые вы хотите отправить в Службу технической поддержки.
6. Нажмите на кнопку **Отправить отчет**.

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

Если связаться со Службой технической поддержки по какой-либо причине невозможно, вы можете сохранить файлы данных на вашем компьютере и впоследствии отправить их с портала My Kaspersky.

Чтобы сохранить файлы данных на диске, выполните следующие действия:

1. Откройте главное окно программы.
2. По ссылке **Поддержка** в нижней части окна откройте окно **Поддержка**.
3. В открывшемся окне перейдите по ссылке **Мониторинг проблем**.
4. Откроется окно **Мониторинг проблем**.
5. В открывшемся окне перейдите по ссылке **Отправить отчет в Службу технической поддержки**.

   Откроется окно **Отправка отчета**.

6. Выберите типы данных, которые вы хотите отправлять:

   - **Информация об операционной системе**. Установите этот флажок, если вы хотите отправить в Службу технической поддержки информацию об операционной системе вашего компьютера.

   - **Собранные для анализа данные**. Установите этот флажок, если вы хотите отправить в Службу технической поддержки файлы трассировки программы. По ссылке **<количество> файлов>, <объем данных>** откройте окно **Собранные для анализа данные**. Установите флажки напротив тех файлов трассировки, которые вы хотите отправлять.

7. Перейдите по ссылке **Сохранить отчет**.

   Откроется окно для сохранения архива.

8. 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 течение всего времени использования программы и безвозвратно удаляются при удалении программы.

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.enc1`.

Все файлы трассировки содержат следующие общие данные:

- Время события.
- Номер потока выполнения.
- Компонент программы, в результате работы которого произошло событие.
- Степень важности события (информационное, предупреждение, критическое, ошибка).
- Описание события выполнения команды компонента программы и результата выполнения этой команды.

Содержание файлов трассировки SRV.log, GUI.log и ALL.log

В файлы трассировки SRV.log и GUI.log может записываться следующая информация:

- Личные данные, в том числе фамилия, имя и отчество, если эти данные являются частью пути к файлам на локальном компьютере.
- Имя пользователя и пароль, если они передавались в открытом виде. Эти данные могут записываться в файлы трассировки при проверке интернет-трафика. Трафик записывается в файлы трассировки только из trafmon2.ppl.
- Имя пользователя и пароль, файлы cookie, если они содержатся в заголовках протокола HTTP.
- Имя учетной записи для входа в Microsoft Windows, если имя учетной записи является частью имени файла.
- Адрес вашей электронной почты или веб-адрес с именем учетной записи и паролем, если они содержатся в имени обнаруженного объекта.

- Веб-сайты, которые вы посещаете, а также ссылки с этих веб-сайтов. Эти данные записываются в файлы трассировки, когда программа проверяет веб-сайты.

- Адрес прокси-сервера, имя компьютера, порт, IP-адрес, имя пользователя, используемое при авторизации на прокси-сервере. Эти данные записываются в файлы трассировки, если программа использует прокси-сервер.

- Внешние IP-адреса, с которыми было установлено соединение с вашего компьютера.

- Тема сообщения, идентификатор, имя отправителя и адрес веб-страницы отправителя сообщения в социальной сети. Эти данные записываются в файлы трассировки, если включен компонент Родительский контроль.

- Информация об активации программы, которая может включать текущий и предыдущий коды активации, локализацию программы, идентификаторы программы, продукта, кастомизации, версию программы, уникальный идентификатор, который генерируется для каждой уникальной инсталляции операционной системы, идентификатор компьютера пользователя, дату и время на компьютере пользователя в момент активации в UTC.

Содержание файлов трассировки HST.log, BL.log, Dumpwriter.log

Файл трассировки HST содержит информацию об обновлении баз и программных модулей.

Файл трассировки BL содержит информацию о событиях, возникающих во время работы программы, а также данные, необходимые для устранения неполадок в работе программы. Этот файл создается, если программа запускается с параметром avp.exe –bl. Также файл BL может содержать информацию об активации программы, которая может включать текущий и предыдущий коды активации, локализацию программы, идентификаторы программы, продукта, кастомизации, версию программы, уникальный идентификатор, который генерируется для каждой уникальной инсталляции операционной системы, идентификатор компьютера пользователя, дату и время на компьютере пользователя в момент активации в UTC.

Файл трассировки dumpwriter.log содержит служебную информацию, необходимую для устранения неполадок, возникающих при записи дампа памяти программы.

Содержание файлов трассировки плагинов программы

Файлы трассировки плагинов программы содержат следующую информацию:

- VirtualKeyboard (VKB.log) содержит служебную информацию о работе плагина и данные, необходимые для устранения неполадок в работе плагина.

- Online Banking (OB.log) содержит служебную информацию о работе плагина, в том числе информацию о событиях проверки веб-сайтов и результатах этой проверки, соединении с удаленными IP-адресами и параметрах прокси-сервера, файлы cookie. Также файл содержит данные, необходимые для устранения неполадок в работе плагина.

- ContentBlocker (CB.log) содержит служебную информацию о работе плагина, в том числе информацию о событиях проверки веб-адресов, результатах проверки, соединении с удаленными IP-адресами, параметрах прокси-сервера. Также файл содержит данные, необходимые для устранения неполадок в работе плагина.

- Office Anti-Virus (OA.log) содержит информацию о проверке документов Microsoft Office. Также этот файл может содержать информацию о полном пути к документу или адресу веб-сайта, с которого этот документ был загружен.

- Файл трассировки плагина запуска задачи проверки из контекстного меню (shellex.dll.log). Содержит информацию о выполнении задачи проверки и данные, необходимые для устранения неполадок в работе плагина.

- Файлы трассировки плагина для Microsoft Outlook®:
  - mcouas.OUTLOOK.EXE. Плагин Анти-Спама;
  - mcou.OUTLOOK.EXE. Плагин Почтового Антивируса.

  Файлы могут содержать части почтовых сообщений, в том числе адреса.
- Файл трассировки плагина для регистрации расширения Google Chrome (NativeMessagingHost.log) содержит служебную информацию о работе плагина.

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. По ссылке **Поддержка** в нижней части окна откройте окно **Поддержка**.
3. В открывшемся окне перейдите по ссылке **Мониторинг проблем**.

   Откроется окно **Мониторинг проблем**.
4. В открывшемся окне перейдите по ссылке **Выполнить скрипт**.

   Откроется 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 Internet Security имеет ряд некритичных для работы программы ограничений.

Ограничения при обновлении предыдущей версии программы

- При обновлении предыдущей версии Kaspersky Internet Security следующие параметры программы заменяются параметрами по умолчанию: источники обновлений, список доверенных веб-адресов, параметры Модуля проверки ссылок.

- При установке новой версии Kaspersky Internet Security поверх версии Kaspersky Internet Security 2011 и ниже 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 программы с версии Kaspersky Internet Security 2012 возможно выполнить преобразование резервных копий файлов и объектов, находящихся на карантине, в новый формат. Хранилище резервных копий в формате Kaspersky Internet Security 2013 и позднее поддерживается и не требует преобразования в новый формат.

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 Internet Security или отключении компонента Мониторинг активности.

- В случае нештатного завершения работы Kaspersky Internet 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**.

Предупреждение о сборе диагностической информации

Диагностическая информация о работе программы, которую вы собираете для Службы технической поддержки, в процессе сбора шифруется. При необходимости шифрование можно выключить.

Ограничения функциональности Защищенные соединения

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. Интернет-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.

Предупреждение о работе компонента Анти-Спам

Функциональность компонента защиты Анти-Спам может быть изменена в результате редактирования файла настройки компонента Анти-Спам.

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 Internet 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 Internet 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 Password Manager 2.0.
- Kaspersky Password Manager 5.0.
- Kaspersky Password Manager 7.0.

Особенности обработки вредоносных объектов компонентами программы

Программа по умолчанию может удалять 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 Endpoint

Работа следующих компонентов Kaspersky Internet Security ограничивается в Защищенном браузере, если программа установлена совместно с Kaspersky Fraud Prevention for Endpoint:

- Веб-Антивирус, кроме Анти-Фишинга;
- Родительский контроль;
- Модуль проверки ссылок;
- Анти-Баннер.

Ограничения работы Kaspersky Internet Security на Microsoft Windows 10

Если вы установили программу на операционную систему Microsoft Windows 10, становится недоступной следующая функциональность:

- Защита от снятия снимков экрана.
- Защита данных буфера обмена.
- Защита доступа к веб-камере.
- Лечение активного заражения.

Также при установке программы на операционную систему Microsoft Windows 10 частично ограничивается следующая функциональность:

- Самозащита. Не работает самозащита графического интерфейса программы, даже если она включена.
- Мониторинг активности.
- Защита от программ-крипторов и программ блокировки экрана. Программа может обнаруживать только самые простые программы-крипторы и программы блокировки экрана.
- Контроль программ. Не работают правила программ, созданные пользователем. Категоризация программ в стиле нового интерфейса Windows выполняется некорректно.

ГЛОССАРИЙ

К

Kaspersky Security Network (KSN)

Инфраструктура онлайн-служб и сервисов, предоставляющая доступ к оперативной базе знаний «Лаборатории Касперского» о репутации файлов, веб-ресурсов и программного обеспечения. Использование данных Kaspersky Security Network обеспечивает более высокую скорость реакции программ «Лаборатории Касперского» на неизвестные 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.

Бонусные баллы

Баллы, которые «Лаборатория Касперского» предоставляет пользователям, участвующим в программе «Защити друга». Бонусные баллы предоставляются пользователю, если пользователь разместил ссылку на программу «Лаборатории Касперского» в социальных сетях или в почтовом сообщении и по этой ссылке его друг загрузил установочный пакет программы и активировал программу.

Бонусный код активации

Код активации Kaspersky Internet Security, который предоставляется пользователю в обмен на бонусные баллы.

В

Вирус

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

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 Internet 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 Internet Security может накладывать ограничения на действия этой программы в операционной системе.

В Kaspersky Internet 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 Internet 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 веб-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 Internet 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 Internet 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 Internet 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.

Профиль пользователя

Сводная информация об участии пользователя в программе «Защити друга». В профиле пользователя содержится количество набранных им бонусных баллов, ссылка на страницу загрузки Kaspersky Internet Security, а также предоставленные пользователю бонусные коды активации.

Р

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 электронных сообщений, 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).

ЗАО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

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

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

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

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

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

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

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

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

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

Веб-сайт «Лаборатории Касперского»:	http://www.kaspersky.ru
Вирусная энциклопедия:	http://www.securelist.com/ru/
Вирусная лаборатория:	newvirus@kaspersky.com (только для отправки возможно зараженных файлов в архивированном виде)
Веб-форум «Лаборатории Касперского»:	http://forum.kaspersky.com

ИНФОРМАЦИЯ О СТОРОННЕМ КОДЕ

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

УВЕДОМЛЕНИЯ О ТОВАРНЫХ ЗНАКАХ

Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.

Google, Google Chrome, YouTube – товарные знаки Google, Inc.

ICQ – товарный знак и / или знак обслуживания ICQ LLC.

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

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

Mail.ru – зарегистрированный товарный знак, правообладателем которого является ООО «Мэйл.Ру».

Mozilla и 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.

ПРЕДМЕТНЫЙ УКАЗАТЕЛЬ