kaspersky

Kaspersky Anti-Virus

Содержание

О программе Kaspersky Anti-Virus

Kaspersky Anti-Virus обеспечивает комплексную защиту от различных видов информационных угроз. Для решения задач комплексной защиты в составе Kaspersky Anti-Virus предусмотрены различные функции и компоненты защиты.

Защита компьютера

Каждый тип угроз обрабатывается отдельным компонентом защиты. Вы можете включать и выключать компоненты защиты, 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 Anti-Virus 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.

Ниже описана работа компонентов защиты в режиме работы Kaspersky Anti-Virus, рекомендованном специалистами "Лаборатории Касперского" (то есть при настройках 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 Anti-Virus 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 сайтах, если эти скрипты представляют угрозу безопасности компьютера. Веб-Антивирус также контролирует весь веб-трафик и блокирует доступ к опасным сайтам.

IM-Антивирус

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

Мониторинг активности

Компонент Мониторинг активности отменяет в операционной системе изменения, вызванные вредоносной и другой активностью программ.

Компонент защищает от вредоносных программ, в том числе от:

- эксплойтов;
- программ блокировки экрана;
- программ-шифровальщиков;
- программ-вымогателей, которые шифруют данные или блокируют доступ к файлам или системе, а затем требуют выкуп за восстановление файлов или доступа к этим файлам.

Не рекомендуется выключать этот компонент.

Защита от сетевых атак

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

Анти-Фишинг

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

Экранная клавиатура

Экранная клавиатура позволяет избежать перехвата данных, вводимых через аппаратную клавиатуру, и защищает персональные данные от перехвата посредством снятия снимков экрана.

My Kaspersky

Если на компьютере установлена программа Kaspersky Anti-Virus, вы можете управлять защитой этого компьютера удаленно на сайте My Kaspersky.

Безопасное подключение

Kaspersky Anti-Virus защищает ваши данные при подключении к небезопасным сетям Wi-Fi.

Что нового

В Kaspersky Anti-Virus появились следующие новые возможности и улучшения:

- Добавлена полнофункциональная поддержка следующих версий Windows:
  - Microsoft Windows 10 1803;
  - Microsoft Windows 10 1809;
  - Microsoft Windows 10 1903;
  - Microsoft Windows 10 1909;
  - Microsoft Windows 10 2004.
- Добавлена возможность передать в "Лабораторию Касперского" оценку программы.
- Улучшена работа Веб-Антивируса:
  - Добавлена возможность использовать хранилище сертификатов Windows при настройке обращений к https-ресурсам в браузере Mozilla Firefox.
  - При отключении службы базовой фильтрации (BFE) программа перезапускает ее, чтобы обеспечить непрерывную защиту.
- Службы программы, такие как Kaspersky Security Network, лицензирование и обновление, теперь работают по безопасному протоколу HTTPS.
- Улучшены настройки защиты от программ удаленного управления. Теперь вы можете разрешить доверенным программам удаленного управления изменять настройки программы.
- Добавлена возможность перехода к использованию программы Kaspersky Free после истечения срока действия лицензии на платную версию программы, а также при удалении платной программы пользователем (доступно не во всех регионах).
- Улучшен контроль создания паролей при регистрации на сайтах. Теперь программа контролирует надежность паролей на сайтах с одним полем для ввода пароля.
- Улучшена работа Почтового Антивируса. Добавлена возможность использовать хранилище сертификатов Windows при настройке обращений к HTTPS-ресурсам в почтовом клиенте Mozilla Thunderbird.
- Добавлена поддержка Яндекс.Браузера.

Аппаратные и программные требования

Общие требования:

- 1500 МБ свободного места на жестком диске.
- Процессор с поддержкой инструкций SSE2.
- Подключение к интернету (для установки и активации программы, использования Kaspersky Security Network, а также обновления баз и программных модулей).
- Microsoft Windows® Installer 4.5 или выше.
- Microsoft .NET Framework 4 или выше.

Требования для операционных систем Microsoft Windows 7 Starter (Service Pack 0 и выше), Microsoft Windows 7 Home Basic (Service Pack 0 и выше), Microsoft Windows 7 Home Premium (Service Pack 0 и выше), Microsoft Windows 7 Professional (Service Pack 0 и выше), Microsoft Windows 7 Ultimate (Service Pack 0 и выше), Microsoft Windows 8 (Service Pack 0 или выше), Microsoft Windows 8 Pro (Service Pack 0 или выше), Microsoft Windows 8 Enterprise (Service Pack 0 или выше), Microsoft Windows 8.1 (Service Pack 0 и Windows 8.1 Update), Microsoft Windows 8.1 Pro (Service Pack 0 и Windows 8.1 Update), Microsoft Windows 8.1 Enterprise (Service Pack 0 и Windows 8.1 Update), Microsoft Windows 10 Home (версии: 1507, 1511, 1607, 1703, 1709, 1803, 1809, 1903, 1909, 2004), Microsoft Windows 10 Enterprise (версии: 1507, 1511, 1607, 1703, 1709, 1803, 1809, 1903, 1909, 2004), Microsoft Windows 10 Pro (версии: 1507, 1511, 1607, 1703, 1709, 1803, 1809, 1903, 1909, 2004):

- 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).

Для работы Веб-Антивируса в операционной системе должна быть запущена служба Base Filtering Engine (служба базовой фильтрации).

Браузеры, которые поддерживают полнофункциональную работу программы:

- Microsoft Edge на базе Chromium 77.0.235.25.
- Mozilla™ Firefox™ версий 52.x – 65.x.
- Mozilla™ Firefox™ ESR 52.x, 60.5.
- Google Chrome™ версий 48.x – 68.x.
- Яндекс.Браузер 18.3.1 – 19.0.3 (есть ограничения).

Браузеры, которые поддерживают установку расширения Kaspersky Protection:

- Microsoft Edge на базе Chromium 77.0.235.25;
- Mozilla™ Firefox™ версий 52.x – 65.x;
- Mozilla™ Firefox™ ESR 52.x, 60.x;
- Google Chrome™ версий 48.x – 72.x.

Браузеры, которые поддерживают Экранную клавиатуру и Проверку защищенных соединений:

- Microsoft Edge на базе Chromium 77.0.235.25;
- Mozilla Firefox версий 52.x – 65.x;
- Mozilla Firefox ESR 52.x – 60.5;
- Google Chrome 48.x – 68.x.

Поддержка более новых версий браузеров возможна, если браузер поддерживает соответствующую технологию.

Kaspersky Anti-Virus поддерживает работу с браузерами Google Chrome и Mozilla Firefox как в 32-разрядной, так и в 64-разрядной операционной системе.

Требования для планшетных компьютеров:

- Microsoft Windows 8, Microsoft Windows 8.1, Microsoft Windows 10;
- 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 или выше.

Совместимость с другими программами "Лаборатории Касперского"

Программа Kaspersky Anti-Virus совместима со следующими программами "Лаборатории Касперского":

- Kaspersky Safe Kids 1.4, 1.5;
- Kaspersky Fraud Prevention for Endpoints 5.0, 6.0, 6.5;
- Kaspersky Password Manager 9.0, 9.1, 9.2;
- Kaspersky System Checker 1.2.1;
- Kaspersky Software Updater 2.1;
- Kaspersky Virus Removal Tool 2015;
- Kaspersky Secure Connection 1.0, 2.0, 3.0, 4.0.

Как установить программу

Kaspersky Anti-Virus 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 **Готово**. Для прекращения работы мастера на любом шаге установки следует закрыть окно мастера.

Количество и последовательность шагов мастера установки зависит от региона, в котором вы устанавливаете программу. Если вы устанавливаете программу на территории Европейского союза, мастер установки предложит вам принять дополнительные соглашения об обработке персональных данных.

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 Anti-Virus на ваш компьютер,

на установочном диске запустите файл с расширением exe.

Далее установка программы выполняется с помощью стандартного мастера установки.

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

Как установить программу с помощью файла autorun

Чтобы установить Kaspersky Anti-Virus с помощью файла autorun, выполните следующие действия:

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

   При нажатии на кнопку **Скачать и установить** в "Лабораторию Касперского" отправляется информация о версии вашей операционной системы.

2. Если скачать программу не удалось, по ссылке **Скачать с сайта и установить вручную** перейдите на веб-страницу и скачайте программу вручную.

Далее установка программы выполняется с помощью стандартного мастера установки.

Для установки Kaspersky Anti-Virus вы также можете самостоятельно скачать установочный пакет из интернета. При этом для некоторых языков локализации мастер установки отображает несколько дополнительных шагов установки.

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

Вместе с Kaspersky Anti-Virus устанавливается программа Kaspersky Secure Connection, предназначенная для включения безопасного соединения с помощью Virtual Private Network (VPN). Вы можете удалить Kaspersky Secure Connection независимо от программы Kaspersky Anti-Virus. Если в вашей стране запрещено использование VPN, программа Kaspersky Secure Connection не устанавливается.

Поиск более новой версии программы

Перед началом установки мастер проверяет наличие более актуальной версии Kaspersky Anti-Virus 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 Anti-Virus, он предложит вам скачать 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.

Начало установки программы

На этом шаге мастер установки предлагает вам установить программу.

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

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

Просмотр Лицензионного соглашения

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

На этом шаге мастер установки предлагает вам ознакомиться с Лицензионным соглашением, которое заключается между вами и "Лабораторией Касперского".

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

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

Если вы устанавливаете программу на территории Европейского союза, для продолжения установки программы вы также должны принять условия Политики конфиденциальности.

Положение о Kaspersky Security Network

На этом шаге мастер установки предлагает вам принять участие в программе Kaspersky Security Network. Участие в программе предусматривает отправку в АО "Лаборатория Касперского" информации об угрозах, обнаруженных на вашем компьютере, о запускаемых программах и о скачиваемых 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.

Если вы устанавливаете программу на территории Европейского союза, Положение о Kaspersky Security Network включает информацию об обработке персональных данных.

Установка программы

Для некоторых версий Kaspersky Anti-Virus, 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.

Проверки во время установки программы

Во время установки Kaspersky Anti-Virus производит ряд проверок. В результате этих проверок могут быть обнаружены следующие проблемы:

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

- наличие прав администратора у пользователя, выполняющего установку программы.

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

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

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

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

Установка Kaspersky Password Manager

Перед завершением установки Kaspersky Anti-Virus предложит вам установить также программу защиты паролей Kaspersky Password Manager. Установка Kaspersky Password Manager может продолжаться после завершения установки Kaspersky Anti-Virus, отдельного уведомления о завершении установки Kaspersky Password Manager не выводится.

Рекомендуемые настройки

На этом шаге вы можете просмотреть и изменить настройки Kaspersky Anti-Virus, которые специалисты "Лаборатории Касперского" рекомендуют включить до начала использования программы.

Чтобы изменить рекомендуемые настройки, выполните следующие действия:

1. Выберите, какие настройки вы хотите включить или выключить:

   - Оставьте установленным флажок **Удалять вредоносные утилиты, рекламные программы, программы автодозвона и подозрительные упаковщики**, если вы хотите, чтобы программа удаляла эти объекты.

   - Оставьте установленным флажок **Обнаруживать другие программы, которые могут быть использованы злоумышленниками для нанесения вреда компьютеру или данным пользователя**, если вы часто устанавливаете новые программы. Это поможет вам обнаруживать программы, которые могут быть использованы для нанесения вреда компьютеру или вашим данным.

   - Оставьте установленным флажок **Посмотреть обзор возможностей программы**, чтобы ознакомиться с новыми и основными возможностями программы.

   Если вы не хотите включать рекомендуемые "Лабораторией Касперского" настройки, снимите соответствующие флажки.

2. Нажмите на кнопку **Применить**.

Завершение установки

На этом шаге мастер информирует вас о завершении установки программы.

Нажмите на кнопку **Готово**.

Все необходимые компоненты программы будут запущены автоматически сразу после завершения установки.

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

Активация программы

При первом запуске Kaspersky Anti-Virus запускается мастер активации программы.

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

Вам предлагаются следующие варианты активации Kaspersky Anti-Virus:

- **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 Internet Security или Kaspersky Total Security, по завершении активации запустится процедура перехода на Kaspersky Internet Security 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 недоступна.

Для активации программы необходимо подключение к интернету.

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

В некоторых версиях программы для получения информации о текущей дате и времени из доверенного источника, во время первого запуска программы может потребоваться аутентификация на прокси-сервере.

Регистрация на My Kaspersky

Этот шаг доступен не во всех версиях Kaspersky Anti-Virus.

Пользователи, зарегистрированные на My Kaspersky, получают возможность отправлять запросы в Службу технической поддержки и Вирусную Лабораторию, удобно управлять кодами активации, а также получают оперативную информацию о новых программах и специальных предложениях "Лаборатории Касперского".

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

В некоторых случаях регистрация на My Kaspersky необходима для использования программы.

Завершение активации

Мастер информирует вас об успешном завершении активации Kaspersky Anti-Virus.

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

Установка программы из командной строки

Вы можете установить Kaspersky Anti-Virus с помощью командной строки.

Некоторые команды можно выполнить только под учетной записью администратора.

Синтаксис командной строки:

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

Подробная инструкция и перечень настроек установки приведены на сайте Службы технической поддержки.

Как подготовить программу к работе

Для полноценной поддержки браузеров программой Kaspersky Anti-Virus в браузерах должно быть установлено и включено расширение Kaspersky Protection. Kaspersky Anti-Virus с помощью расширения Kaspersky Protection внедряет в трафик скрипт. Программа использует этот скрипт для взаимодействия с веб-страницей. Программа защищает передаваемые скриптом данные с помощью цифровой подписи. Kaspersky Anti-Virus может внедрять скрипт без использования расширения Kaspersky Protection.

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

Установка расширения Kaspersky Protection в браузеры Microsoft Edge на базе Chromium, Mozilla Firefox и Google Chrome

Расширение Kaspersky Protection не устанавливается в браузеры Microsoft Edge на базе Chromium, Mozilla Firefox и Google Chrome автоматически. Если в браузере не установлено расширение Kaspersky Protection, то при запуске браузера программа предложит вам перейти на страницу загрузки расширения и установить Kaspersky Protection вручную.

Поддержка Яндекс.Браузера

При использовании Яндекс.Браузера работают следующие компоненты программы:

- Проверка ссылок;
- Веб-Антивирус;
- Анти-Фишинг.

Как обновить программу

Программа обновляется автоматически. При наличии действующей лицензии на использование Kaspersky Anti-Virus предыдущих версий вам не понадобится активировать программу: мастер установки автоматически получит информацию о лицензии на использование предыдущей версии Kaspersky Anti-Virus и применит ее во время установки новой версии Kaspersky Anti-Virus.

Также программа автоматически обновляется, если вы устанавливаете новую версию программы поверх старой.

Во время скачивания обновления программа сравнивает Лицензионное соглашение, Положение о Kaspersky Security Network и Положение об обработке данных для маркетинговых целей предыдущей и новой версий. Если соглашения или положения различаются, программа предложит вам заново прочитать и принять их.

Программа может быть обновлена, если на вашем компьютере установлены следующие версии Kaspersky Anti-Virus:

- Kaspersky Anti-Virus 2013;
- Kaspersky Anti-Virus 2014;
- Kaspersky Anti-Virus 2015;
- Kaspersky Anti-Virus 2016;
- Kaspersky Anti-Virus 2017;
- Kaspersky Anti-Virus 2018;
- Kaspersky Anti-Virus 2019.

Обновление более ранних версий программы не поддерживается.

Ограничения при обновлении предыдущей версии программы

После обновления предыдущей версии программы Kaspersky Anti-Virus запускается автоматически, даже если в сохраненных настройках автозапуск программы выключен. При последующих перезагрузках операционной системы Kaspersky Anti-Virus не запускается автоматически, если в сохраненных настройках автозапуск программы выключен.

При обновлении предыдущей версии Kaspersky Anti-Virus следующие настройки программы заменяются настройками по умолчанию:

- настройки отображения Kaspersky Anti-Virus;
- расписание проверки;
- участие в Kaspersky Security Network;
- уровень защиты Файлового Антивируса;
- уровень защиты Почтового Антивируса;
- источники обновлений;

- список доверенных веб-адресов;
- настройки Проверки ссылок.

При обновлении версий Kaspersky Anti-Virus 2013, 2014, 2015 до новой версии программы, применение старой лицензии возможно не во всех случаях. Это связано с особенностями лицензирования в этих версиях программы. Также при обновлении версий Kaspersky Anti-Virus 2013, 2014, 2015 до новой версии программы, в новой версии Kaspersky Anti-Virus будут использованы настройки программы по умолчанию.

Установка поверх других программ "Лаборатории Касперского"

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

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

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

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

Установка Kaspersky Anti-Virus поверх Kaspersky Security Cloud

Если вы устанавливаете Kaspersky Anti-Virus поверх Kaspersky Security Cloud, вы не можете использовать Kaspersky Anti-Virus по лицензии на Kaspersky Security Cloud. Вы можете использовать по этой лицензии программу Kaspersky Security Cloud на другом устройстве.

Настройки программы Kaspersky Security Cloud не сохраняются и не могут быть применены в Kaspersky Anti-Virus.

Переход с Kaspersky Anti-Virus к использованию других программ "Лаборатории Касперского"

Переход к использованию Kaspersky Internet Security

Kaspersky Anti-Virus позволяет перейти к использованию программы Kaspersky Internet Security без дополнительного скачивания и установки программного обеспечения.

Kaspersky Internet Security – это программа, предназначенная для комплексной защиты вашего компьютера.

По сравнению с Kaspersky Anti-Virus программа Kaspersky Internet Security обладает рядом дополнительных возможностей, которые реализуются с помощью следующих компонентов и функций:

- Контроль программ.
- Режим Безопасных программ.
- Родительский контроль.
- Сетевой экран.
- Безопасные платежи.
- Блокирование доступа к опасным сайтам.
- Менеджер программ.
- Мониторинг сети.
- Контроль доступа к веб-камере.
- Защита от сбора данных.
- Анти-Спам.
- Анти-Баннер.
- Защита ввода данных с аппаратной клавиатуры.

Вы можете временно перейти на пробную версию Kaspersky Internet Security, чтобы ознакомиться с ее возможностями, или приобрести лицензию и перейти к использованию Kaspersky Internet Security.

Переход к использованию Kaspersky Total Security

В некоторых регионах возможен переход с Kaspersky Anti-Virus на Kaspersky Total Security.

Kaspersky Total Security предоставляет те же возможности, что и Kaspersky Internet Security, а также ряд дополнительных функций:

- Резервное копирование.
- Виртуальные сейфы.

- Защита паролей.

Переход к использованию Kaspersky Total Security выполняется так же, как и переход к использованию Kaspersky Internet Security.

При использовании программы по подписке, а также при работе с программой в некоторых регионах временный переход на пробную версию Kaspersky Internet Security и Kaspersky Total Security не предусмотрен.

Переход к использованию Kaspersky Security Cloud

По истечении лицензии на Kaspersky Anti-Virus программа предложит вам приобрести подписку на Kaspersky Security Cloud.

Kaspersky Security Cloud – это решение, которое дает вам больше возможностей по защите от вирусов и других угроз компьютерной безопасности. Программа предоставляет вам персональные рекомендации о том, как лучше защитить себя и свою семью.

Kaspersky Security Cloud предоставляет такие дополнительные функции как:

- Контроль небезопасных настроек операционной системы.
- Контроль устройств в сети Wi-Fi.
- Новости безопасности.

По подписке Kaspersky Security Cloud вы сможете использовать бесплатно программу защиты детей Kaspersky Safe Kids и программу защиты паролей Kaspersky Password Manager.

Переход на Kaspersky Security Cloud доступен не во всех регионах.

Временное использование Kaspersky Internet Security

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

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

1. Откройте главное окно программы.

   В раскрывающемся списке **Больше функций** выберите элемент **Расширение защиты**.

2. В открывшемся окне нажмите на кнопку **Пробная версия**.

   Запустится мастер миграции.

3. Следуйте указаниям мастера.

При использовании программы по подписке, а также при работе с программой в некоторых регионах временный переход на пробную версию Kaspersky Internet Security не предусмотрен. В этих случаях элемент **Расширение защиты** в раскрывающемся списке **Больше функций** отсутствует.

При переходе к использованию Kaspersky Internet Security на территории Европейского союза программа предложит вам повторно просмотреть и принять Лицензионное соглашение, Положение о Kaspersky Security Network и Положение об обработке данных для маркетинговых целей.

Запрос на активацию пробной версии Kaspersky Internet Security

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

Начало расширения защиты

На этом шаге мастер выводит на экран сообщение о готовности к переходу на пробную версию Kaspersky Internet Security.

Для продолжения работы мастера нажмите на кнопку **Продолжить**.

Удаление несовместимых программ

На этом шаге мастер проверяет, нет ли на вашем компьютере программ, несовместимых с Kaspersky Internet Security. Если таких программ нет, мастер автоматически 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 Internet Security продолжается.

Переход к использованию пробной версии Kaspersky Internet Security

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

Перезапуск программы

На этом шаге перехода к пробной версии Kaspersky Internet Security требуется перезапустить программу.

Для этого нажмите на кнопку **Готово** в окне мастера.

Завершение активации

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

Анализ операционной системы

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

По завершении анализа мастер автоматически переходит к следующему шагу.

Завершение миграции

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

После истечения срока действия лицензии на пробную версию Kaspersky Internet Security повторный временный переход с Kaspersky Anti-Virus на пробную версию Kaspersky Internet Security недоступен.

Переход к постоянному использованию Kaspersky Internet Security

Если вы хотите перейти к постоянному использованию Kaspersky Internet Security, вам необходимо приобрести лицензию на использование Kaspersky Internet 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 **Больше функций** выберите элемент **Расширение защиты**.
3. По ссылке **Купить лицензию** перейдите на сайт интернет-магазина "Лаборатории Касперского" или компании-партнера, где вы можете приобрести лицензию для Kaspersky Internet Security.

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

Переход к использованию Kaspersky Free при истечении лицензии Kaspersky Anti-Virus

Когда срок действия лицензии Kaspersky Anti-Virus истекает, вы можете приобрести новую лицензию и продолжить пользоваться всеми возможностями программы. Также программа может предложить вам перейти к использованию Kaspersky Free, чтобы сохранить базовый уровень защиты вашего компьютера.

Переход к использованию Kaspersky Free может быть осуществлен автоматически по окончании срока действия лицензии Kaspersky Anti-Virus. После перехода программа уведомляет вас о нем и предлагает продлить лицензию или продолжить пользоваться бесплатной версией защиты.

Чтобы продлить лицензию или начать пользоваться Kaspersky Free, выполните одно из следующих действий:

- Чтобы продлить лицензию, нажмите на кнопку **Продлить лицензию**.

  При нажатии на эту кнопку вы будете перенаправлены в магазин.

- Чтобы начать пользоваться Kaspersky Free, закройте окно с сообщением об активации Kaspersky Free.

Переход к использованию Kaspersky Free при удалении пробной версии Kaspersky Anti-Virus

При удалении пробной версии Kaspersky Anti-Virus вы можете перейти к использованию Kaspersky Free, чтобы сохранить базовый уровень защиты.

Когда вы удаляете пробную версию Kaspersky Anti-Virus, программа предлагает вам приобрести лицензию и продолжить пользоваться всеми возможностями программы.

Чтобы продлить лицензию или перейти к использованию Kaspersky Free, выполните одно из следующих действий:

- Чтобы приобрести лицензию, нажмите на кнопку **Продлить лицензию**.

  При нажатии на эту кнопку вы будете перенаправлены в магазин.

- Чтобы начать переход к использованию Kaspersky Free, нажмите на кнопку **Нет, спасибо**.

  При нажатии на эту кнопку запустится мастер миграции на Kaspersky Free.

Начало перехода к использованию Kaspersky Free

На этом шаге мастер миграции выводит на экран предложение перейти к использованию Kaspersky Free и сохранить базовый уровень защиты вашего компьютера.

Чтобы перейти на Kaspersky Free, нажмите на кнопку **Перейти на Kaspersky Free**.

Подтверждение перехода на Kaspersky Free

На этом шаге мастер миграции выводит на экран предложение подтвердить переход к использованию Kaspersky Free или отказаться от него.

Выполните одно из следующих действий:

- Чтобы подтвердить переход, нажмите на кнопку **Перейти**.

  Мастер миграции перейдет к следующему шагу.

- Чтобы отказаться от перехода к использованию Kaspersky Free и прервать работу мастера миграции, нажмите кнопку **Отмена**.

  Мастер миграции завершит свою работу.

Поиск несовместимого программного обеспечения

На этом шаге мастер миграции проверяет, нет ли на вашем компьютере программ, несовместимых с Kaspersky Free. Если таких программ нет, мастер автоматически переходит к следующему шагу. Если на этом шаге вы закрываете окно мастера миграции, поиск несовместимых программ продолжается в фоновом режиме.

Если несовместимые программы найдены, мастер миграции выводит их список в окне и предлагает вам удалить их.

После удаления несовместимых программ мастер миграции переходит к следующему шагу.

Завершение перехода к использованию Kaspersky Free

На этом шаге мастер миграции сообщает вам о завершении перехода к использованию Kaspersky Free.

Чтобы запустить Kaspersky Free, нажмите на кнопку **Запустить**.

Как удалить программу

В результате удаления Kaspersky Anti-Virus компьютер и ваши персональные данные окажутся незащищенными.

Удаление Kaspersky Anti-Virus выполняется с помощью мастера установки.

Как удалить программу в операционной системе Windows 7

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

в меню **Пуск** выберите пункт **Все Программы** → **Kaspersky Anti-Virus** → **Удалить Kaspersky Anti-Virus**.

Как удалить программу в операционной системе Windows 8 и выше

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

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

Ввод пароля для удаления программы

Чтобы удалить Kaspersky Anti-Virus, требуется ввести пароль для доступа к настройкам 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.

Сохранение кода активации

Убедитесь, что ваш код активации Kaspersky Anti-Virus сохранен в My Kaspersky. Код активации понадобится, если вы будете устанавливать Kaspersky Anti-Virus на другой компьютер.

Если Kaspersky Anti-Virus не подключен к My Kaspersky, мастер установки предложит вам войти в My Kaspersky, после чего сохранит код активации в My Kaspersky.

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).

Вы можете сохранить следующие данные:

- **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.

  После удаления Kaspersky Anti-Virus с компьютера файлы на карантине недоступны. Для работы с этими файлами нужно установить Kaspersky Anti-Virus.

- **Настройки работы программы** – параметры работы программы, установленные во время ее настройки.

  Вы также можете экспортировать настройки 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.

Подтверждение удаления программы

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

Завершение удаления

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

После завершения удаления Kaspersky Anti-Virus вы можете указать причины удаления программы на сайте "Лаборатории Касперского". Для этого требуется перейти на сайт "Лаборатории Касперского" по кнопке **Заполнить форму**.

Эта функциональность может быть недоступна в некоторых регионах.

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

Лицензирование программы

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

О Лицензионном соглашении

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

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

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

О лицензии

Лицензия – это ограниченное по времени право на использование программы, предоставляемое вам на основании Лицензионного соглашения. С лицензией связан уникальный код активации вашего экземпляра Kaspersky Anti-Virus.

Лицензия включает в себя право на получение следующих видов услуг:

- Использование программы на одном или нескольких устройствах.

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

- Обращение в Службу технической поддержки "Лаборатории Касперского".

- Получение прочих услуг, предоставляемых вам "Лабораторией Касперского" или ее партнерами в течение срока действия лицензии.

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

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

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

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

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

Если вы не хотите возобновлять защиту вашего компьютера, вы можете удалить Kaspersky Anti-Virus.

О режиме ограниченной функциональности

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

Функции Kaspersky Anti-Virus в режиме ограниченной функциональности

Функциональность	Ограничения	Режим ограниченной функциональности
Файловый Антивирус		есть
Проверка на вирусы	Только запуск проверки вручную. Проверка по расписанию и настройка проверки недоступны.	есть
Проверка на уязвимости		нет
Обновление баз и программных модулей	Настройка недоступна.	есть
Защита от рекламных программ и программ-шпионов		есть
Веб-Антивирус	Работает без ограничений.	есть
Почтовый Антивирус	Работает без ограничений.	есть
IM-Антивирус	Работает без ограничений.	есть
Эвристический анализ	Работает без ограничений.	есть
Защита от руткитов		нет
Защита от эксплойтов		есть
Мониторинг активности		есть
Защита от фишинга		есть
Проверка репутации файлов и ссылок в Kaspersky Security Network		нет
Дополнительные средства защиты и управления		есть
Проверка ссылок		нет

Защита ввода данных		нет
Диск аварийного восстановления	Доступно скачивание через интерфейс программы.	есть
Защита паролем настроек программы		есть
Производительность	Доступна настройка производительности программы.	есть
Менеджер задач	Менеджер задач только отображает результаты проверки, нет возможности управлять проверкой или ее настройками.	есть
Игровой режим	Работает без ограничений.	есть
Угрозы и исключения	Работает без ограничений.	есть
Самозащита	Работает без ограничений.	есть
Карантин	Работает без ограничений.	есть
Уведомления	Можно настроить только получение рекламных сообщений от "Лаборатории Касперского".	есть
Настройка отображения программы	Работает без ограничений.	есть
My Kaspersky		есть
Восстановление после заражения		нет
Защита от сетевых атак		нет
My Kaspersky	Только просмотр и управление кодами активации	есть

О коде активации

Код активации – это код, который вы получаете, приобретая лицензию на использование Kaspersky Anti-Virus. 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 Anti-Virus, код активации указан в документации или на коробке, в которой находится установочный компакт-диск.
- Если вы приобрели Kaspersky Anti-Virus в интернет-магазине, код активации высылается по адресу электронной почты, указанному вами при заказе.

Отсчет срока действия лицензии начинается с даты активации программы. Если вы приобрели лицензию, допускающую использование Kaspersky Anti-Virus 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".

Как восстановить коды активации

Если вы потеряли ранее предоставленный вам код активации, вы можете найти его на My Kaspersky. Для этого вам нужно войти в свою учетную запись на My Kaspersky.

Чтобы восстановить коды активации, выполните следующие действия:

1. Откройте главное окно программы.
2. По ссылке **Лицензия** в главном окне программы перейдите в окно **Лицензирование**.
3. По ссылке **Восстановить мои коды активации** перейдите в окно **Подключение к My Kaspersky**.
4. Введите адрес электронной почты, который вы использовали при регистрации на My Kaspersky, и пароль.
5. Нажмите на кнопку **Войти**.

Будет выполнен переход на My Kaspersky в раздел **Лицензии**, где отображаются ваши коды активации.

О подписке

Подписка на Kaspersky Anti-Virus – это использование программы с выбранными настройками (дата окончания, количество защищаемых устройств). Подписку на Kaspersky Anti-Virus 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 сайте поставщика услуги.

Поставщики услуг могут предоставлять два типа подписки на использование Kaspersky Anti-Virus: 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 Anti-Virus после окончания ограниченной подписки необходимо самостоятельно продлить ее. Неограниченная подписка продлевается автоматически при условии своевременного внесения предоплаты поставщику услуг.

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

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

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

Если на момент регистрации подписки Kaspersky Anti-Virus уже используется по действующей лицензии, то после регистрации подписки Kaspersky Anti-Virus 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 Anti-Virus.

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.

Как приобрести лицензию

Вы можете приобрести лицензию или продлить срок ее действия. При приобретении лицензии вы получите код активации, с помощью которого нужно активировать программу.

Чтобы приобрести лицензию, выполните следующие действия:

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

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

Как активировать программу

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 Anti-Virus, появляющиеся в области уведомлений панели задач.

Чтобы активировать программу Kaspersky Anti-Virus, 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 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 Anti-Virus.

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

Как продлить срок действия лицензии

Вы можете продлить срок действия лицензии. Для этого вы можете указать резервный код активации, не дожидаясь истечения срока действия лицензии. По истечении срока действия лицензии программа Kaspersky Anti-Virus 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: осталось N дней**, 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 Anti-Virus отправит данные на сервер активации "Лаборатории Касперского" для проверки. После истечения срока действия лицензии сервер активации повторно проверит данные при первой попытке активировать программу с помощью резервного кода активации.
5. Нажмите на кнопку **Готово**.

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.

Предоставление информации

Этот раздел содержит информацию о том, какие данные вы предоставляете в "Лабораторию Касперского". Подраздел Сохранение данных в отчет о работе программы содержит данные, которые хранятся локально на вашем компьютере и не отправляются в "Лабораторию Касперского".

Предоставление данных в рамках Лицензионного соглашения за пределами территории Европейского союза

Этот раздел содержит информацию о том, какие данные передаются в "Лабораторию Касперского", если у вас установлена версия программы, не предназначенная для использования на территории Европейского союза.

Вы соглашаетесь в автоматическом режиме предоставлять указанную ниже информацию посредством установленного вами программного обеспечения (далее ПО), правообладателем которого является АО "Лаборатория Касперского" (далее "Лаборатория Касперского", Правообладатель), в "Лабораторию Касперского" **для повышения уровня оперативной защиты и формирования наиболее подходящих предложений информационного и рекламного характера, для улучшения качества работы ПО и своевременного выявления и исправления ошибок, связанных с механизмом установки, удаления и обновления ПО, для учета количества пользователей**:

- Информация о контрольных суммах обрабатываемых файлов (MD5 и SHA256), количестве запусков файла и его формат, идентификаторе версии настроек ПО, информация для определения репутации URL (URL, по которому запрашивается репутация, идентификатор протокола соединения и номер используемого порта), полная версия и тип используемого ПО, уникальный идентификатор установки ПО, информация о типах обнаруженных угроз, идентификатор обнаруженной угрозы в базе угроз, название угрозы согласно классификации Правообладателя, идентификатор задачи проверки, в которой обнаружена угроза, информация об используемых цифровых сертификатах и информация, необходимая для проверки их подлинности: контрольные суммы (SHA256) сертификата, которым подписан проверяемый объект, и открытого ключа сертификата; идентификатор типа аутентификации при подключении к сети Wi-Fi, контрольные суммы (SHA256), полученные с использованием уникального идентификатора компьютера, уникальный идентификатор установки ПО на компьютер, имя беспроводной сети и MAC-адрес точки доступа, список сетей Wi-Fi, доступных на момент предоставления данных, имя домена и контрольная сумма (SHA256) пути из URL-адреса службы предоставления доступа в интернет, значение настроек безопасности, точки доступа WPS (Wi-Fi Protected Setup). Данные о дополнительных технических характеристиках по применяемым технологиям обнаружения, признак подключения установленного ПО к My Kaspersky, список устройств, поддерживающих UPnP протокол (производитель, название, модель (если информация доступна), дата последнего подключения, контрольные суммы (MD5 и SHA256) MAC-адреса (BSSID) точки доступа, контрольные суммы (MD5 и SHA256) MAC-адреса (BSSID) точки доступа с модификатором, массив структур настроек WPS от точек доступа со включенной технологией (контрольная сумму имени устройства, номер модели, наименование модели, производителя), значение настроек DHCP (структура контрольных сумм (SHA256) с модификатором от IPv4-адресов и маски, полученной по DHCP после подключения к сети Wi-Fi, контрольные суммы Gateway Local IP, DHCP IP, DNS1 IP, DNS2 IP, маски подсети), значение настроек DHCP IPv6 (структура контрольных сумм (SHA256) с модификатором от IPv6-адресов и маски, полученной по DHCP после подключения к сети Wi-Fi, контрольные суммы Gateway Local IPv6, DHCP IPv6, DNS1 IPv6, DNS2 IPv6, маски подсети), список доступных сетей Wi-Fi (информация о 7 сетях с самым высоким качеством сигнала, типы аутентификации и шифрования).

- Информация о контрольных суммах (MD5 и SHA256) обрабатываемых файлов, их упаковщиках (если файлы были упакованы), исходных контейнерах файлов (если есть), размере контейнеров файлов, информация для определения репутации URL (URL, о котором запрашивается репутация, идентификатор протокола соединения и номер используемого порта), полная версия, идентификатор и тип используемого ПО, цифровой идентификатор сборки в Системе кастомизации сборок, имя проверяемого файла или архива, если файл упакован, полный путь к файлу (или архиву), не включающий само имя файла,

название угрозы согласно классификации Правообладателя, дополнительные технические характеристики по применяемым технологиям проверки, ответы службы FNew, отправленные Пользователю (массив посчитанных для файла контрольных сумм (MD5) паттернов, типы паттернов, версии баз и результата работы консолидатора), статус задач проверки, признак подключения установленного ПО к My Kaspersky, идентификатор, выдаваемый службой хранения паролей по факту успешной аутентификации Пользователя, список уникальных идентификаторов рекламных сообщений.

- Информация о компьютере (идентификатор, тип), используемом ПО и его настройках, разрядность, тип, редакция, версия, номер пакета обновления установленной на компьютере операционной системы (далее ОС), информация о несовместимом программном обеспечении, если Пользователь принял условия Положения о Kaspersky Security Network, уникальный идентификатор Пользователя в службах Правообладателя, тип, версия, идентификатор локализации установленного ПО в соответствии с международными стандартами для кодов языков ISO 639-1 и ISO 639-2, предыдущая языковая локализация, код алфавита языковой локализации установленного ПО в соответствии с международным стандартом ISO 15924, код страны в соответствии с международным стандартам ISO 3166-1 Alpha-2, код кастомизации ПО, идентификатор, соответствующий полному имени ПО, режим работы ПО, идентификаторы приложений, которые могут быть активированы на компьютере Пользователя, список программ, совместимых с текущим ПО, интегральное состояние защиты ПО, статус компонентов защиты, информация об используемой лицензии (состояние, тип лицензии (если ПО активировано), идентификатор действующей лицензии, срок действия, количество дней, прошедших с момента ввода лицензии в действие, количество дней до окончания срока действия лицензии, количество дней, прошедших с момента окончания срока действия лицензии, признак активации ПО с использованием Activation Service 1.0, ключ, если ПО активировано ключом старого формата или кодом активации от Activation Service 1.0, идентификатор последовательности используемых лицензий, номер заказа, для которого была выписана текущая лицензия, идентификатор позиции прайс-листа, на которую была выписана текущая лицензия, тип и версия Лицензионного соглашения, признак согласия Пользователя с условиями Лицензионного соглашения, время изменения факта принятия Лицензионного соглашения, тип и текущее состояние подписки, причина текущего состояния или изменения состояния подписки, дата окончания подписки, символьный идентификатор элемента пользовательского интерфейса ПО, в котором Пользователь принял решение о приобретении ПО, индексированный массив чисел и строк, используемый для передачи дополнительной информации поставщиком услуг, идентификатор информационной схемы, используемой поставщиком услуг, список игнорируемых проблем, признак изменения информации об использовании лицензии для ознакомительных целей, массив возможностей ПО. Также будет предоставляться информация о содержимом, контрольной сумме (SHA1) и типе сертификата, значение служебного параметра Службы редиректов, идентификаторы компьютера Пользователя (PCID, контрольная сумма от Machine ID, Windows SID, Windows crypto GUID), класс (модель) USB-устройства, производитель, название (если информация доступна), дата последнего подключения.

- Информация об установленном на компьютере аппаратном обеспечении: данные о производителе, модели и объеме жесткого диска (HDD), контрольная сумма серийного номера жесткого диска (HDD) или случайного числа, если серийный номер определить не удалось, объем физической и виртуальной памяти, производитель и объем оперативной памяти, производитель и модель материнской платы, производитель и название программы BIOS, модель и число ядер установленного процессора, производитель и модель видеокарты и объем видеопамяти, производитель и тип сетевого адаптера, его скорость передачи данных, производитель и название монитора, производитель и модель компьютера, производитель, модель и тип корпуса компьютера, признак наличия аккумуляторной батареи. Данные о подключенных к компьютеру устройствах: класс/модель устройства, производитель устройства и название, уникальный идентификатор, дата последнего подключения устройства к компьютеру. Информация об устройствах, поддерживающих UPnP протокол, название производителя, модель и имя устройства, дата последнего подключения. Данные о загрузке системы, размер свободной и используемой памяти, размер свободного места на диске.

- Сведения обо всех установленных программах, название и версию установленной программы, версии установленных обновлений, название издателя, дата и полный путь установки на компьютере, конфигурация (настройки) программ и браузеров.

- Имя компьютера в сети (локальное и доменное имена), региональные настройки ОС (данные о часовом поясе, раскладке клавиатуры по умолчанию, языке интерфейса), настройки UAC, настройки сетевого экрана ОС и признак его активности, настройки родительского контроля ОС, настройки Windows Update.

- Название и размещение любых файлов на компьютере.

- Общая информация об устройстве (сетевое имя, тип устройства, тип токена, признак необходимости возврата токена службой уведомлений, идентификатор, который выдается программному обеспечению службой идентификации устройств по факту успешной регистрации или аутентификации связки "пользователь+устройство" (сессионный токен), идентификатор устройства на My Kaspersky, предыдущий идентификатор ПО на My Kaspersky, одноразовый пароль для автоматического подключения ПО, содержимое списка проблем на My Kaspersky, информация о сработавшей записи (идентификатор, статус, тип), время добавления записи в базу, тип области, в котором произошло событие, содержимое раздела Рекомендации списка проблем на My Kaspersky.

- Агрегированная информация об активности Пользователя на компьютере, длительность взаимодействия Пользователя с компьютером, срок агрегирования информации, общее количество событий за этот срок, агрегированная информация о запущенных Пользователем процессах в системе, имя процесса, общее количество запусков процесса, общая длительность его работы, контрольная сумма (CRC64) имени учетной записи, от которой запущен процесс, полный путь к файлу процесса, информация о ПО, к которому относится процесс (название, описание, производитель и версия), общее количество показов окна ПО и общая длительность его отображения, статистические параметры названия окна, язык локализации названия и распределение слов в названии.

- Информация о посещенных сайтах, веб-адрес сайта, доменные части веб-адресов, которые Пользователь вводил в адресной строке браузера или которые открывал из поисковых систем.

- Информация об использовании пользовательского интерфейса ПО, время взаимодействия Пользователя с интерфейсом, идентификаторы использованных элементов управления и тип взаимодействия пользователя с интерфейсом.

- Значение фильтра TARGET задачи обновления, информацию о включении режима Device Guard, имя проверяемого файла, путь к нему и код шаблона пути, контрольные суммы (MD5 и SHA256) и размер файла и его упаковщика (если файл был упакован) в байтах, дата добавления записи в базу, информация о сработавшей записи в базе, в случае обнаружения угрозы, категория и код ошибки, состояние антивирусных баз и процедуры обновления ПО, уникальный идентификатор запуска задачи обновления, статус задачи обновления антивирусных баз, полная версия ПО, на которое осуществляется обновление, идентификаторы программ сторонних производителей, которые были предложены для установки, выбраны Пользователем для установки и которые были установлены вместе с ПО, идентификатор сообщения, которое ПО отправляет на My Kaspersky.

- Информация о дате установки и активации ПО на компьютере, длительность задачи установки ПО, идентификатор задачи установки, тип установки ПО на компьютере (первичная установка, обновление и т.д.), признак успешности установки или номер ошибки установки, информация о приобретенных кодах активации, коде активации, которым ПО активировано на данный момент, предыдущий код активации, уникальный идентификатор Пользователя (Kaspersky User ID), тип учетной записи Пользователя, информация о привязке кода активации к Пользователю (уникальный идентификатор Пользователя на My Kaspersky, код активации, тип владения лицензией, подпись KPC Infra), номер обновления, тикет, полученный от службы активации, заголовок тикета, код партнера, для которого была разработана кастомизация, символьный код, подтверждающий, что ПО разработано для определенного партнера; канал продаж, идентификатор, полное название или имя и страна партнера, у которого приобретена лицензия, номер заказа, используемый партнером, признак участия Пользователя в KSN.

- Идентификатор установки ПО на компьютере, полная версия установленного ПО, идентификатор типа ПО, уникальный идентификатор компьютера, на котором установлено ПО.

- Идентификатор компонента и идентификатор сценария, запросившего репутацию файла или URL-адреса.

- Идентификатор пользователя веб-сайта партнера, загрузившего дистрибутив ПО, идентификатор товарной позиции.

В целях улучшения качества защиты Пользователя при проведении платежных операций в интернете вы соглашаетесь в автоматическом режиме предоставить финансовому сайту информацию о наименовании и версии ПО и настройке кастомизации ПО, идентификатор состояния плагина ПО в используемом для обращения к финансовому сайту браузере, идентификатор использования безопасного или обычного браузера.

Передаваемая информация не содержит персональных данных и иной конфиденциальной информации Пользователя и служит для обеспечения работы ПО Правообладателя, если не указано иное.

Полученная информация защищается Правообладателем в соответствии с установленными законом требованиями и требуется для обеспечения работы лицензированного вами ПО.

"Лаборатория Касперского" может использовать полученные статистические данные, созданные на основе полученной информации, для мониторинга тенденций в области угроз компьютерной безопасности и публикации отчетов о них.

Предоставление данных в рамках Лицензионного соглашения на территории Европейского союза

Этот раздел содержит информацию о том, какие данные передаются в "Лабораторию Касперского", если у вас установлена версия программы, предназначенная для использования на территории Европейского союза. **Приведенная в этом разделе информация не содержит персональных данных Пользователя и служит для обеспечения работы ПО Правообладателя, если не указано иное**.

Для повышения уровня оперативной защиты, для улучшения качества работы ПО и своевременного выявления и исправления ошибок, связанных с механизмом установки, удаления и обновления ПО, а также для учета количества пользователей, вы соглашаетесь в автоматическом режиме при использовании ПО передавать следующие данные в "Лабораторию Касперского":

- статус установки / удаления ПО (успешная или с ошибкой), код ошибки установки;
- идентификатор ПО;
- идентификатор сборки;
- идентификатор товарной позиции;
- локализация ПО;
- код ребрендинга;
- срок действия лицензии;
- тип платформы и производитель ОС (Windows, iOS, Android), версия ОС, номер сборки ОС, номер обновления ОС, редакция ОС, расширенная информация о редакции ОС, тип ОС (сервер, рабочая станция, контроллер домена), разрядность ОС, дополнительная информация об ОС;
- тип устройства (ноутбук, десктоп, планшет);
- тип установки (новая установка или обновление), время, затраченное на установку ПО в секундах, факт прерывания установки пользователем;
- тип и версия ПО;

- статус лицензии, по которой используется ПО;
- информация об обновлении баз и программных модулей, статус задачи обновления баз и программных модулей;
- режим работы ПО;
- информация о статусе защиты устройства, статус использования компонентов защиты;
- версия протокола, по которому осуществляется управление настройками ПО с сайта My Kaspersky;
- список проблем безопасности, список игнорируемых проблем безопасности, рекомендации списка проблем безопасности;
- информация о сработавшей записи базы данных;
- статус задач проверки;
- время последнего изменения статуса;
- сертификат проверяемого файла, публичный ключ сертификата проверяемого файла, отпечаток сертификата проверяемого файла;
- порт, по которому осуществляется соединение;
- содержимое и тип сертификата сайта, к которому обращается Пользователь, IP-адрес сайта, к которому обращается Пользователь, домен сайта, к которому обращается Пользователь;
- название обнаруженной угрозы;
- протокол, по которому получены данные статистики.

В целях улучшения качества защиты Пользователя при проведении платежных операций в интернете вы соглашаетесь в автоматическом режиме предоставить финансовому сайту информацию о наименовании и версии ПО и настройке кастомизации ПО, идентификатор состояния плагина ПО в используемом для обращения к финансовому сайту браузере, идентификатор использования безопасного или обычного браузера.

Полученная информация защищается Правообладателем в соответствии с установленными законом требованиями и требуется для обеспечения работы лицензированного вами ПО.

"Лаборатория Касперского" может использовать полученные статистические данные, созданные на основе полученной информации, для мониторинга тенденций в области угроз компьютерной безопасности и публикации отчетов о них.

Предоставление данных в Kaspersky Security Network

Состав данных, передаваемых в Kaspersky Security Network, описан в Положении о Kaspersky Security Network.

Чтобы ознакомиться с Положением о Kaspersky Security Network, выполните следующие действия:

1. Откройте главное окно программы.

2. Нажмите на кнопку ⚙ в нижней части окна программы.

   Откроется окно **Настройка**.

3. В окне **Настройка** выберите раздел **Дополнительно**.

4. В разделе **Дополнительно** выберите пункт **Дополнительные средства защиты и управления**.

   Откроется окно **Настройки дополнительных средств защиты**.

5. По ссылке **Положение о Kaspersky Security Network** откройте текст Положения о Kaspersky Security Network.

Сохранение данных в отчет о работе программы

Файлы отчетов могут содержать персональные данные, полученные в результате работы компонентов защиты, таких как Файловый Антивирус, Почтовый Антивирус, Веб-Антивирус.

Файлы отчетов могут содержать следующие персональные данные:

- IP-адрес устройства пользователя;
- история посещения сайтов;
- версия браузера и операционной системы;
- имена и пути расположения файлов cookie и других файлов;
- адрес электронной почты, отправитель, тема письма.

Файлы отчетов хранятся локально на вашем компьютере и не передаются в "Лабораторию Касперского". Путь к файлам отчетов: %allusersprofile%\Kaspersky Lab\AVP20.0\Report\Database.

Отчеты содержатся в следующих файлах:

- reports.db;
- reports.db-wal;
- reports.db-shm (не содержит персональных данных).

Файлы отчетов защищены от несанкционированного доступа, если в программе Kaspersky Anti-Virus включена самозащита. Если самозащита выключена, файлы отчетов не защищаются.

Сохранение данных для Службы технической поддержки

Программа обрабатывает и хранит следующие персональные данные для анализа Службой технической поддержки:

- Данные, которые отображаются в интерфейсе программы:
  - адрес электронной почты, используемый для подключения к My Kaspersky;

- адреса сайтов, которые были добавлены в исключения (отображаются в компоненте Сеть и в окне Отчеты);
- данные о лицензии.

Эти данные хранятся локально в немодифицированном виде и доступны для просмотра под любой учетной записью на компьютере.

- Данные о системной памяти процессов Kaspersky Anti-Virus на момент создания дампа памяти.
- Данные, собираемые при включении записи событий.

Эти данные хранятся локально в модифицированном виде и доступны для просмотра под любой учетной записью на компьютере. Эти данные передаются в "Лабораторию Касперского" только с вашего согласия при обращении в Службу технической поддержки. Ознакомиться с составом данных можно по ссылке **Положение о предоставлении данных** в окне **Мониторинг проблем**.

Об использовании программы на территории Европейского союза

Версии программы, которые "Лаборатория Касперского" и наши партнеры распространяют на территории Европейского союза, отвечают требованиям Общеевропейского регламента о персональных данных (General Data Protection Regulation).

Чтобы установить программу, вы должны принять Лицензионное соглашение и условия Политики конфиденциальности.

Кроме этого, мастер установки предложит вам принять следующие соглашения об обработке ваших персональных данных:

- Положение о Kaspersky Security Network. Это положение позволяет специалистам "Лаборатории Касперского" своевременно получать информацию об угрозах, обнаруженных на вашем компьютере, о запускаемых программах и о скачиваемых подписанных программах, а также информацию об операционной системе для улучшения вашей защиты.
- Положение об обработке данных для маркетинговых целей. Это положение позволяет нам делать более выгодные предложения для вас.

Вы можете в любой момент принять или отказаться от Положения о Kaspersky Security Network, а также принять или отказаться от Положения об обработке данных для маркетинговых целей в окне **Настройка** → **Дополнительно** → **Дополнительные средства защиты и управления**.

Для чего нужен My Kaspersky

My Kaspersky – это сайт "Лаборатории Касперского", предназначенный для централизованного хранения информации и управления программами "Лаборатории Касперского", которые вы используете.

На My Kaspersky вы можете:

- просматривать информацию о лицензиях и сроках их действия;
- управлять защитой компьютера удаленно;
- безопасно хранить и синхронизировать пароли и другую личную информацию, если вы используете Kaspersky Password Manager;
- скачивать приобретенные программы;
- обратиться в Службу технической поддержки за помощью;
- узнавать о новых программах и специальных предложениях "Лаборатории Касперского".

Чтобы иметь доступ к возможностям My Kaspersky, нужна учетная запись.

Подробную информацию о работе с My Kaspersky вы найдете в Справке My Kaspersky.

Об учетной записи My Kaspersky

Учетная запись My Kaspersky требуется для входа на сайт My Kaspersky, а также для работы с сайтом и некоторыми программами "Лаборатории Касперского".

Если у вас еще нет учетной записи, вы можете создать ее на сайте My Kaspersky или в программах, совместимых с ним. Вы также можете использовать для входа на сайт учетные данные других ресурсов "Лаборатории Касперского".

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

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

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

Активируйте учетную запись по ссылке из сообщения.

Как создать учетную запись My Kaspersky

Чтобы создать учетную запись My Kaspersky, выполните следующие действия:

1. Откройте главное окно программы.

2. В раскрывающемся списке **Больше функций** выберите элемент **My Kaspersky**.

3. В окне **My Kaspersky** нажмите на кнопку **Войти**.

   Откроется окно **Подключение к My Kaspersky**.

4. Нажмите на кнопку **У меня нет учетной записи**.

5. Введите адрес электронной почты в поле **Адрес электронной почты**.

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

7. Установите флажок **Я соглашаюсь предоставить "Лаборатории Касперского" адрес своей электронной почты для получения персональных маркетинговых предложений**, если вы хотите получать уведомления от "Лаборатории Касперского" на адрес электронной почты.

   Если вы используете программу на территории Европейского союза, этот флажок называется **Я подтверждаю, что разрешаю АО "Лаборатория Касперского" использовать мой адрес электронной почты, имя и фамилию, чтобы оповещать меня по электронной почте о персонализированных специальных предложениях, обзорах, опросах, напоминать о незавершенных заказах, отправлять актуальные новости и события** или **Я подтверждаю, что разрешаю АО "Лаборатория Касперского" использовать мой адрес электронной почты, чтобы оповещать меня по электронной почте о персонализированных специальных предложениях, обзорах, опросах, напоминать о незавершенных заказах, отправлять актуальные новости и события**.

8. Укажите свое имя в поле **Ваше имя**.

9. Укажите свою фамилию в поле **Ваша фамилия**.

10. Нажмите на кнопку **Создать**.

    На указанный вами адрес электронной почты будет отправлено письмо со ссылкой, по которой необходимо перейти для активации учетной записи My Kaspersky.

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

Состав полей при создании учетной записи формируется специалистами "Лаборатории Касперского" и может меняться.

Об удаленном управлении защитой компьютера

Если на компьютере установлена программа Kaspersky Anti-Virus и компьютер подключен к My Kaspersky, вы можете управлять защитой этого компьютера удаленно.

Чтобы удаленно управлять защитой компьютера, вам нужно войти в My Kaspersky под своей учетной записью и перейти в раздел **Устройства**.

В разделе **Устройства** вы можете:

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

- настраивать компоненты программы Kaspersky Anti-Virus.

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

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

Как перейти к удаленному управлению защитой компьютера

Чтобы перейти к удаленному управлению защитой компьютера, вам нужно подключить устройство к My Kaspersky. Программа автоматически подключается к My Kaspersky, если ранее вы вводили свои учетные данные в другой программе "Лаборатории Касперского" на этом компьютере. Если программе не удалось автоматически подключить ваше устройство к My Kaspersky, вам нужно выполнить подключение вручную.

Чтобы подключить устройство к My Kaspersky, выполните следующие действия:

1. Откройте главное окно программы.
2. В раскрывающемся списке **Больше функций** выберите элемент **My Kaspersky**.
3. Нажмите на кнопку **Войти**.
   - В окне **Подключение к My Kaspersky** введите данные для подключения программы к My Kaspersky и нажмите кнопку **Войти**.
   - Если у вас еще нет учетной записи на My Kaspersky, выполните следующие действия:
     a. Нажмите на кнопку **У меня нет учетной записи**, и зарегистрируйтесь на My Kaspersky.
     b. Нажмите на кнопку **Создать**.

Программа подключит устройство к My Kaspersky.

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

1. Откройте главное окно программы.
2. В раскрывающемся списке **Больше функций** выберите элемент **My Kaspersky**.
3. В окне **My Kaspersky** нажмите на кнопку **Перейти на My Kaspersky**.

В браузере по умолчанию откроется окно My Kaspersky.

Подключение к My Kaspersky может отсутствовать в результате сбоя в работе My Kaspersky. В этом случае Kaspersky Anti-Virus показывает уведомление о том, что на My Kaspersky возникли проблемы, которые решаются специалистами "Лаборатории Касперского". Если вы не можете подключиться к My Kaspersky в результате сбоя в работе My Kaspersky, повторите попытку подключения позже.

Восстановление операционной системы после заражения

Этот раздел содержит информацию о восстановлении операционной системы после заражения вредоносными программами.

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. В раскрывающемся списке **Больше функций** выберите элемент **Восстановление 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 **Готово**. Для прекращения работы мастера на любом этапе следует нажать на кнопку **Отмена**.

Рассмотрим подробнее шаги мастера.

Запуск восстановления операционной системы

a. Выберите один из двух вариантов работы мастера:

- **Выполнить поиск повреждений, связанных с активностью вредоносных программ**. Мастер выполнит поиск проблем и возможных повреждений.
- **Отменить изменения**. Мастер отменит исправления ранее выявленных проблем и повреждений.

b. Нажмите на кнопку **Далее**.

Поиск проблем

Если вы выбрали вариант **Выполнить поиск повреждений, связанных с активностью вредоносных программ**, мастер выполняет поиск проблем и возможных повреждений, которые следует исправить. По завершении поиска мастер автоматически переходит к следующему шагу.

Выбор действий для устранения повреждений

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

Всего выделено три группы:

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

Раскройте список выбранной группы, чтобы просмотреть повреждения, входящие в эту группу.

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

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

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

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.

Завершение работы мастера

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

Об аварийном восстановлении операционной системы

Для аварийного восстановления операционной системы предназначена программа Kaspersky Rescue Disk. Вы можете использовать Kaspersky Rescue Disk для проверки и лечения зараженного компьютера, который нельзя вылечить другим способом (например, с помощью антивирусных программ).

Более подробную информацию об использовании Kaspersky Rescue Disk вы найдете на сайте Службы технической поддержки.

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 Anti-Virus или в режиме Connected Standby в Windows 8. Уведомления о запуске программы автоматически закрываются по истечении 1 часа. При автоматическом закрытии уведомления Kaspersky Anti-Virus выполняет действие, рекомендованное по умолчанию.

Уведомления не отображаются в течение первого часа работы программы в случае приобретения компьютера с предустановленной программой Kaspersky Anti-Virus (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**. В этом окне приведена подробная информация о состоянии защиты компьютера и предложены варианты действий для устранения проблем и угроз.

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

В разделе **Рекомендации** отображаются уведомления о действиях, которые рекомендуется выполнить для оптимизации работы программы и более эффективного ее использования.

В разделе **Показать N игнорируемых уведомлений** отображаются уведомления, к которым было применено действие **Игнорировать**. Проблемы в этом разделе не влияют на цвет индикатора защиты в главном окне программы.

Обновление баз и программных модулей

Этот раздел содержит информацию об обновлении баз и программных модулей.

Об обновлении баз и программных модулей

Пакет установки Kaspersky Anti-Virus включает в себя базы и программные модули. С помощью этих баз:

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

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

Обновление баз и программных модулей выполняется поэтапно:

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

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

Источники обновлений

Вы можете использовать следующие источники обновлений:

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

Особенности обновления баз и программных модулей

Обновление баз и программных модулей имеет следующие особенности и ограничения:

- Базы устаревают по истечении одного дня и сильно устаревают по истечении семи дней.
- Для скачивания пакета обновлений с серверов обновлений "Лаборатории Касперского" требуется соединение с интернетом.
- Обновление баз и программных модулей недоступно в следующих случаях:

- Истек срок действия лицензии, и не предусмотрен льготный период или режим ограниченной функциональности.

- Используется высокоскоростное мобильное подключение к интернету. Это ограничение действует при работе в операционной системе Microsoft Windows 8 и выше, если выбран автоматический режим обновления или режим обновления по расписанию и установлено ограничение трафика при высокоскоростном мобильном подключении. Чтобы в этом случае выполнялось обновление баз и программный модулей, требуется снять флажок **Ограничивать трафик при лимитном подключении** в окне **Настройка → Дополнительно → Сеть**.

- Программа используется по подписке, и вы приостановили подписку на сайте поставщика услуг.

Установка пакета исправлений

При получении пакета исправлений (патча) Kaspersky Anti-Virus устанавливает его автоматически. Для завершения установки пакета исправлений требуется перезагрузить компьютер. До перезагрузки компьютера значок программы в области уведомлений имеет красный цвет, а в окне **Центр уведомлений** Kaspersky Anti-Virus отображается предложение перезагрузить компьютер.

Как запустить обновление баз и программных модулей

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

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

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

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

   Откроется окно **Обновление баз**.

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

Проверка компьютера

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

Полная проверка

Во время полной проверки по умолчанию Kaspersky Anti-Virus проверяет следующие объекты:

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

Рекомендуется выполнить полную проверку сразу после установки Kaspersky Anti-Virus 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 Anti-Virus начнет полную проверку компьютера.

Выборочная проверка

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

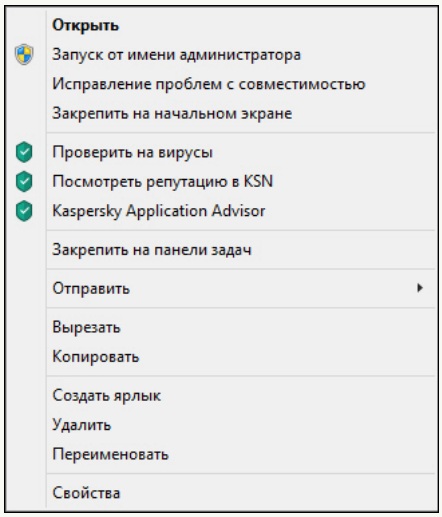
Запустить выборочную проверку вы можете следующими способами:

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

Как запустить выборочную проверку из контекстного меню объекта

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**.



Контекстное меню объекта

[Как запустить выборочную проверку из главного окна программы](#)

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

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

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

Быстрая проверка

Во время быстрой проверки Kaspersky Anti-Virus по умолчанию проверяет следующие объекты:

- объекты, которые загружаются при запуске операционной системы;
- системная память;

- загрузочные сектора диска.

Чтобы запустить быструю проверку, выполните следующие действия:

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

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

Kaspersky Anti-Virus начнет быструю проверку компьютера.

Поиск уязвимостей

В операционной системе и программах, установленных на компьютере, могут быть уязвимости, через которые способны проникнуть вредоносные программы. Проверка вашего компьютера поможет найти эти уязвимости и предотвратить заражение компьютера.

Чтобы запустить поиск уязвимостей, выполните следующие действия:

1. Откройте главное окно программы.
2. В раскрывающемся списке **Больше функций** выберите элемент **Поиск уязвимостей**.
3. В окне **Поиск уязвимостей** нажмите на кнопку **Начать поиск**.

Kaspersky Anti-Virus начнет проверку вашего компьютера на наличие уязвимостей.

Проверка файлов в облачном хранилище OneDrive

На операционной системе Windows 10 RS3 и выше Kaspersky Anti-Virus не проверяет файлы в облачном хранилище OneDrive. Если программа обнаруживает такие файлы во время проверки, она показывает уведомление о том, что файлы в облачном хранилище не были проверены.

Следующие компоненты не проверяют файлы в облачном хранилище OneDrive:

- Полная проверка;
- Выборочная проверка;
- Быстрая проверка;
- Фоновая проверка.

Отчет о работе Kaspersky Anti-Virus содержит список файлов в облачном хранилище OneDrive, пропущенных во время проверки.

Файлы, загруженные из облачного хранилища OneDrive на локальный компьютер, проверяются компонентами постоянной защиты. Если проверка файла происходит в отложенном режиме и файл был загружен обратно в облачное хранилище OneDrive до начала проверки, такой файл может быть пропущен при проверке.

Как восстановить удаленный или вылеченный программой объект

"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 Anti-Virus 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 Anti-Virus 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. В раскрывающемся списке **Больше функций** выберите элемент **Карантин**.
3. В открывшемся окне **Карантин** выберите нужный файл в списке и нажмите на кнопку **Восстановить**.

Как настроить Почтовый Антивирус

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

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

Чтобы настроить Почтовый Антивирус, выполните следующие действия:

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

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

   В окне отобразятся настройки Почтового Антивируса.
4. Убедитесь, что переключатель в верхней части окна, включающий / выключающий Почтовый Антивирус, включен.
5. Выберите уровень безопасности:

   - **Рекомендуемый**. При установке этого уровня безопасности Почтовый Антивирус проверяет входящие и исходящие сообщения, вложенные архивы, а также выполняет эвристический анализ с уровнем детализации **Средний**.
   - **Низкий**. При установке этого уровня безопасности Почтовый Антивирус проверяет только входящие сообщения и не проверяет вложенные архивы.
   - **Высокий**. При установке этого уровня безопасности Почтовый Антивирус проверяет входящие и исходящие сообщения, вложенные архивы, а также проводит эвристический анализ с уровнем детализации **Глубокий**.
6. В раскрывающемся списке **Действие при обнаружении угрозы** выберите действие, которое Почтовый Антивирус будет выполнять при обнаружении зараженного объекта (например, лечить).

Если угрозы в почтовом сообщении не были обнаружены или зараженные объекты были успешно вылечены, почтовое сообщение становится доступным для работы. Если зараженный объект вылечить не удалось, Почтовый Антивирус переименовывает или удаляет объект из сообщения и помещает в тему сообщения уведомление о том, что оно обработано Kaspersky Anti-Virus. В случае удаления объекта Kaspersky Anti-Virus создает его резервную копию и помещает на карантин.

При переходе на более новую версию программы настроенные пользователем настройки Почтового Антивируса не сохраняются. Новая версия программы будет использовать установленные по умолчанию настройки Почтового Антивируса.

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

Защита персональных данных в интернете

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

О защите персональных данных в интернете

С помощью Kaspersky Anti-Virus вы можете защитить от кражи свои персональные данные:

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

В состав Kaspersky Anti-Virus входят компоненты и инструменты, позволяющие защитить ваши персональные данные от кражи злоумышленниками, использующими такие методы как фишинг и перехват данных, вводимых с клавиатуры.

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

Для защиты от перехвата данных, введенных с клавиатуры, предназначена Экранная клавиатура.

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

Об Экранной клавиатуре

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

В таких случаях существует опасность перехвата персональных данных с помощью аппаратных перехватчиков или клавиатурных шпионов – программ, регистрирующих нажатие клавиш. Экранная клавиатура позволяет избежать перехвата данных, вводимых с клавиатуры.

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

Экранная клавиатура имеет следующие особенности:

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

нужно нажимать правой клавишей мыши (например, если в настройках операционной системы для переключения языка ввода задана комбинация **LEFT ALT**+**SHIFT**, то на клавишу **LEFT ALT** нужно нажимать левой клавишей мыши, а на клавишу **SHIFT** нужно нажимать правой клавишей мыши).

Для защиты данных, вводимых с помощью Экранной клавиатуры, после установки Kaspersky Anti-Virus необходимо перезагрузить компьютер.

Использование Экранной клавиатуры имеет следующие ограничения:

- Экранная клавиатура защищает от перехвата персональных данных только при работе с браузерами Microsoft Internet Explorer, Mozilla Firefox и Google Chrome. При работе с другими браузерами Экранная клавиатура не защищает вводимые персональные данные от перехвата.
- Экранная клавиатура недоступна в браузере Microsoft Internet Explorer (версии 10 и 11) в стиле Fluent Design. В этом случае рекомендуется вызывать Экранную клавиатуру из интерфейса Kaspersky Anti-Virus.
- Экранная клавиатура не может защитить ваши персональные данные в случае взлома сайта, требующего ввода таких данных, поскольку в этом случае информация попадет непосредственно в руки злоумышленников.
- Экранная клавиатура не предотвращает снятие снимков экрана с помощью нажатия клавиши **Print Screen** и других комбинаций клавиш, заданных в настройках операционной системы.
- При запуске Экранной клавиатуры в браузере Microsoft Internet Explorer перестает работать функция автозаполнения полей ввода, так как реализация системы автозаполнения позволяет злоумышленникам перехватывать вводимые данные.

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". В статье перечислены ограничения на защиту ввода с аппаратной клавиатуры в Kaspersky Internet Security, эти ограничения распространяются и на Экранную клавиатуру в Kaspersky Anti-Virus.

Как открыть Экранную клавиатуру

Открыть Экранную клавиатуру можно следующими способами:

- из контекстного меню значка программы в области уведомлений;
- из окна программы;
- из панели инструментов браузеров Microsoft Edge на базе Chromium, Mozilla Firefox или Google Chrome;
- с помощью комбинации клавиш аппаратной клавиатуры.

Запуск Экранной клавиатуры из контекстного меню

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

выберите пункт **Экранная клавиатура**.

Запуск Экранной клавиатуры из окна программы

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

1. Откройте главное окно программы.
2. Нажмите на кнопку **Экранная клавиатура**.

Запуск Экранной клавиатуры из панели инструментов браузера

Чтобы открыть Экранную клавиатуру из панели инструментов браузера Microsoft Edge на базе Chromium, Mozilla Firefox или Google Chrome, выполните следующие действия:

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

Запуск Экранной клавиатуры с помощью аппаратной клавиатуры

Чтобы открыть Экранную клавиатуру с помощью аппаратной клавиатуры,

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

Проверка безопасности сайта

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

Компонент Проверка ссылок проверяет ссылки на веб-странице, открытой в браузере Microsoft Edge на базе Chromium, Google Chrome или Mozilla Firefox. Рядом с проверенной ссылкой Kaspersky Anti-Virus 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, по данным "Лаборатории Касперского" может быть использована злоумышленниками для нанесения вреда компьютеру или вашим данным;

– 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 Anti-Virus проверяет ссылки только в результатах поиска. Вы можете включить проверку ссылок на любом сайте.

Чтобы настроить проверку ссылок на сайтах, выполните следующие действия:

1. Откройте главное окно программы.

2. Нажмите на кнопку ⚙ в нижней части окна программы.

   Откроется окно **Настройка**.

3. В разделе **Защита** выберите подраздел **Веб-Антивирус**.

   В окне отобразятся настройки Веб-Антивируса.

4. По ссылке **Расширенная настройка** в нижней части окна откройте окно дополнительных настроек Веб-Антивируса.

5. В блоке **Проверка ссылок** установите флажок **Проверять ссылки**.

6. Чтобы Kaspersky Anti-Virus проверял содержимое всех сайтов, выберите вариант **На всех сайтах, кроме указанных**.

7. Если необходимо, укажите веб-страницы, которым вы доверяете, в окне **Исключения**. Окно открывается по ссылке **Настроить исключения**. Kaspersky Anti-Virus не будет проверять содержимое указанных веб-страниц.

8. Чтобы Kaspersky Anti-Virus проверял содержимое только определенных веб-страниц, выполните следующие действия:

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

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

   c. Нажмите на кнопку **Добавить**.

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

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

   f. Нажмите на кнопку **Добавить**.

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

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

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

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

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

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

Kaspersky Anti-Virus будет проверять ссылки на указанных веб-страницах и отображать информации о категориях ссылок в соответствии с выбранными настройками.

Как изменить настройки защищенных соединений

Защищенные соединения – это соединения, которые устанавливаются по протоколам SSL и TLS. По умолчанию программа Kaspersky Anti-Virus выполняет проверку таких соединений по запросу компонента Проверка ссылок.

Чтобы изменить настройки защищенных соединений, выполните следующие действия:

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

   Откроется окно **Настройка**.
3. Перейдите в раздел **Дополнительно**.
4. По ссылке **Сеть** перейдите в окно **Настройки сети**.
5. В блоке **Проверка защищенных соединений** по ссылке **сайты** откройте окно **Сайты**.

   Окно содержит список сайтов, защищенное соединение на которых не может быть расшифровано. Проверка защищенных соединений на этих сайтах не может быть выполнена. Список обновляется специалистами "Лаборатории Касперского".
6. Выберите вариант действия при подключении к сайтам по защищенному соединению:

   - **Не проверять защищенные соединения**. Программа не проверяет защищенные соединения.
   - **Проверять защищенные соединения по запросу компонентов защиты**. Программа проверяет защищенные соединения, только если на это будет запрос от компонента Проверка ссылок. Этот вариант действия выбран по умолчанию.
   - **Всегда проверять защищенные соединения**. Программа всегда проверяет защищенные соединения.
7. Выберите вариант действия, если возникают ошибки при проверке защищенных соединений:

   - **Игнорировать**. Если выбран этот вариант, программа разрывает соединение с сайтом, на котором возникла ошибка проверки защищенного соединения.
   - **Спрашивать**. Если выбран этот вариант, при возникновении ошибки проверки защищенного соединения с сайтом, программа показывает уведомление, в котором вы можете выбрать вариант действия:

     - **Игнорировать**. Если выбран этот вариант, программа разрывает соединение с сайтом, на котором возникла ошибка проверки.
     - **Добавлять сайт в исключения**. Если выбран этот вариант, программа добавляет адрес сайта в список исключений. Программа не проверяет защищенные соединения на сайтах, которые входят в список исключений. Такие сайты отображаются в окне **Сайты с ошибками проверки**.

     Этот вариант выбран по умолчанию.
   - **Добавлять сайт в исключения**. Если выбран этот вариант, программа добавляет сайт в список исключений. Программа не проверяет защищенные соединения на сайтах, входящих в список исключений. Такие сайты отображаются в окне **Сайты с ошибками проверки**.

8. По ссылке **Сайты с ошибками проверки** откройте окно **Сайты с ошибками проверки**. Программа не проверяет защищенное соединение на этих сайтах. Однако программа проверяет адреса этих сайтов по базе адресов вредоносных сайтов. Если сайт входит в базу адресов вредоносных сайтов, программа разрывает соединение с таким сайтом.

9. По ссылке **Настроить исключения** откройте окно **Исключения** и выполните следующие действия:

   a. Нажмите на кнопку **Добавить**, чтобы добавить сайт в список исключений из проверки защищенных соединений.

   b. Укажите доменное имя сайта в поле **Доменное имя**.

   c. Нажмите на кнопку **Добавить**.

      Программа не будет проверять защищенное соединение с этим сайтом. Обратите внимание, что добавление сайта в список исключений означает, что функциональность проверки этого сайта компонентом Проверка ссылок будет ограничена.

Запуск программы защиты паролей Kaspersky Password Manager

Программа Kaspersky Password Manager предназначена для безопасного хранения и синхронизации паролей между вашими устройствами. Kaspersky Password Manager нужно устанавливать независимо от Kaspersky Anti-Virus, например, с помощью ярлыка **Kaspersky Passwords**, который создается на Рабочем столе вашего компьютера в процессе установки Kaspersky Anti-Virus.

После установки вы можете запускать Kaspersky Password Manager из меню **Пуск** (в операционных системах Microsoft Windows 7, Microsoft Windows 10) или с начального экрана (в операционных системах Microsoft Windows 8, Microsoft Windows 8.1).

Как скачать и установить программу Kaspersky Password Manager

Чтобы скачать и установить программу защиты паролей Kaspersky Password Manager,

воспользуйтесь одним из следующих способов:

- двойным щелчком мыши на ярлыке **Kaspersky Passwords** на Рабочем столе;
- кнопкой **Узнать больше** в окне **Центр уведомлений** в разделе **Рекомендации** напротив предложения установить Kaspersky Password Manager.

Kaspersky Anti-Virus скачает установочный пакет Kaspersky Password Manager и установит программу на ваш компьютер.

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

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

Как устранить следы работы на компьютере

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

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

Сведения о действиях пользователя, содержащие конфиденциальные данные, могут оказаться доступными злоумышленникам и посторонним лицам.

В состав Kaspersky Anti-Virus входит мастер устранения следов активности пользователя в операционной системе.

Чтобы запустить мастер устранения следов активности, выполните следующие действия:

1. Откройте главное окно программы.
2. В раскрывающемся списке **Больше функций** выберите элемент **Устранение следов активности**, чтобы запустить 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 **Готово**. Для прекращения работы мастера на любом этапе следует нажать на кнопку **Отмена**.

Рассмотрим подробнее шаги мастера.

Начало работы мастера

a. Выберите один из двух вариантов работы мастера:

- **Выполнить поиск следов активности пользователя**. Мастер выполнит поиск следов вашей работы на компьютере.
- **Отменить внесенные ранее изменения**. Мастер отменит изменения, которые были сделаны в результате предыдущей работы мастера устранения следов активности. Этот вариант действия доступен, если в результате предыдущей работы мастера следы активности были устранены.

b. Нажмите на кнопку **Далее**, чтобы начать работу мастера.

Поиск следов активности

Если вы выбрали вариант **Выполнить поиск следов активности пользователя**, мастер осуществляет поиск следов активности на вашем компьютере. Поиск может занять некоторое время. По завершении поиска мастер автоматически переходит к следующему шагу.

Выбор действий для устранения следов активности

По завершении поиска мастер сообщает об обнаруженных следах активности и предлагаемых действиях для их устранения.

Для просмотра действий, включенных в группу, раскройте список выбранной 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**.

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.

Завершение работы мастера

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

Как сохранить ресурсы операционной системы для компьютерных игр

При одновременной работе Kaspersky Anti-Virus 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 Anti-Virus отвлекают от игры.

Чтобы не изменять настройки Kaspersky Anti-Virus вручную перед каждым переходом в полноэкранный режим, вы можете использовать Игровой режим. Если Игровой режим используется и вы играете или работаете с программами в полноэкранном режиме, Kaspersky Anti-Virus не запускает задачи проверки и обновления, не отображает уведомления.

Чтобы включить использование Игрового режима, выполните следующие действия:

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

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

   В окне отобразятся настройки производительности Kaspersky Anti-Virus.
4. Установите флажок **Использовать Игровой режим**.

Как защитить доступ к управлению Kaspersky Anti-Virus с помощью пароля

На одном компьютере могут работать несколько пользователей с разным опытом и уровнем компьютерной грамотности. Неограниченный доступ разных пользователей к управлению Kaspersky Anti-Virus и его настройке 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 программы;
- завершение работы программы;
- удаление программы.

Чтобы защитить доступ к Kaspersky Anti-Virus с помощью пароля, выполните следующие действия:

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

   Откроется окно **Настройка**.
3. В левой части окна выберите раздел **Общие** и по ссылке **Установить защиту паролем** откройте окно **Защита паролем**.
4. В открывшемся окне заполните поля **Новый пароль** и **Подтверждение пароля**.

   Требования к паролю:

   1. Длина пароля должна быть не менее 8 символов;
   2. Пароль должен содержать не менее одной цифры;
   3. Пароль должен содержать прописные и строчные буквы одновременно.
5. В блоке настроек **Область действия пароля** укажите действия с программой, доступ к которым нужно защитить паролем.

Забытый пароль восстановить нельзя. Если пароль забыт, для восстановления доступа к настройкам Kaspersky Anti-Virus потребуется обращение в Службу технической поддержки.

Как приостановить и возобновить защиту компьютера

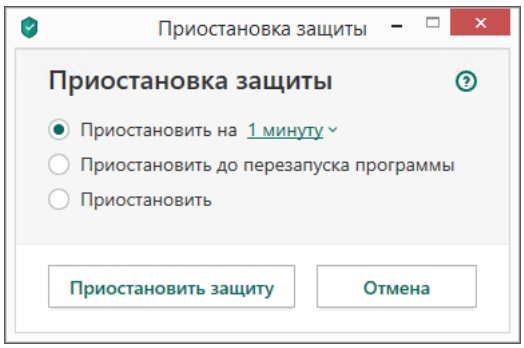
Приостановка защиты означает выключение на некоторое время всех ее компонентов.

Во время приостановки защиты или выключения Kaspersky Anti-Virus 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 Anti-Virus использует эту информацию для защиты вашего компьютера от вредоносных действий, которые могли быть выполнены во время приостановки защиты или выключения Kaspersky Anti-Virus. Хранение информации о результатах контроля активности программ не ограничено по времени. Эта информация удаляется в случае удаления Kaspersky Anti-Virus с вашего компьютера.

Чтобы приостановить защиту компьютера, выполните следующие действия:

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

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



Окно Приостановка защиты

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

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

3. Нажмите на кнопку **Приостановить защиту** и подтвердите действие в открывшемся окне.

Как возобновить защиту компьютера

Чтобы возобновить защиту компьютера,

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

Как восстановить стандартные настройки работы программы

Вы в любое время можете восстановить настройки Kaspersky Anti-Virus, рекомендуемые "Лабораторией Касперского". Восстановление настроек осуществляется с помощью мастера.

В результате работы мастера для всех компонентов защиты будет установлен уровень безопасности **Рекомендуемый**.

Чтобы восстановить стандартные настройки работы программы, выполните следующие действия:

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

   Откроется окно **Настройка**.
3. Выберите раздел **Общие**.

   В окне отобразятся настройки Kaspersky Anti-Virus.
4. В нижней части окна в раскрывающемся списке **Управление настройками** выберите элемент **Восстановить настройки**.
5. Нажмите на кнопку **Далее**.

   В окне мастера отобразится процесс восстановления настроек работы программы до тех, которые заданы специалистами "Лаборатории Касперского" по умолчанию.
6. После того как процесс восстановления стандартных настроек работы программы будет завершен, нажмите на кнопку **Готово**.

Как просмотреть отчет о работе программы

Kaspersky Anti-Virus ведет отчеты о работе каждого компонента защиты. С помощью отчета вы можете получить статистическую информацию о работе программы (например, узнать, сколько обнаружено и обезврежено вредоносных объектов за определенный период, сколько раз за это время обновлялись базы и программные модули и многое другое).

Чтобы просмотреть отчет о работе программы, выполните следующие действия:

1. Откройте главное окно программы.

2. Нажмите на кнопку **Отчеты**.

   В окне **Отчеты** отображаются отчеты о работе программы за текущий день (в левой части окна) и за период (в правой части окна).

3. Если вам нужно просмотреть подробный отчет о работе программы, откройте окно **Подробные отчеты** по ссылке **Подробные отчеты**, расположенной в верхней части окна **Отчеты**.

   В окне **Подробные отчеты** данные представлены в табличном виде. Для удобства просмотра отчетов вы можете выбирать различные варианты фильтрации записей.

Как применить настройки программы на другом компьютере

Настроив программу, вы можете применить настройки ее работы к программе Kaspersky Anti-Virus, установленной на другом компьютере. В результате программа на обоих компьютерах будет настроена одинаково.

Настройки работы программы сохраняются в конфигурационном файле, который вы можете перенести с одного компьютера на другой.

Перенос настроек Kaspersky Anti-Virus с одного компьютера на другой производится в три этапа:

1. Сохранение настроек программы в конфигурационном файле.
2. Перенос конфигурационного файла на другой компьютер (например, по электронной почте или на съемном диске).
3. Импорт настроек из конфигурационного файла в программу, установленную на другом компьютере.

Как экспортировать настройки программы

Чтобы экспортировать настройки программы, выполните следующие действия:

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

   Откроется окно **Настройка**.
3. В окне **Настройка** выберите раздел **Общие**.
4. В раскрывающемся списке **Управление настройками** выберите элемент **Экспортировать настройки**.
5. Откроется окно **Сохранение**.
6. Задайте имя конфигурационного файла и нажмите на кнопку **Сохранить**.

   Настройки программы будут сохранены в конфигурационный файл.

Вы также можете экспортировать настройки работы программы при помощи командной строки, используя команду: `avp.com EXPORT <имя_файла>`.

Как импортировать настройки программы

Чтобы импортировать настройки в программу, установленную на другом компьютере, выполните следующие действия:

1. Откройте главное окно программы Kaspersky Anti-Virus, установленной на другом компьютере.
2. Нажмите на кнопку ⚙ в нижней части окна.

   Откроется окно **Настройка**.
3. В окне **Настройка** выберите раздел **Общие**.
4. В раскрывающемся списке **Управление настройками** выберите элемент **Импортировать настройки**.

   Откроется окно **Открыть**.
5. Укажите конфигурационный файл и нажмите на кнопку **Открыть**.

Настройки будут импортированы в программу, установленную на другом компьютере.

Участие в Kaspersky Security Network

Чтобы повысить эффективность защиты вашего компьютера, Kaspersky Anti-Virus использует облачную защиту. Облачная защита реализуется с помощью инфраструктуры Kaspersky Security Network, использующей данные, полученных от пользователей во всем мире.

Kaspersky Security Network (KSN) – это облачная база знаний "Лаборатории Касперского", которая содержит информацию о репутации программ и сайтов. Использование данных Kaspersky Security Network обеспечивает более высокую скорость реакции Kaspersky Anti-Virus 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 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 Anti-Virus.

Как включить и выключить участие в Kaspersky Security Network

Участие в Kaspersky Security Network является добровольным. Вы можете включить или выключить использование Kaspersky Security Network (KSN) во время установки Kaspersky Anti-Virus и / или в любой момент после установки программы.

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

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

   Откроется окно **Настройка**.
3. В разделе **Дополнительно** выберите блок **Дополнительные средства защиты и управления**.

   В открывшемся окне **Настройки дополнительных средств защиты** отобразятся сведения о Kaspersky Security Network и настройки участия в Kaspersky Security Network.
4. Включите или выключите участие в Kaspersky Security Network:

   - Если вы хотите участвовать в Kaspersky Security Network, нажмите на кнопку **Включить**.

     Откроется окно с текстом Положения о Kaspersky Security Network. Если вы согласны с условиями положения, нажмите на кнопку **Я согласен**.

   - Если вы не хотите участвовать в Kaspersky Security Network, нажмите на кнопку **Выключить**.

Если вы установили программу на территории Европейского союза, вместо информации о Kaspersky Security Network в окне **Настройки дополнительных средств защиты** отображается **Положение о Kaspersky Security Network**.

Чтобы принять Положение о Kaspersky Security Network, выполните следующие действия:

1. Нажмите на кнопку **Принять** в блоке **Положение о Kaspersky Security Network**.

   Откроется Положение о Kaspersky Security Network. Это положение позволяет специалистам "Лаборатории Касперского" своевременно получать информацию об угрозах, обнаруженных на вашем компьютере, о запускаемых программах и о скачиваемых подписанных программах, а также информацию об операционной системе для улучшения вашей защиты.

2. Если вы принимаете условия положения, нажмите на кнопку **Принять**.

Чтобы отказаться от Положения о Kaspersky Security Network,

нажмите на кнопку **Отказаться** в блоке **Положение о Kaspersky Security Network**.

Как проверить подключение 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. В раскрывающемся списке **Больше функций** выберите элемент **Облачная защита**.

В окне **Облачная защита** отобразится статус подключения к Kaspersky Security Network.

Защита с помощью аппаратной виртуализации

В этом разделе вы узнаете, как вы можете защитить свой компьютер с помощью аппаратной виртуализации.

О защите с помощью аппаратной виртуализации

Программа Kaspersky Anti-Virus, установленная в 64-разрядной операционной системе Microsoft Windows 8, Microsoft Windows 8.1 или Microsoft Windows 10, использует технологию гипервизора для дополнительной защиты от сложных вредоносных программ, которые могут похищать ваши персональные данные с помощью буфера обмена и фишинга.

Защита с помощью аппаратной виртуализации включена по умолчанию. Если защита была выключена вручную, вы можете включить ее в окне настройки программы.

Функциональность защиты с помощью аппаратной виртуализации (гипервизора) Kaspersky Anti-Virus имеет следующие ограничения в 64-разрядных операционных системах Microsoft Windows 8, Microsoft Windows 8.1 или Microsoft Windows 10:

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

Как включить защиту с помощью аппаратной виртуализации

Чтобы включить защиту с помощью аппаратной виртуализации, выполните следующие действия:

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

   Откроется окно **Настройка**.
3. В левой части окна выберите раздел **Дополнительно**.
4. В правой части раздела **Дополнительно** выберите подраздел **Дополнительные средства защиты и управления**.

   Откроется окно **Настройки дополнительных средств защиты**.

5. Установите флажок **Использовать аппаратную виртуализацию, если она доступна**. Флажок отображается в 64-разрядной версии Windows 8, Windows 8.1 и Windows 10.

6. Установите флажок **Использовать расширенные возможности аппаратной виртуализации**, если вы хотите, чтобы аппаратная виртуализация включалась при запуске операционной системы.

Если на вашем компьютере выключена аппаратная виртуализация, защита с помощью аппаратной виртуализации не работает. Чтобы получить информацию о том, как включить аппаратную виртуализацию, пройдите по ссылке **Подробнее** в окне **Дополнительные средства защиты и управления**.

Работа с программой из командной строки

Вы можете работать с Kaspersky Anti-Virus 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 Anti-Virus 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.

Вы можете включать и выключать запись событий программы (создание файлов трассировки) через командную строку, если ранее вы установили пароль на защиту доступа к управлению Kaspersky Anti-Virus в окне настройки программы.

Если вы не установили пароль в окне настройки программы, вы не сможете создать пароль и включить запись событий из командной строки.

Некоторые команды можно выполнить только под учетной записью администратора.

Оценка работы Kaspersky Anti-Virus

Вы можете отправить в "Лабораторию Касперского" вашу оценку работы Kaspersky Anti-Virus.

По истечении некоторого времени с момента установки программа предлагает вам оценить ее работу.

Чтобы оценить работу Kaspersky Anti-Virus, выполните следующие действия:

1. В окне **Нам важно ваше мнение** выполните одно из следующих действий:

   - Если вы готовы оценить работу Kaspersky Anti-Virus, поставьте программе оценку по 10-балльной шкале.

   - Если вы не хотите оценивать работу Kaspersky Anti-Virus, нажмите на кнопку ×, чтобы закрыть окно оценки.

2. Нажмите на кнопку **Отправить**.

3. Нажмите на кнопку **Закрыть**, чтобы закрыть окно.

Обращение в Службу технической поддержки

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

Способы получения технической поддержки

Если вы не нашли решения вашей проблемы в справке программы или в одном из источников информации о программе, рекомендуем обратиться в Службу технической поддержки "Лаборатории Касперского". Сотрудники Службы технической поддержки ответят на ваши вопросы об установке и использовании программы.

Прежде чем обратиться в Службу технической поддержки, ознакомьтесь с правилами предоставления технической поддержки.

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 сайта My Kaspersky. Этот способ позволяет вам связаться со специалистами Службы технической поддержки через форму запроса.

Техническая поддержка предоставляется только пользователям, которые приобрели лицензию на использование программы. Техническая поддержка для пользователей пробных версий не осуществляется.

Техническая поддержка по телефону

В большинстве регионов по всему миру вы можете позвонить специалистам Службы технической поддержки. Вы можете найти информацию о способах получения технической поддержки в вашем регионе и контакты Службы технической поддержки на веб-сайте Службы технической поддержки "Лаборатории Касперского".

Перед обращением в Службу технической поддержки ознакомьтесь с правилами предоставления технической поддержки.

Техническая поддержка через My Kaspersky

Сайт My Kaspersky – это единый онлайн-ресурс для управления защитой ваших устройств и кодами активации программ "Лаборатории Касперского", а также для получения технической поддержки.

Для доступа к сайту My Kaspersky вам нужно зарегистрироваться. Для этого вам нужно указать адрес электронной почты и задать пароль.

Для получения технической поддержки вы можете выполнять следующие действия на сайте My Kaspersky:

- отправлять запросы в Службу технической поддержки;

- обмениваться сообщениями со Службой технической поддержки без использования электронной почты;
- отслеживать состояние ваших запросов в реальном времени.

Вы также можете просматривать полную историю ваших запросов в Службу технической поддержки.

Электронный запрос в Службу технической поддержки

В электронном запросе в Службу технической поддержки вам нужно указать следующую информацию:

- тему вашего запроса;
- название и номер версии программы;
- название и номер версии операционной системы;
- описание проблемы.

Специалист Службы технической поддержки направляет ответ на ваш вопрос на сайт My Kaspersky и на адрес электронной почты, который вы указали при регистрации.

Сбор информации для Службы технической поддержки

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

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 настройки программы. Для этого может потребоваться выполнение следующих действий:

- Собрать расширенную диагностическую информацию.
- Выполнить более тонкую настройку работы отдельных компонентов программы, недоступную через стандартные средства пользовательского интерфейса.
- Изменить настройки 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 настройки, 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 настроек работы программы способами, не описанными в справке 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.

Как создать отчет о состоянии операционной системы

Чтобы создать отчет о состоянии операционной системы, выполните следующие действия:

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

   Откроется окно **Поддержка**.
3. В открывшемся окне по ссылке **Мониторинг проблем** откройте окно **Мониторинг проблем**.
4. В открывшемся окне по ссылке **Как создать отчет об операционной системе** откройте в браузере статью в Базе знаний о том, как создать отчет об операционной системе.
5. Следуйте инструкции, приведенной в статье Базы знаний.

Как отправлять файлы данных

Созданные файлы трассировки и отчет о состоянии операционной системы необходимо отправить специалистам Службы технической поддержки "Лаборатории Касперского".

Чтобы загрузить файлы на сервер Службы технической поддержки, вам понадобится номер запроса. Этот номер доступен на сайте My Kaspersky при наличии активного запроса.

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

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

   Откроется окно **Поддержка "Лаборатории Касперского"**.
3. По ссылке **Мониторинг проблем** откройте окно **Мониторинг проблем**.
4. В открывшемся окне по ссылке **Отправить отчет в Службу технической поддержки** откройте окно **Отправка отчета**.
5. Установите флажки рядом с теми данными, которые вы хотите отправить в Службу технической поддержки.
6. Введите номер запроса, назначенный Службой технической поддержки.
7. Нажмите на кнопку **Отправить отчет**.

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

Если отправить файлы по какой-либо причине невозможно, вы можете сохранить файлы данных на вашем компьютере и впоследствии отправить их с сайта My Kaspersky.

Чтобы сохранить файлы данных на диске, выполните следующие действия:

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

   Откроется окно **Поддержка "Лаборатории Касперского"**.
3. В открывшемся окне по ссылке **Мониторинг проблем** откройте окно **Мониторинг проблем**.
4. В открывшемся окне по ссылке **Отправить отчет в Службу технической поддержки** откройте окно **Отправка отчета**.
5. Выберите типы данных, которые вы хотите сохранить на диске:

   - **Информация об операционной системе**. Установите этот флажок, если вы хотите сохранить на диске информацию об операционной системе вашего компьютера.
   - **Полученные для анализа данные**. Установите этот флажок, если вы хотите сохранить файлы трассировки программы. По ссылке **<количество файлов>, <объем данных>** откройте окно **Полученные для анализа данные**. Установите флажки напротив тех файлов трассировки, которые вы хотите сохранить.
6. По ссылке **Сохранить отчет на компьютере** откройте окно для сохранения архива с файлами данных.
7. Задайте имя архива и подтвердите сохранение.

Созданный архив вы можете отправить в Службу технической поддержки через сайт My Kaspersky.

О составе и хранении служебных файлов данных

Файлы трассировки и дампов хранятся на вашем компьютере в открытом виде в течение семи дней с момента выключения записи данных. По истечении семи дней файлы трассировки и дампов безвозвратно удаляются.

Файлы трассировки хранятся в папке ProgramData\Kaspersky Lab.

Файлы трассировки имеют следующие названия: `KAV<номер версии_dateXX.XX_timeXX.XX_pidXXX.><тип файла трассировки>.log`.

Файлы трассировки могут содержать конфиденциальные данные. Ознакомиться с содержимым файла трассировки вы можете, открыв его в текстовом редакторе (например, "Блокнот").

Ограничения и предупреждения

Kaspersky Anti-Virus имеет ряд некритичных для работы программы ограничений.

Ограничения работы некоторых компонентов и обработки файлов в автоматическом режиме

Обработка зараженных файлов и вредоносных ссылок 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.

Если проверка устройства запускается с сайта My Kaspersky, файлы будут обработаны в автоматическом режиме по правилам, заданным в программе. Обнаруженные на устройстве файлы могут быть обработаны в автоматическом режиме по запросу с сайта My Kaspersky без вашего подтверждения, даже если в программе включена интерактивная защита.

Особенности обработки файлов в интерактивном режиме защиты

Если зараженный файл является частью приложения из Магазина Windows, в интерактивном режиме защиты программа показывает уведомление с предложением удалить такой файл. Действие **Лечить** недоступно.

Ограничения подключения к Kaspersky Security Network

Во время работы программа может обращаться за информацией в Kaspersky Security Network. Если данные из Kaspersky Security Network получить не удалось, программа принимает решения на основании локальных антивирусных баз.

Ограничения функциональности Мониторинга активности

Функциональность противодействия программам-шифровальщикам (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-шифровальщиков не предоставляется. При этом уведомление о невыполнении копирования (непредоставлении защиты) не выводится.

- Временные файлы удаляются автоматически при завершении работы Kaspersky Anti-Virus или отключении компонента Мониторинг активности.

- В случае нештатного завершения работы Kaspersky Anti-Virus 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**.

- Защита от программ-шифровальщиков выполняется только для файлов, расположенных на носителях информации, отформатированных в файловой системе NTFS.

- Количество подлежащих восстановлению файлов не должно превышать 50 на один процесс шифрования.

- Суммарный объем изменений в файлах не должен превышать 100 МБ. Файлы, изменения в которых превышают этот лимит, не подлежат восстановлению.
- Не контролируются изменения файлов, инициированные через сетевой интерфейс.
- Не поддерживаются файлы, зашифрованные системой EFS.
- Для включения защиты от программ-шифровальщиков после установки Kaspersky Anti-Virus требуется перезагрузить компьютер.

Ограничения функциональности проверки защищенных соединений

В связи с техническими ограничениями реализации алгоритмов проверки проверка защищенных соединений не поддерживает некоторые расширения протокола TLS 1.0 и выше (в частности NPN и ALPN). Подключение по этим протоколам может быть ограничено. Браузеры с поддержкой протокола SPDY используют вместо SPDY протокол HTTP поверх TLS, даже если сервер, к которому выполняется подключение, поддерживает SPDY. При этом уровень защиты соединения не снижается. Если сервер поддерживает только протокол SPDY и возможность установить соединение с помощью протокола HTTPS отсутствует, программа не будет контролировать установленное соединение.

Программа Kaspersky Anti-Virus не поддерживает обработку трафика, передаваемого через HTTPS/2 Proxy. Также программа не обрабатывает трафик, передаваемый через расширения протокола HTTP/2.

Программа Kaspersky Anti-Virus препятствует обмену данными по протоколу QUIC. Браузеры используют стандартный транспортный протокол (TLS или SSL) независимо от того, включена в браузере поддержка протокола QUIC или нет.

Программа Kaspersky Anti-Virus контролирует только те защищенные соединения, которые она может расшифровать. Программа не контролирует соединения, добавленные в список исключений (ссылка **Сайты** в окне **Настройки сети**). Проверка и расшифровка зашифрованного трафика по умолчанию выполняется следующими компонентами:

- Веб-Антивирус;
- Проверка ссылок.

Kaspersky Anti-Virus расшифровывает зашифрованный трафик при работе пользователя в браузере Google Chrome, если в этом браузере отсутствует или выключено расширение Kaspersky Protection.

Kaspersky Anti-Virus не контролирует трафик, если браузер загружает веб-страницу или ее элементы из локального кеша, а не из интернета.

Ограничения исключений из проверки защищенных соединений

При проверке защищенных соединений с сайтами, добавленными в исключения, компонент Проверка ссылок может продолжать проверять защищенные соединения. Компонент Веб-Антивирус не проверяет сайты, добавленные в исключения.

Особенности обработки зараженных файлов компонентами программы

Kaspersky Anti-Virus по умолчанию может удалять зараженные файлы, если их лечение невозможно. Удаление по умолчанию может выполняться при обработке файлов такими компонентами, как Почтовый Антивирус, Файловый Антивирус, при выполнении задач проверки, а также при обнаружении опасной активности программ компонентом Мониторинг активности.

Предупреждение об изменении функциональности IM-Антивируса

Начиная с версии Kaspersky Anti-Virus 2016 компонент IM-Антивирус не проверяет сообщения, переданные по протоколу IRC.

IM-Антивирус поддерживает работу только со следующими версиями ICQ: ICQ 8 – ICQ 8.3. Более поздние версии не поддерживаются.

IM-Антивирус поддерживает работу с Mail.ru Агент только версий ниже 10.

Особенности работы процесса autorun

Процесс autorun выполняет запись результатов своей работы. Данные сохраняются в текстовые файлы с названием вида “kl-autorun-<date><time>.log”. Чтобы просмотреть данные, требуется открыть окно **Выполнить** (**Запуск программы** в Windows XP), в поле **Открыть** ввести %TEMP% и нажать на кнопку **OK**.

В файлы трассировки сохраняются пути к файлам установки, загруженным в ходе использования autorun. Данные хранятся в течение работы процесса autorun и безвозвратно удаляются при завершении этого процесса. Данные никуда не отправляются.

Ограничения работы Kaspersky Anti-Virus при включенном режиме Device Guard на Microsoft Windows 10 RS4

Частично ограничена работа следующей функциональности:

- защита буфера обмена;
- защита браузера от программ эмуляции ввода с клавиатуры и мыши (подмен вводимых данных);
- защита от программ удаленного управления;
- защита браузера (управление через API, защита от атак при помощи опасных сообщений окнам браузера, защита от управления очередью сообщений);
- эвристический анализ (эмуляция запуска вредоносных программ).

Если в операционной системе Windows включен режим работы UMCI, Kaspersky Anti-Virus не обнаруживает программы блокировки экрана.

О записи событий, касающихся Лицензионного соглашения и Kaspersky Security Network, в журнал событий Windows

События принятия или отказа от условий Лицензионного соглашения, а также принятия или отказа от участия в Kaspersky Security Network записываются в журнал Windows.

Ограничения проверки репутации локальных адресов в Kaspersky Security Network

Ссылки, ведущие на локальные ресурсы, не проверяются в Kaspersky Security Network.

Предупреждение о программах сбора информации

Если у вас на компьютере установлена программа, выполняющая сбор и отправку информации на обработку, Kaspersky Anti-Virus может классифицировать такую программу как вредоносную. Чтобы избежать этого, вы можете исключить программу из проверки, настроив Kaspersky Anti-Virus способом, описанным в этом документе.

Предупреждение о создании отчета об установке программы

При установке программы на компьютер создается файл отчета об установке. Если установка программы завершилась с ошибкой, файл отчета об установке сохраняется, и вы можете отправить его в Службу поддержки "Лаборатории Касперского". Вы можете ознакомиться с содержимым файла отчета об установке по ссылке из окна программы. В случае успешной установки программы файл отчета об установке сразу же удаляется с вашего компьютера.

Ограничение первого запуска программы после обновления операционной системы Microsoft Windows 7 до Microsoft Windows 10

Если вы обновили операционную систему Microsoft Windows 7 до Microsoft Windows 8 / 8.1 или Microsoft Windows 10 / RS1 / RS2 / RS3, при первом запуске Kaspersky Anti-Virus работает со следующими ограничениями:

- Работает только Файловый Антивирус (постоянная защита). Остальные компоненты программы не работают.
- Работает самозащита файлов и системного реестра. Самозащита процессов не работает.
- Интерфейс программы недоступен до перезагрузки компьютера. Программа показывает уведомление о том, что некоторые компоненты программы не работают, и о том, что требуется перезагрузка компьютера после завершения адаптации к новой операционной системе.
- В контекстном меню значка в области уведомлений доступен только пункт **Выход**.
- Программа не показывает уведомления и автоматически выбирает рекомендованное действие.

Предупреждение об ошибке адаптации драйверов программы при обновлении операционной системы с Windows 7 до Windows 10

При обновлении Windows с версии 7 до версии 10 может произойти ошибка адаптации драйверов Kaspersky Anti-Virus. Адаптация драйверов происходит в фоновом режиме, вы не получаете оповещений о ее процессе.

В случае возникновения ошибки адаптации драйверов вы не сможете воспользоваться следующими функциями программы:

- функцией обнаружения угроз во время загрузки операционной системы;

- функцией защиты процессов программы с помощью технологии Protected Process Light (PPL) от Microsoft.

Вы можете воспользоваться следующими способами исправления ошибки:

- перезагрузить компьютер и повторить адаптацию программы из оповещения в Центре уведомлений;
- удалить и заново установить программу.

Ограничения проверки трафика, передаваемого по протоколу HTTPS, в браузере Mozilla Firefox

В версиях Mozilla Firefox 58.x и выше программа не проверяет трафик, передаваемый по протоколу HTTPS, если изменение настроек браузера защищено мастер-паролем. При обнаружении мастер-пароля в браузере, программа показывает уведомление, в котором содержится ссылка на статью в Базе знаний. Статья содержит инструкцию для решения этой проблемы.

Если трафик, передаваемый по протоколу HTTPS, не контролируется, ограничена работа следующих компонентов:

- Веб-Антивирус;
- Анти-Фишинг;
- Защита ввода данных.

Ограничения работы расширения Kaspersky Protection в браузерах Google Chrome и Mozilla Firefox

Расширение Kaspersky Protection не работает в браузерах Google Chrome и Mozilla Firefox, если на вашем компьютере установлена программа Malwarebytes for Windows.

Особенности установки программы на операционной системе Microsoft Windows 7 Service Pack 0 и Service Pack 1

При установке программы на операционные системы, которые не поддерживают сертификаты с цифровой подписью SHA256, программа устанавливает свой доверенный сертификат.

Другие источники информации о программе

Страница Kaspersky Anti-Virus в Базе знаний

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

На странице Kaspersky Anti-Virus в Базе знаний вы найдете статьи, которые содержат полезную информацию, рекомендации и ответы на часто задаваемые вопросы о приобретении, установке и использовании программы.

Статьи Базы знаний могут отвечать на вопросы, которые относятся не только к Kaspersky Anti-Virus, но и к другим программам "Лаборатории Касперского". Статьи Базы знаний также могут содержать новости Службы технической поддержки.

Обсуждение программ "Лаборатории Касперского" в нашем сообществе

Если ваш вопрос не требует срочного ответа, вы можете обсудить его со специалистами "Лаборатории Касперского" и с другими пользователями в нашем сообществе.

В сообществе вы можете просматривать опубликованные темы, добавлять свои комментарии, создавать новые темы для обсуждения.

Глоссарий

Kaspersky Security Network (KSN)

Облачная база знаний "Лаборатории Касперского", которая содержит информацию о репутации программ и сайтов. Использование данных Kaspersky Security Network обеспечивает более высокую скорость реакции программ "Лаборатории Касперского" на угрозы, повышает эффективность работы некоторых компонентов защиты, а также снижает вероятность ложных срабатываний.

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.

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.

Вирус

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

Вирусная атака

Ряд целенаправленных попыток заразить устройство вирусом.

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).

Группа доверия

Группа, в которую Kaspersky Anti-Virus 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 Anti-Virus может накладывать ограничения на действия этой программы в операционной системе.

В Kaspersky Anti-Virus используются следующие группы доверия: "Доверенные", "Слабые ограничения", "Сильные ограничения", "Недоверенные".

Доверенный процесс

Программный процесс, файловые операции которого не контролируются программой "Лаборатории Касперского" в режиме постоянной защиты. При обнаружении подозрительной активности доверенного процесса Kaspersky Anti-Virus исключает этот процесс из списка доверенных и блокирует его действия.

Доступное обновление

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

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.

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 шпион

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

Код активации

Код, который вы получаете, приобретая лицензию на использование Kaspersky Anti-Virus. 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 Anti-Virus, предназначенные для защиты компьютера от отдельных типов угроз (например, Анти-Фишинг). Каждый компонент защиты относительно независим от других компонентов и может быть отключен или настроен отдельно.

Ложное срабатывание

Ситуация, когда незараженный объект определяется программой "Лаборатории Касперского" как зараженный из-за того, что его код напоминает код вируса.

Маска файла

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

Настройки задачи

Настройки работы программы, специфичные для каждого типа задач.

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 Anti-Virus.

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.

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.

Потенциально заражаемый файл

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

Проверка трафика

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

Программные модули

Файлы, входящие в состав 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.

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").

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 сайты.

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

Спам

Несанкционированная массовая рассылка сообщений электронной почты, чаще всего рекламного характера.

Срок действия лицензии

Период времени, в течение которого вы можете пользоваться функциями программы и дополнительными услугами.

Степень угрозы

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

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

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

Технология iChecker

Технология, позволяющая увеличить скорость антивирусной проверки за счет исключения тех объектов, которые не были изменены с момента предыдущей проверки, при условии, что настройки 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 настройки проверки. Если вы изменили состав архива, добавив в него новый объект, изменили настройки 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.

Упакованный файл

Исполняемый файл в сжатом виде, который содержит в себе программу-распаковщик и инструкции операционной системе для ее выполнения.

Уровень безопасности

Под уровнем безопасности понимается предустановленный набор настроек 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.

Фишинг

Вид интернет-мошенничества, заключающийся в рассылке сообщений электронной почты с целью кражи конфиденциальных данных, как правило, финансового характера.

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.

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).

Эксплойт

Программный код, который использует какую-либо уязвимость в системе или программном обеспечении. Эксплойты часто используются для установки вредоносного программного обеспечения на компьютере без ведома пользователя.

АО "Лаборатория Касперского"

"Лаборатория Касперского" – известный в мире производитель систем компьютерной защиты от различных видов угроз, включая защиту от вирусов и других вредоносных программ, нежелательной почты (спама), сетевых и хакерских атак.

В 2008 году "Лаборатория Касперского" вошла в четверку мировых лидеров рынка программных решений для обеспечения информационной безопасности конечных пользователей (рейтинг "IDC Worldwide Endpoint Security Revenue by Vendor"). В России, по данным IDC, "Лаборатория Касперского" – самый предпочитаемый производитель систем компьютерной защиты для домашних пользователей ("IDC Endpoint Tracker 2014").

"Лаборатория Касперского" основана в России в 1997 году. Сегодня "Лаборатория Касперского" – это международная группа компаний с 38 офисами в 33 странах мира. В компании работает более 3000 квалифицированных специалистов.

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

Линейка персональных продуктов включает программы, обеспечивающие информационную безопасность настольных компьютеров и ноутбуков, планшетных компьютеров, смартфонов и других мобильных устройств.

Компания предлагает решения и технологии для защиты и контроля рабочих станций и мобильных устройств, виртуальных машин, файловых и веб-серверов, почтовых шлюзов, сетевых экранов. Также в портфеле компании есть специализированные продукты для защиты от DDoS-атак, защиты сред под управлением АСУТП и предотвращения финансового мошенничества. Использование этих решений в сочетании с централизованными средствами управления позволяет построить и эксплуатировать эффективную автоматизированную защиту организации любого размера от компьютерных угроз. Продукты "Лаборатории Касперского" сертифицированы крупными тестовыми лабораториями, совместимы с программным обеспечением многих поставщиков программного обеспечения и оптимизированы для работы на многих аппаратных платформах.

Вирусные аналитики "Лаборатории Касперского" работают круглосуточно. Каждый день они находят сотни тысяч новых компьютерных угроз, создают средства их обнаружения и лечения и включают сигнатуры этих угроз в базы, используемые программами "Лаборатории Касперского".

Технологии. Многие технологии, без которых трудно представить себе современный антивирус, впервые разработаны именно "Лабораторией Касперского". Не случайно программное ядро Антивируса Касперского используют в своих продуктах многие другие разработчики программного обеспечения, среди них: Alcatel-Lucent, Alt-N, Asus, BAE Systems, Blue Coat, Check Point, Cisco Meraki, Clearswift, D-Link, Facebook, General Dynamics, H3C, Juniper Networks, Lenovo, Microsoft, NETGEAR, Openwave Messaging, Parallels, Qualcomm, Samsung, Stormshield, Toshiba, Trustwave, Vertu, ZyXEL. Многие из инновационных технологий компании подтверждены патентами.

Достижения. За годы борьбы с компьютерными угрозами "Лаборатория Касперского" завоевала сотни наград. Например, в 2014 году по итогам испытаний и исследований, проведенных авторитетной австрийской антивирусной лабораторией AV-Comparatives, "Лаборатория Касперского" стала одним из двух лидеров по количеству полученных сертификатов Advanced+, в результате компания была удостоена сертификата Top Rated. Но главная награда "Лаборатории Касперского" – это приверженность пользователей по всему миру. Продукты и технологии компании защищают более 400 миллионов пользователей. Количество организаций, являющихся ее клиентами, превышает 270 тысяч.

Сайт "Лаборатории Касперского":	https://www.kaspersky.ru
Вирусная энциклопедия:	https://securelist.ru/
Kaspersky VirusDesk:	https://virusdesk.kaspersky.ru/ (для проверки подозрительных файлов и сайтов)

Сообщество пользователей "Лаборатории Касперского":	https://community.kaspersky.com

Информация о стороннем коде

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

Уведомления о товарных знаках

Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.

Dropbox – товарный знак Dropbox, Inc.

Google, Google Chrome, Google Talk, Chrome, SPDY, YouTube, Android – 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.

JABBER – зарегистрированный товарный знак и его использование лицензируется XMPP Standards Foundation.

Mail.Ru – зарегистрированный товарный знак, правообладателем которого является ООО "Мэйл.Ру".

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

Mozilla, Thunderbird и Firefox – товарные знаки Mozilla Foundation.

VMware – товарный знак VMware, Inc. или зарегистрированный в США или других юрисдикциях товарный знак VMware, Inc.

iOS – зарегистрированный в Соединенных Штатах Америки и в других странах товарный знак Cisco Systems, Inc. и / или ее аффилированных компаний.

История вызова модулей программ

Вид

В раскрывающемся списке можно выбрать следующие варианты фильтрации записей:

- **Показывать разрешенные вручную**. В списке отображаются модули, запуск которых был разрешен вручную.
- **Скрывать разрешенные вручную**. В списке не отображаются модули, запуск которых был разрешен вручную.
- **Сбросить все изменения, внесенные вручную**. Для всех модулей, запуск которых вы разрешили, сбрасываются настройки запуска, и программа определяет, запускать или нет эти модули, по информации из Kaspersky Security Network.

Список заблокированных модулей

Во время работы программы Kaspersky Anti-Virus может заблокировать запуск модулей, которые не являются доверенными. Список содержит информацию о модулях программ, вызов которых был заблокирован или разблокирован. Сведения о блокировке / разблокировании вызова модулей располагаются в хронологическом порядке.

Вызов заблокированных модулей программ можно разрешить вручную и, при необходимости, снова заблокировать с помощью переключателей в правой части списка.

Программа

В графе отображаются сведения о модулях программ, вызов которых был заблокирован или разрешен.

При нажатии на кнопку ▶ в строке списка отображаются вложенные строки с информацией о названиях заблокированных или разблокированных модулей программ.

При нажатии на кнопку ◢ строки с информацией о названиях модулей программ сворачиваются в одну строку.

Папка

В графе отображается путь к папке, в которой расположен файл модуля программы.

Время запуска

В графе отображаются дата и время блокировки или разблокирования модуля программой.

Статус запуска

В графе отображается статус модуля программы: заблокирован / разблокирован.

Переключатели

В графе отображаются переключатели, которые позволяют заблокировать / разблокировать вызов отдельных модулей программ или группы модулей.

Контекстное меню

По правой клавише мыши на строке с названием модуля программы отображается контекстное меню, в котором доступны следующие пункты:

- **Разрешить запуск**. Если выбран этот пункт, модулю программы разрешены все действия.
- **Запретить запуск**. Если выбран этот пункт, модулю программы запрещены все действия.
- **Уведомления**. Для выбора доступны два варианта работы с уведомлениями:
  - **Показывать уведомления о блокировке**. Если выбран этот вариант, Kaspersky Anti-Virus показывает уведомления о блокировке выбранного модуля.
  - **Не показывать уведомления о блокировке**. Если выбран этот пункт, Kaspersky Anti-Virus не показывает уведомления о блокировке выбранного модуля.
  - **Открыть папку**. Если выбран этот пункт, открывается папка, в которой расположен файл модуля программы.

Если выбрано несколько записей, контекстное меню включает следующие пункты:

- **Разрешить выбранные**. Если выбран этот пункт, блокировка снимается со всех выбранных модулей программ.
- **Блокировать выбранные**. Если выбран этот пункт, блокировка устанавливается для всех выбранных модулей программ.
- **Показывать уведомления о блокировке**. Если выбран этот пункт, Kaspersky Anti-Virus показывает уведомления о блокировке выбранных модулей.
- **Не показывать уведомления о блокировке**. Если выбран этот пункт, Kaspersky Anti-Virus не показывает уведомления о блокировке выбранных модулей.

Окно Расширение защиты

Пробная версия

Кнопка, при нажатии на которую запускается переход с Kaspersky Anti-Virus на пробную версию Kaspersky Internet Security.

Купить код активации

По ссылке открывается окно браузера на странице интернет-магазина, в котором вы можете приобрести лицензию Kaspersky Internet Security.

Ввести код активации

По ссылке запускается мастер активации Kaspersky Internet Security.

Окно Расширение защиты

Купить код активации

По ссылке открывается окно браузера на странице интернет-магазина, в котором вы можете приобрести код активации Kaspersky Total Security.

Ввести код активации

По ссылке запускается мастер активации Kaspersky Total Security.

Пробная версия

Кнопка, при нажатии на которую запускается переход с Kaspersky Anti-Virus на пробную версию Kaspersky Total Security.

Активация с помощью резервного кода активации

После нажатия на кнопку **Далее** будет применен резервный код активации.

Если срок действия лицензии еще не истек, вы можете применить код активации, с помощью которого программа была активирована ранее, на другом компьютере.

По ссылке **Отмена** вы можете отменить активацию программы.

Отмена

По ссылке вы можете отменить применение резервного кода активации и вернуться к окну **Лицензирование**.

Окно Ввод кода активации

Код активации

Поля для ввода кода активации программы. Код активации состоит из четырех групп символов (например, **ABA9C-CDEFG-ABCBC-ABC2D**). Первую группу символов нужно ввести в первое поле ввода, вторую группу – во второе и так далее.

По ссылке **Где найти код активации?** открывается окно браузера на сайте Службы технической поддержки с подробной информацией о коде активации.

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

Активировать пробную версию программы

По ссылке выполняется активация пробной версии программы. Вы сможете использовать пробную версию программы в течение короткого ознакомительного периода в режиме полной функциональности. По истечении срока действия лицензии повторная активация пробной версии программы невозможна.

Этот вариант доступен, если пробная версия программы еще не использовалась.

Купить лицензию

По ссылке открывается окно браузера на странице интернет-магазина, в котором вы можете приобрести лицензию.

Код активации нельзя сделать резервным

Окно отображается, если введенный код активации не может быть указан в качестве резервного. Это может произойти, если введен код активации для подписки. В этом случае введенный код активации можно использовать для немедленной активации Kaspersky Anti-Virus.

Код активации, примененный ранее, можно повторно применить на другом компьютере до истечения срока действия лицензии.

Применить введенный код активации сейчас

Если флажок установлен, при нажатии на кнопку **Продолжить** введенный код активации будет применен для активации Kaspersky Anti-Virus. Код активации, примененный ранее, можно повторно применить на другом компьютере.

Кнопка **Продолжить** не доступна, если флажок снят.

Код активации соответствует другой программе

Это окно отображается, если введенный код активации соответствует другой программе. Название программы указано в строке **Соответствующая программа**. Вы можете перейти к использованию этой программы сейчас или после истечения срока действия лицензии на Kaspersky Anti-Virus.

Отмена

По ссылке вы можете отменить активацию программы.

Продолжить

При нажатии на кнопку запускается установка и активация той программы, которой соответствует введенный вами код активации.

Окно Найдена информация о действующей лицензии

Да, использовать <программа>

При выборе этого варианта работа мастера активации завершается. Программа будет работать по обнаруженной действующей лицензии. Если обнаружена лицензия на Kaspersky Internet Security или Kaspersky Total Security, будет запущен мастер миграции.

Нет, продолжить работу мастера и ввести новый код активации

При выборе этого варианта мастер активации продолжает работу и активирует Kaspersky Anti-Virus. Вам потребуется ввести новый код активации, соответствующий Kaspersky Anti-Virus.

Окно Регистрация

В этом окне нужно указать регистрационные данные, которые понадобятся в случае обращения в Службу технической поддержки.

Отсутствует соединение с интернетом

Это окно отображается, если попытка активировать программу не удалась из-за проблем с подключением к интернету.

Повторить попытку

По ссылке мастер активации пытается активировать программу повторно. Если проблемы с интернетом краткосрочные, то повторная попытка может оказаться успешной.

Ошибка активации

Не удалось активировать программу. По ссылке **Причины и возможные решения** вы можете просмотреть информацию о проблеме в базе знаний.

Причины и возможные решения

По ссылке вы можете перейти к статье базы знаний с информацией о причинах ошибки и возможных решениях.

Для некоторых ошибок ссылка на статью в базе знаний может отсутствовать.

Отмена

По ссылке вы можете отменить активацию программы.

Переход к использованию другой программы

После нажатия на кнопку **Далее** будет запущен мастер миграции. В результате работы мастера миграции будет установлена программа, соответствующая введенному коду активации (Kaspersky Internet Security или Kaspersky Total Security).

Если срок действия лицензии на Kaspersky Anti-Virus еще не истек, вы можете применить код активации Kaspersky Anti-Virus на другом компьютере.

По ссылке **Отмена** вы можете отменить переход на Kaspersky Internet Security или Kaspersky Total Security.

Отмена

По ссылке можно отменить запуск мастера миграции и вернуться к предыдущему шагу.

Убедитесь, что введенный код активации не является кодом активации для подписки

Убедитесь, что код активации, который вы указываете в качестве резервного, не предназначен для использования программы по подписке. Оплата за использование программы по подписке взимается с момента оформления подписки. Если вы оформили подписку на Kaspersky Anti-Virus, откажитесь от использования программы по действующей лицензии и активируйте программу с помощью кода активации для подписки.

Вы можете применить код активации, с помощью которого программа была активирована ранее, на другом компьютере до истечения срока действия лицензии.

Окно Последовательность запуска

Последовательность запуска программ

В списке содержится информация о программах, запущенных выбранной программой (дочерних программах). По умолчанию дочерние программы отсортированы по времени запуска, начиная с самого раннего.

Запуск

В графе отображается время запуска дочерней программы.

ID процесса

В графе отображается идентификатор процесса дочерней программы.

Программа

В графе отображается название дочерней программы.

Группа доверия

В графе отображается группа доверия, в которую входит программа:

- **Доверенные**. Программа работает без ограничений, но контролируется компонентом Файловый Антивирус.
- **Слабые ограничения**. Программе запрещено обращаться к конфиденциальным данным и настройкам пользователя, изменять публичные данные. При попытке изменения системных данных и выполнения привилегированных операций запрашивается разрешение пользователя. Сетевая активность такой программы ограничена.
- **Сильные ограничения**. Программе запрещено обращаться к конфиденциальным данным и настройкам пользователя, публичным и системным данным. При попытке выполнения привилегированных операций запрашивается разрешение пользователя. Сетевая активность такой программы заблокирована.
- **Недоверенные**. Работа такой программы полностью блокируется.

Закладка Работающие

Список работающих программ

В списке отображаются программы и процессы, выполняемые на вашем компьютере в настоящее время.

По правой клавише мыши можно открыть контекстное меню заголовка любой графы. С помощью контекстного меню можно настроить отображение граф с дополнительной информацией о программах и процессах:

- название исполняемого файла программы или процесса;
- сведения о производителе программы;
- идентификатор процесса;
- расположение исполняемого файла программы;
- имя пользователя, запустившего программу или процесс;
- время создания и запуска программы или процесса;
- настройки автозапуска программы.

С помощью пункта **Упорядочить столбцы по умолчанию** можно восстановить исходный вид таблицы.

По правой клавише мыши на строке программы или процесса открывается контекстное меню. Из контекстного меню можно выполнить следующие действия:

- открыть окно **Правила программы**, в котором можно настроить правила для контроля действий программы;
- отобразить последовательность запуска процессов в окне **Последовательность запуска**;
- переместить программу в другую группу доверия;
- установить для программы настройки контроля активности, предусмотренные по умолчанию;
- завершить процесс;
- открыть папку, в которой расположен исполняемый файл программы.

Вид

В раскрывающемся списке можно включить отображение системных процессов и процессов Kaspersky Anti-Virus:

- **Показывать системные процессы**. При выборе этого элемента в общем списке программ и процессов отображаются процессы, необходимые для работы операционной системы.
- **Показывать процессы Kaspersky Anti-Virus**. При выборе этого элемента в общем списке программ и процессов отображаются процессы, запущенные Kaspersky Anti-Virus.

В раскрывающемся списке также можно выбрать способ отображения программ и процессов:

- **Показывать как список**. При выборе этого варианта программы / процессы отображаются в виде списка.
- **Показывать как дерево**. При выборе этого варианта программы / процессы отображаются в виде иерархической структуры в соответствии с последовательностью вызова процессов.

Программа

В графе отображается название программы или процесса.

Цифровая подпись

В графе отображается информация о наличии цифровой подписи у программы и владельце цифровой подписи.

Группа доверия

В графе отображается группа доверия, в которую помещена программа. В зависимости от группы доверия программы в графе отображаются следующие значки:

- Красный значок означает, что программа находится в группе "Недоверенные".
- Розовый значок означает, что программа находится в группе "Сильные ограничения".
- Желтый значок означает, что программа находится в группе "Слабые ограничения".
- Зеленый значок означает, что программа находится в группе "Доверенные".

Популярность

В графе отображается уровень популярности программы среди участников Kaspersky Security Network (KSN). Уровень популярности соответствует числу участников KSN, использующих программу.

Процессор

В графе отображается текущее потребление ресурсов центрального процессора программой / процессом.

Память

В графе отображается текущее потребление оперативной памяти программой / процессом.

Диск

В графе отображается суммарная скорость чтения и записи данных на диск программой или процессом.

Сеть

В графе отображается суммарная скорость приема и передачи данных программой через сетевой интерфейс.

Завершить процесс

При нажатии на кнопку завершается работа программы, выбранной в списке.

Закладка Запускаемые при старте

Список программ, запускаемых при старте

Список содержит программы, которые запускаются при старте операционной системы.

По правой клавише мыши можно открыть контекстное меню заголовка любой графы. С помощью контекстного меню можно настроить отображение граф в таблице. С помощью пункта **Упорядочить столбцы по умолчанию** можно восстановить исходный вид таблицы.

По правой клавише мыши на строке программы или процесса открывается контекстное меню. Из контекстного меню можно выполнить следующие действия:

- открыть окно **Правила программы**, в котором можно настроить правила для контроля действий программы;
- переместить программу в другую группу доверия;
- установить для программы настройки контроля активности, предусмотренные по умолчанию;
- открыть папку, в которой расположен исполняемый файл программы.

Программа

В графе отображается название программы, запускаемой при старте операционной системы.

Статус

В графе отображается состояние программы: *Выполняется* или *Закрыта*.

Цифровая подпись

В графе отображается информация о наличии цифровой подписи у программы и владельце цифровой подписи.

Группа доверия

В графе отображается группа доверия, в которую помещена программа. В зависимости от группы доверия программы в графе отображаются следующие значки:

- Красный значок означает, что программа находится в группе "Недоверенные".
- Розовый значок означает, что программа находится в группе "Сильные ограничения".
- Желтый значок означает, что программа находится в группе "Слабые ограничения".
- Зеленый значок означает, что программа находится в группе "Доверенные".

Популярность

В графе отображается уровень популярности программы среди участников Kaspersky Security Network (KSN). Уровень популярности соответствует числу участников KSN, использующих программу.

Последний запуск

В графе отображается время последнего запуска программы.

Закладка Все программы

Список программ

В списке содержатся программы, установленные на вашем компьютере. Для каждой программы в списке отображается информация о статусе, цифровой подписи, группе доверия, популярности программы среди пользователей KSN и времени последнего запуска.

По двойному щелчку мышью на строке программы или процесса открывается окно **Правила программы**. В окне можно настроить правила для контроля действий программы.

По правой клавише мыши на строке программы открывается контекстное меню. В контекстном меню можно выполнить следующие действия:

- открыть окно **Правила программы**, в котором можно настроить разрешения для действий программы;
- разрешить или запретить запуск программы;
- переместить программу в другую группу доверия;
- установить для программы настройки контроля активности, предусмотренные по умолчанию (сбросить настройки программы);
- удалить программу из списка;
- открыть папку, содержащую исполняемый файл программы.

Программы в списке объединены в группы и подгруппы. По правой клавише мыши на строке группы открывается контекстное меню. В контекстном меню можно выполнить следующие действия:

- открыть окно **Правила группы**, в котором можно настроить разрешения для действий программ из этой группы, используемые по умолчанию;
- создать подгруппу внутри группы; по умолчанию к подгруппе применяются правила, указанные для группы, в которую она входит;
- добавить программу в группу; по умолчанию к программе применяются правила, указанные для группы, в которую она входит;
- установить для группы и всех входящих в нее подгрупп и программ настройки контроля активности, предусмотренные по умолчанию (сбросить настройки группы);
- установить для подгрупп и программ, входящих в группу, настройки контроля активности, предусмотренные по умолчанию, оставив настройки группы без изменений (сбросить настройки подгрупп и программ);
- удалить входящие в группу подгруппы и программы.

Программа

В графе отображается название программы.

Статус

В графе отображается состояние программы: *Выполняется* или *Закрыта*.

Цифровая подпись

В графе отображается информация о наличии цифровой подписи у программы и владельце цифровой подписи.

Группа доверия

В графе отображается группа доверия, в которую помещена программа. Группа доверия определяет правила использования программы на компьютере: запрет или разрешение запуска, доступ программы к файлам и системному реестру, ограничения сетевой активности программы.

Популярность

В графе отображается уровень популярности программы среди участников Kaspersky Security Network (KSN). Уровень популярности соответствует числу участников KSN, использующих программу.

Последний запуск

В графе отображается время последнего запуска программы.

Окно Нецензурные слова

Соглашение

Содержит условие, в соответствии с которым вы можете внести изменения в список нецензурных фраз.

Я достиг совершеннолетия и согласен с этими условиями

Установка флажка означает согласие с условиями, изложенными в соглашении. Если флажок установлен, список нецензурных фраз доступен для редактирования.

Если флажок снят, список нецензурных фраз недоступен для редактирования.

Окно Отправить отзыв

Проблема

Раскрывающийся список, где вы можете выбрать категорию, к которой относится ваш отзыв. Категория отзыва может затрагивать проблему с сайтом, открытым в Защищенном браузере:

- **Не использую**. Выберите этот элемент, если вы не используете или решили отказаться от использования Безопасных платежей.
- **Медленно открывается сайт**. Выберите этот элемент, если сайт работает медленнее, чем в браузере, запущенном в обычном режиме.
- **Защищенный браузер запускается не тогда, когда нужно**. Выберите этот элемент, если в Защищенном браузере открываются сайты, не требующие использования Безопасных платежей.
- **Не получается авторизоваться на сайте**. Выберите этот элемент, если при попытках авторизоваться на сайте, открытом в Защищенном браузере, возникают ошибки.
- **Не открывается или неправильно отображается сайт**. Выберите этот элемент, если сайты не открываются в Защищенном браузере или отображаются с ошибками / искажениями.
- **Сертификаты сайта проверяются с ошибками**. Выберите этот элемент, если при проверке сертификатов сайта появляются сообщения об ошибках.
- **Невозможно сделать снимок экрана, если запущен Защищенный браузер**. Выберите этот элемент, если в Защищенном браузере не создаются скриншоты.
- **Ошибки во время ввода данных с клавиатуры или из буфера обмена**. Выберите этот элемент, если во время ввода данных в Защищенном браузере возникают ошибки.
- **Не печатается страница, открытая в Защищенном браузере**. Выберите этот элемент, если вы не можете распечатать открытую страницу сайта.
- **Появляется предупреждение о том, что не установлены важные обновления операционной системы**. Выберите этот элемент, если при запуске Защищенного браузера появляется сообщение "Не установлены важные обновления операционной системы".
- **В качестве Защищенного запускается другой браузер**. Выберите этот элемент, если Защищенный браузер открывается не в том браузере, в котором вы его запустили.
- **Работает с ошибками**. Выберите этот элемент, если в работе Защищенного браузера возникают ошибки, не указанные в списке.
- **Другое**. Выберите этот элемент, если ваша проблема не относится к указанным в других пунктах.

Указывать категорию отзыва не обязательно.

Подробнее

В поле вы можете указать информацию, которая поможет сотрудникам "Лаборатории Касперского" решить вашу проблему. Заполнять поле необязательно.

Отправить

Отправка отзыва в "Лабораторию Касперского".

Вы можете отправить до 10 отзывов о работе с Безопасными платежами в сутки. Если программе не удается отправить отзыв (например, отсутствует соединение с интернетом), программа сохраняет отзыв на вашем компьютере. Отзывы хранятся в открытом виде в течение 30 дней.

Окно Защита данных с помощью шифрования

Создать новый сейф

При нажатии на кнопку открывается окно, в котором вы можете поместить файлы и папки в создаваемый сейф.

Кнопка **Создать новый сейф** отображается, если у вас еще нет сейфа.

У меня уже есть сейф

По ссылке открывается окно **Выбор файла сейфа**. В окне вы можете выбрать для подключения сейф, созданный ранее.

Поиск повреждений / Поиск изменений

В этом окне отображается процесс поиска повреждений в операционной системе или процесс анализа изменений, выполненных ранее мастером восстановления после заражения.

Процесс может занять некоторое время. Можно прервать процесс, нажав на кнопку **Отмена**.

Восстановление после заражения

Выполнить поиск повреждений, связанных с активностью вредоносных программ

Kaspersky Anti-Virus начинает в операционной системе поиск повреждений, связанных с активностью вредоносных программ.

Отменить изменения

Kaspersky Anti-Virus отменяет изменения, которые были сделаны в результате предыдущей работы мастера.

Этот вариант действия доступен, если во время предыдущей работы мастера были выполнены действия, направленные на устранение обнаруженных повреждений.

Поиск повреждений завершен / Поиск изменений завершен

Список повреждений

Список содержит найденные повреждения операционной системы. Найденные повреждения Kaspersky Anti-Virus группирует с точки зрения опасности, которую они представляют:

- *Повреждения, которые настоятельно рекомендуется устранить.* Критические повреждения операционной системы, которые представляют серьезную угрозу безопасности компьютера.
- *Повреждения, которые рекомендуется устранить.* Повреждения операционной системы, которые угрожают безопасности компьютера в данный момент.
- *Повреждения, которые можно устранить.* Повреждения операционной системы, которые в данный момент не опасны, но могут угрожать безопасности компьютера в дальнейшем.

Если флажок в строке с названием повреждения установлен, Kaspersky Anti-Virus пытается устранить повреждение.

Если флажок в строке с названием повреждения снят, Kaspersky Anti-Virus не устраняет повреждение.

Если на первом шаге был выбран вариант **Отменить изменения**, в списке содержатся устраненные ранее повреждения. Вы можете отменить действия, выполненные для устранения этих повреждений.

Устранение повреждений / Отмена изменений

В этом окне отображается процесс устранения повреждений операционной системы, обнаруженных в ходе анализа. Устранение повреждений может занять некоторое время.

Если на первом шаге был выбран вариант **Отменить изменения**, мастер восстановления после заражения выполняет откат действий, выбранных на предыдущем шаге.

Завершение работы

Перезагрузить компьютер

Если флажок установлен, компьютер перезагружается после завершения работы мастера.

Готово

Кнопка, при нажатии на которую Kaspersky Anti-Virus завершает работу мастера восстановления системы.

Доверенные программы

В окне отображается список программ, которые установлены на вашем компьютере.

Чтобы добавить нужную вам программу в исключения, выполните следующие действия:

1. Выберите программу из списка. Если в списке не отображается нужная вам программа, нажмите на кнопку **Обзор** и добавьте программу вручную.

2. Нажмите на кнопку **Далее**.

   Будет выполнен переход в окно **Исключения для программы**, в котором вы можете настроить правила исключения для выбранной программы.

Окно Информация о лицензии

В окне содержится информация о лицензии на программу:

- Лицензионный ключ.
- Статус лицензии.
- Количество компьютеров, на которые распространяется лицензия.
- Дата активации.
- Дата окончания срока действия лицензии.
- Количество дней, оставшихся до окончания срока действия лицензии.
- Идентификатор активации.

Посмотреть на My Kaspersky

По ссылке открывается сайт My Kaspersky на странице с информацией о коде активации, с помощью которого была активирована программа. Может потребоваться ввести имя пользователя и пароль от вашей учетной записи на My Kaspersky.

Как настроить безопасное соединение для выбранного сайта

Чтобы настроить безопасное соединение для выбранного сайта, выполните следующие действия:

1. Откройте главное окно программы.
2. В главном окне программы нажмите на кнопку .
3. В раскрывающемся меню выберите пункт **Настройка**.

   Откроется окно **Настройка**.
4. Нажмите на кнопку **Настроить правила для сайтов**.

   Откроется окно **Правила подключения к сайтам**.
5. В блоке **Исключения для сайтов** нажмите на кнопку **Настроить**.

   Откроется окно **Исключения для сайтов**.
6. Нажмите на кнопку **Добавить**, чтобы добавить сайт в список исключений из настроек, которые заданы для категорий сайтов.

   Откроется окно **Добавление сайта**.
7. В поле **Веб-адрес (URL)** введите адрес сайта.
8. В блоке **Действие при открытии сайта** укажите, какое действие должна выполнять программа, когда вы заходите на этот сайт:

   - **Включать безопасное соединение**. Программа Kaspersky Anti-Virus включает безопасное соединение, когда вы посещаете указанный сайт. Например, вы можете указать, что программа должна включать безопасное соединение, когда вы посещаете сайт вашего банка. Настройка действует, даже если в окне **Правила подключения к сайтам** в блоке **При посещении незащищенных банковских сайтов** выбран вариант **Не реагировать**.

     a. В раскрывающемся списке **Выбирать виртуальный сервер** выберите регион, через который вы хотите устанавливать безопасное соединение, когда посещаете этот сайт. Если для сайта и категории, в которую входит этот сайт, заданы разные регионы для включения безопасного соединения, подключение к сайту происходит через тот регион, который указан для этого сайта, а не всей категории.

     b. Установите флажок **Уведомлять о включении**, если вы хотите получать уведомления о включении безопасного соединения, когда вы посещаете этот сайт.

   - **Не реагировать**. Программа Kaspersky Anti-Virus не включает безопасное соединение, когда вы посещаете указанный сайт.
9. Нажмите на кнопку **Добавить**.

Kaspersky Secure Connection не включает безопасное соединение, если подключение к сайту выполняется по протоколу HTTPS.

Вернуться в справку Kaspersky Secure Connection.

Как настроить безопасное соединение для категорий сайтов

По умолчанию программа Kaspersky Secure Connection не устанавливает безопасное соединение, когда вы открываете сайты в браузере. Вы можете настроить включение безопасного соединения для разных категорий сайтов, если на вашем компьютере установлена и активирована программа Kaspersky Internet Security, Kaspersky Total Security или Kaspersky Security Cloud. Например, вы можете указать, что безопасное соединение должно включаться, когда вы посещаете сайты платежных систем или социальных сетей.

Чтобы настроить безопасное соединение для категорий сайтов, выполните следующие действия:

1. Откройте главное окно программы.
2. В главном окне программы нажмите на кнопку ☰.
3. В раскрывающемся меню выберите пункт **Настройка**.

   Откроется окно **Настройка**.
4. Нажмите на кнопку **Настроить правила для сайтов**.

   Откроется окно **Правила подключения к сайтам**.
5. Выберите категорию сайтов:

   - Банковские сайты. К этой категории относятся сайты банков.
   - Платежные системы. К этой категории относятся сайты платежных систем.
   - Интернет-магазины с онлайн-оплатой. К этой категории относятся сайты интернет-магазинов, содержащих встроенные платежные системы.
   - Социальные сети. К этой категории относятся сайты социальных сетей.
6. Выберите вариант действия при посещении выбранной категории сайтов:

   - **Включать безопасное соединение**. Программа будет включать безопасное соединение при посещении сайтов выбранной категории.
   - **Спрашивать**. При посещении какого-либо сайта из выбранной категории программа будет спрашивать вас, нужно ли включать безопасное соединение для этого сайта. В окне браузера выберите нужное действие и установите флажок **Запомнить выбор для этого сайта**. Программа будет выполнять выбранное вами действие каждый раз при посещении этого сайта. Если флажок не установлен, программа запоминает ваш выбор на один час.
   - **Не реагировать**. Программа не будет включать безопасное соединение при посещении сайтов выбранной категории.
7. Если выбран вариант **Включать безопасное соединение**, в раскрывающемся списке **Выбирать виртуальный сервер** укажите регион, через который вы хотите устанавливать безопасное соединение для этой категории сайтов.
8. Установите флажок **Уведомлять о включении**, если вы хотите получать уведомления о включении безопасного соединения, когда вы посещаете сайт этой категории.

По умолчанию Kaspersky Secure Connection не предлагает включать безопасное соединение, если подключение к сайту выполняется по протоколу HTTPS.

Вернуться в справку Kaspersky Secure Connection.

Анализ программ завершен. Требуется ваше решение

Во время анализа программ, установленных на компьютере, были обнаружены программы, информации о которых недостаточно. Если вам известны эти программы и вы хотите работать с ними в режиме Безопасных программ, разрешите запуск этих программ. После этого включите режим Безопасных программ.

Не включать

При нажатии на кнопку включение режима Безопасных программ отменяется. Открывается окно **Инструменты**.

Перейти к списку программ и файлов, чтобы принять решение

По ссылке выполняется переход к окну со списком программ, запуск которых будет заблокирован при включении режима Безопасных программ. В окне также можно разрешить запуск программ, которым вы доверяете.

Анализ программ завершен. Требуется ваше решение

В процессе анализа программ, установленных на компьютере, были обнаружены программы, информации о которых недостаточно. При использовании режима Безопасных программ запуск этих программ будет заблокирован. Вы можете разрешить запуск программ, которым вы доверяете, и включить режим Безопасных программ.

Список программ и модулей

Список содержит программы и модули, которые по умолчанию будут заблокированы при использовании режима Безопасных программ. Вы можете разрешить запуск программ и модулей, которым вы доверяете, с помощью переключателей в правой части списка.

Программы

В графе отображается название программы.

При нажатии на кнопку ▸ отображается дополнительная информация о программе: название, версия, сведения о производителе, а также причина, по которой в режиме Безопасных программ блокируется запуск программы (например, отсутствие цифровой подписи).

Файл

В графе отображается путь к исполняемому файлу программы.

При нажатии правой клавиши мыши на программе в списке отображается контекстное меню. Из контекстного меню можно открыть папку, в которой расположен исполняемый файл программы, а также разрешить или запретить запуск программы.

Включить режим Безопасных программ

При нажатии на кнопку включается режим Безопасных программ.

Анализ программ завершен. Обнаружены неизвестные системные файлы

Во время анализа программ, установленных на компьютере, были обнаружены неизвестные системные файлы. Если вам известны эти файлы и вы хотите работать с ними в режиме Безопасных программ, разрешите запуск этих файлов. Для этого нажмите на кнопку **Разрешить и продолжить**.

Перейти к списку неизвестных системных файлов

По ссылке открывается окно **Неизвестные системные файлы**. В этом окне можно просмотреть список неизвестных системных файлов, обнаруженных Kaspersky Anti-Virus.

Не включать

При нажатии на кнопку включение режима Безопасных программ отменяется. Открывается окно **Инструменты**.

Разрешить и продолжить

По ссылке Kaspersky Anti-Virus разрешает запуск неизвестных системных файлов. Выполняется переход к следующему шагу включения режима Безопасных программ.

Анализ установленных программ

Процесс анализа программ

В блоке отображается процесс анализа системных файлов и программ, установленных на вашем компьютере. Kaspersky Anti-Virus выполняет анализ, чтобы определить, целесообразно ли использовать режим Безопасных программ на вашем компьютере. В процессе анализа Kaspersky Anti-Virus отображает количество доверенных файлов, а также количество файлов, для которых требуется ваше решение.

Состояние выполнения отдельных этапов анализа отображается в процентах.

Вы можете пропустить выполнение отдельных этапов анализа, нажав на кнопку **Пропустить**. Также вы можете остановить анализ, нажав на кнопку **Остановить**.

Пропустить

При нажатии на кнопку процесс анализа установленных программ прерывается. В открывшемся окне вы можете включить режим Безопасных программ или продолжить прерванный анализ установленных программ.

Кнопка недоступна, пока Kaspersky Anti-Virus выполняет анализ системных файлов.

Остановить

При нажатии на кнопку прерывается анализ установленных программ. Открывается окно **Режим Безопасных программ**. Включение режима Безопасных программ отменяется.

Анализ установленных программ завершен

Анализ программ, установленных на вашем компьютере, завершен. При включении режима Безопасных программ запуск доверенных программ будет разрешен. Мы рекомендуем вам включить режим Безопасных программ.

Включить режим Безопасных программ

При нажатии на кнопку включается режим Безопасных программ.

Анализ установленных программ прерван

Продолжить

При нажатии на кнопку анализ установленных программ возобновляется.

Пропустить

По ссылке открывается окно **Анализ установленных программ и исполняемых файлов завершен**. В этом окне можно просмотреть результаты анализа программ, а также включить режим Безопасных программ.

Включение режима Безопасных программ

Для работы режима Безопасных программ необходимо включить компоненты Контроль программ, Файловый Антивирус и Мониторинг активности. При нажатии на кнопку **Продолжить** эти компоненты защиты будут включены автоматически.

Продолжить

При нажатии на кнопку Kaspersky Anti-Virus запускает процесс анализа программ, установленных на вашем компьютере. По результатам анализа Kaspersky Anti-Virus определяет, целесообразно ли использовать режим Безопасных программ на вашем компьютере.

Неизвестные программы и модули

Отображать: Список / Программы / Производители / Папки

Ссылками изменяется способ отображения программ и модулей в списке.

Можно выбрать один из следующих способов отображения программ и модулей:

- По ссылке **Список** программы и модули располагаются в алфавитном порядке.
- По ссылке **Программы** программы и модули распределяются по программам, к которым они относятся.
- По ссылке **Производители** программы и модули распределяются по названиям производителей.
- По ссылке **Папки** программы и модули распределяются по папкам, в которых они располагаются.

Разрешить все

По ссылке устанавливается разрешение на запуск всех программ в списке.

Заблокировать все

По ссылке устанавливается запрет на запуск всех программ в списке.

Список программ и модулей

Список содержит программы и модули, которые по умолчанию будут заблокированы при использовании режима Безопасных программ. Вы можете разрешить запуск программ и модулей, которым вы доверяете, с помощью переключателей в правой части списка.

Программы / Группы и программы / Производители и программы / Программы и папки

В зависимости от выбранного способа отображения в графе отображается название программы или модуля, программы, производителя или папки.

Если выбран способ отображения **Список**, при нажатии на кнопку ▸ отображается дополнительная информация о программе: группа программ, версия, сведения о производителе, а также причина, по которой Kaspersky Anti-Virus блокирует запуск программы (например, отсутствие цифровой подписи).

Если выбран способ группировки **Программы** / **Производители** / **Папки**, при нажатии на кнопку ▸ отображаются дочерние программы и модули.

Файл

В графе отображается путь к исполняемому файлу программы или модуля.

Запуск

В графе отображается информация о том, запрещен или разрешен запуск программы, а также переключатель, с помощью которого можно разрешить или запретить запуск программы.

Неизвестные системные файлы

Список неизвестных системных файлов

Список содержит перечень неизвестных системных файлов, обнаруженных в процессе анализа установленных программ.

Программа

В графе отображается название неизвестного системного файла.

При нажатии на кнопку ▸ отображается дополнительная информация о системном файле: название продукта, версия, сведения о производителе, а также причина, по которой Kaspersky Anti-Virus не считает программу, к которой относится этот файл, доверенной (например, у программы отсутствует цифровая подпись).

Подробнее

В графе отображается путь к системному файлу.

Контроль программ

В блоке **Программы** отображается информация о количестве программ, которые контролирует Kaspersky Anti-Virus.

Управление программами

По ссылке открывается окно **Управление программами**. В этом окне можно указать группы доверия программ, разрешить или запретить запуск программ, а также перейти к настройке разрешений для отдельной программы.

В блоке **Текущая активность** отображается информация о количестве программ и процессов, выполняемых в данный момент. В графическом виде представлена информация о загрузке центрального процессора, объеме оперативной памяти и дискового пространства, а также о сетевой активности.

Показать всю активность

По ссылке открывается окно **Активность программ** на закладке **Работающие**. В этом окне можно просмотреть информацию о потреблении ресурсов компьютера каждой из программ, выполняемых в текущий момент, а также перейти к настройке разрешений для отдельной программы.

Закладка Исключения

Исключения

Содержит ресурсы с персональными данными, исключаемые из области защиты Контроля программ. Ресурсом может быть файл, папка или ключ реестра.

Ресурс

Графа, в которой указывается название ресурса.

Путь

Графа, в которой указывается расположение ресурса. Путь может содержать маску.

Статус

В графе отображается раскрывающийся список со статусом ресурса:

- **Включить контроль**. Если выбран этот вариант, программа контролирует действия с этим ресурсом.
- **Выключить контроль**. Если выбран этот вариант, программа не контролирует действия с этим ресурсом.

Нажав левой клавишей мыши на значок статуса, в раскрывающемся списке вы можете включить или выключить контроль ресурса.

Добавить

При нажатии на кнопку открывается окно, в котором можно указать ресурс с персональными данными, добавляемыми в список.

Изменить

Кнопка, при нажатии на которую открывается окно **Изменение файла или папки / Изменение ключа реестра**. В окне можно изменить настройки выбранного ресурса.

Ресурсы, добавленные в список по умолчанию, не подлежат изменению.

Удалить

Кнопка, при нажатии на которую выбранный ресурс удаляется из списка.

Ресурсы, добавленные в список по умолчанию, не подлежат удалению.

Закладка Общие

Закладка Общие

Описание выбранной группы программ.

Запущена новая программа

В этом окне отображается ход анализа запускаемой программы с помощью Контроля программ.

Закладка Ресурсы

На этой закладке можно выбрать системные ресурсы или ресурсы пользователя и изменить права доступа программ к этим ресурсам.

Кнопка 

С помощью кнопки-переключателя можно открывать или скрывать панель настройки правил.

Вид

В раскрывающемся списке можно выбрать два варианта фильтрации ресурсов:

- **Скрывать системные программы**. Если выбран этот вариант, в списке ресурсов не отображаются ресурсы системных программ.
- **Скрывать Kaspersky Anti-Virus**. Если выбран этот вариант, в списке не отображаются ресурсы Kaspersky Anti-Virus.

Операционная система

Содержит настройки и ресурсы операционной системы выбранной категории. Ресурсом может быть файл или папка, ключ реестра, сетевой сервис или IP-адрес. Контроль программ контролирует доступ других программ к ресурсам из списка.

По умолчанию в список **Операционная система** входят следующие объекты:

- ключи реестра, содержащие настройки автозапуска;
- ключи реестра, содержащие настройки работы в интернете;
- ключи реестра, влияющие на безопасность операционной системы;
- ключи реестра, содержащие настройки системных служб;
- системные файлы и папки;
- папки автозапуска.

Персональные данные

Содержит персональные данные пользователя, распределенные по ресурсам и категориям. Ресурсом может быть файл или папка. Контроль программ анализирует действия других программ над ресурсами из списка.

По умолчанию в список персональных данных входят следующие объекты:

- файлы пользователя (папка "Мои документы", файлы cookies, данные об активности пользователя);
- файлы, папки и ключи реестра, содержащие настройки работы и важные данные наиболее часто используемых программ: браузеров, файловых менеджеров, почтовых клиентов, IM-клиентов и электронных кошельков.

Ресурс

Графа, в которой содержится название ресурса операционной системы, защищаемого Контролем программ.

Путь

Графа, в которой указывается расположение ресурса. Путь может содержать маску.

Статус

В графе отображается раскрывающийся список со статусом ресурса:

- **Включить контроль**. Если выбран этот вариант, программа контролирует действия с этим ресурсом.
- **Выключить контроль**. Если выбран этот вариант, программа не контролирует действия с этим ресурсом.

Нажав левой клавишей мыши на значок статуса, в раскрывающемся списке вы можете включить или выключить контроль ресурса.

Добавить

В раскрывающемся списке можно добавить категорию ресурсов, файл или папку с ресурсами или ключ системного реестра.

Изменить

По ссылке открывается окно, в котором можно изменить название выбранного ресурса и путь к нему.

Удалить

По ссылке можно удалить из списка выбранную категорию ресурсов, файл или папку с ресурсами или ключ системного реестра. Контроль программ не будет контролировать доступ других программ к этому ресурсу.

Восстановить

В раскрывающемся списке можно выбрать варианты действия:

- **настройки категории**. Если выбран этот вариант, настройки выбранной категории получат значения по умолчанию.
- **настройки подгрупп и ресурсов**. Если выбран этот вариант, настройки входящих в категорию подгрупп и ресурсов получат значения по умолчанию.

Список программ

В списке отображаются группы доверия и программы, входящие в эти группы доверия. В графах **Чтение**, **Запись**, **Создание**, **Удаление** указаны права доступа программы или группы программ к выбранному ресурсу.

В таблице ниже приведено описание действий Kaspersky Anti-Virus, если программа или группа программ пытается получить доступ к ресурсу.

Описание действий Kaspersky Anti-Virus

Действие	Описание
Наследовать	Программа или группа программ наследует реакцию из вышестоящей группы.
Разрешить	Kaspersky Anti-Virus разрешает программам, входящим в выбранную группу, доступ к ресурсу.
Запретить	Kaspersky Anti-Virus запрещает программам, входящим в выбранную группу, доступ к ресурсу.
Запросить действие	Kaspersky Anti-Virus запрашивает пользователя о предоставлении программе или группе программ доступа к ресурсу.
Записывать в отчет	Помимо заданной реакции Kaspersky Anti-Virus записывает в отчет информацию о попытке доступа программы к ресурсу.

Окно Лицензионное соглашение

Окно содержит текст Лицензионного соглашения. Для просмотра Лицензионного соглашения вы можете воспользоваться полосой прокрутки.

Окно Лицензирование

В блоке, расположенном в верхней части окна, представлена информация о лицензии:

- Лицензионный ключ.

  Использование программы по действующей лицензии можно прекратить, нажав на кнопку .
- Статус ключа.
- Количество компьютеров, на которое распространяется лицензия.
- Дата активации.
- Дата окончания срока действия лицензии.
- Количество дней, оставшихся до окончания срока действия лицензии.

  Для подписки возможно отображение дополнительной информации о статусе подписки.

О лицензии / О подписке

По ссылке открывается окно со сведениями о действующей лицензии или подписке.

Лицензионное соглашение

При нажатии на кнопку открывается окно с текстом Лицензионного соглашения.

В зависимости от наличия лицензии, подписки и от особенностей вашей версии программы в окне могут отображаться различные кнопки для запуска действий, связанных с лицензией или подпиской. Ниже приведены описания кнопок, предусмотренных по умолчанию.

Активировать программу / Ввести код активации

Кнопка, при нажатии на которую запускается мастер активации программы.

Кнопка отображается, если программа не активирована, если можно ввести резервный код активации, если подписка, по которой вы используете программу, истекла или истекает.

Купить лицензию

При нажатии на кнопку открывается окно браузера на странице интернет-магазина, в котором вы можете приобрести лицензию.

Кнопка не отображается, если при наличии действующей лицензии вы указали резервный код активации.

Восстановить мои коды активации

По ссылке вы можете перейти на сайт My Kaspersky и посмотреть информацию о ваших кодах активации.

Активировать сейчас

Кнопка, при нажатии на которую программу можно немедленно активировать с помощью резервного кода активации.

Кнопка отображается, если по истечении срока действия лицензии программа не активировалась с помощью резервного кода активации автоматически.

Удалить код активации

Кнопка, при нажатии на которую резервный код активации удаляется. На действующую лицензию это не влияет.

Кнопка отображается, если вы указали резервный код активации.

Обновить базы

Кнопка, при нажатии на которую запускается обновление баз программы.

Кнопка отображается, если возникшие проблемы с лицензией можно решить обновлением баз (например, дата выпуска баз не соответствует сроку действия лицензии).

Причины и возможные решения

Кнопка, при нажатии на которую открывается окно браузера на сайте Службы технической поддержки с информацией о возникшей проблеме.

Кнопка отображается, если возникли проблемы с действующей лицензией или с резервным кодом активации.

Проверить код активации

Кнопка, при нажатии на которую запускается мастер активации программы с целью проверки резервного кода активации.

Кнопка отображается, если попытка автоматической проверки резервного кода активации не удалась.

Проверить статус подписки

Кнопка, при нажатии на которую с сервера поставщика услуг скачивается актуальная информация о статусе подписки.

Кнопка отображается, если программа используется по подписке.

Посетить сайт поставщика услуг

Кнопка, при нажатии на которую открывается окно браузера на сайте поставщика услуг.

Кнопка отображается, если программа используется по подписке.

Найдены другие несовместимые программы

Список несовместимых программ

В списке перечислены программы, несовместимые с устанавливаемой программой. Для корректной работы устанавливаемой программы нужно удалить несовместимые с ней программы.

Удалить вручную

Кнопка, при нажатии на которую открывается окно со списком программ, установленных на компьютере. В этом списке можно выбрать программы, несовместимые с устанавливаемой программой, чтобы удалить их с компьютера.

Продолжить

Кнопка, при нажатии на которую несовместимые программы, представленные в списке, остаются на компьютере, а мастер продолжает работу.

Одновременное использование программ, несовместимых с устанавливаемой программой, может привести к некорректной работе устанавливаемой программы и существенному ослаблению защиты вашего компьютера.

Найдены несовместимые программы

Список несовместимых программ

В списке перечислены программы, несовместимые с устанавливаемой программой. Для корректной работы устанавливаемой программы нужно удалить несовместимые с ней программы.

Удалить отмеченные

Кнопка, при нажатии на которую несовместимые программы, представленные в списке, удаляются с компьютера, а мастер продолжает работу.

Продолжить

Кнопка, при нажатии на которую несовместимые программы, представленные в списке, остаются на компьютере, а мастер продолжает работу.

Одновременное использование программ, несовместимых с устанавливаемой программой, может привести к некорректной работе устанавливаемой программы и существенному ослаблению защиты вашего компьютера.

Необходимо перезагрузить компьютер

Перезагрузить компьютер

Флажок включает / выключает перезагрузку компьютера, необходимую для продолжения работы мастера миграции.

Если флажок установлен, то при нажатии на кнопку **Готово** компьютер перезагружается, после чего мастер миграции продолжает работу.

Если флажок снят, то компьютер не перезагружается. Мастер миграции автоматически продолжит работу после того, как вы перезагрузите или выключите и снова включите компьютер.

Начало работы

Показать информацию о сертификате

Ссылка, по которой открывается окно с информацией о сертификате "Лаборатории Касперского".

Далее

Кнопка, при нажатии на которую мастер установки сертификата начинает работу.

Установка сертификата

В этом окне отображается процесс автоматической установки сертификата. Выполнение задачи может занять некоторое время.

Kaspersky Anti-Virus выполняет поиск браузеров, установленных на компьютере пользователя, и автоматически устанавливает сертификаты в хранилище сертификатов Microsoft Windows.

В процессе установки сертификата на экране может появиться предупреждение системы безопасности Microsoft Windows, в котором потребуется подтвердить намерение установить сертификат.

Завершение работы мастера

Готово

Кнопка, при нажатии на которую Kaspersky Anti-Virus завершает работу мастера установки сертификата.

Окно История действий программы

Раскрывающийся список для фильтрации записей

Возможна фильтрация событий по следующим видам активности, доступным из раскрывающегося списка:

- **Все события**. В списке отображается информация о всех действиях программы.
- **Реестр**. В списке отображается информация о действиях программы в реестре (например, создание, удаление ключей и значений, изменение прав).
- **Файлы**. В списке отображается информация о действиях программы в файловой системе (например, создание, удаление файлов).
- **Программы**. В списке отображается информация о действиях программы в операционной системе (например, запуск, остановка процессов).

История действий программы

Содержит отчет об активности программы, которую Мониторинг активности обнаружил в операционной системе. Мониторинг активности отслеживает файловые, реестровые и системные события в операционной системе, связанные с программой.

Для каждого действия программы в списке доступно описание и информация о подробностях действия (например, путь к файлу, или сведения об изменении значения в ключе реестра).

Окно История появления программы

Окно **История появления программы** содержит результаты исследования опасной активности программы, проведенного Мониторингом активности. Доступны следующие данные о программе:

- название программы;
- местоположение программы на компьютере;
- время окончания установки программы на компьютер;
- название процесса, который произвел установку программы на компьютер;
- последовательность запуска программы.

История действий программы

Окно содержит отчет об активности программы, которую Мониторинг активности обнаружил в операционной системе. Мониторинг активности отслеживает файловые, реестровые и системные события, связанные с программой.

Окно Откат действий программы

Список действий, выполненных Мониторингом активности

В списке отображаются действия, предпринятые Мониторингом активности для устранения последствий вредоносных действий, обнаруженных этим компонентом защиты.

Объект

В графе отображается название объекта, в отношении которого был выполнен откат вредоносных действий.

Действие

В графе отображается действие, которое было применено к объекту, указанному в графе **Объект**.

Время

В графе отображается время выполнения действия, указанного в графе **Действие**.

Раздел Заблокированные компьютеры

Заблокированные компьютеры

Содержит данные о компьютерах, сетевую активность которых по отношению к вашему компьютеру заблокировал компонент Защита от сетевых атак.

Адрес компьютера

Графа, в которой отображается IP-адрес заблокированного компьютера.

Время начала блокирования

Графа, в которой отображается время с момента блокирования.

По умолчанию компонент Защита от сетевых атак блокирует входящий трафик от атакующего компьютера в течение часа.

Вы можете разблокировать выбранный в списке компьютер с помощью его контекстного меню.

Разблокировать

При нажатии на кнопку компонент Защита от сетевых атак разблокирует выбранный компьютер.

Разблокировать все компьютеры

По ссылке компонент Защита от сетевых атак разблокирует все заблокированные компьютеры.

Раздел Открытые порты

Вид

При нажатии на кнопку открывается меню, которое содержит следующие пункты:

- **Показывать все порты** – в списке отображаются все открытые порты вашего компьютера.
- **Скрывать порты loopback** – в списке отображаются все порты, кроме тех, которые используются сетевым программным обеспечением операционной системы.

Открытые порты

Содержит информацию обо всех открытых в данный момент портах для каждого процесса.

Для каждого порта указана следующая информация:

- номер порта;
- имя процесса (программы, службы, сервера), который использует порт;
- идентификатор процесса;
- локальный IP-адрес процесса;
- протокол, по которому выполняется соединение через порт.

По двойному щелчку на строке списка открывается окно **Правила программы** на закладке **Сетевые правила**. В этом окне вы можете настроить сетевые правила для программы, которая использует выбранный порт.

По правой клавише мыши на элементе списка открывается контекстное меню, из которого можно перейти к настройке сетевых правил.

Меню содержит следующие пункты:

- **Сетевые правила программы**. При выборе этого пункта меню открывается окно **Правила программы** на закладке **Сетевые правила**. В окне вы можете настроить сетевое правило для программы, которая использует порт, выбранный в списке.
- **Все сетевые правила**. При выборе этого пункта меню открывается окно **Пакетные правила**. В окне вы можете настроить пакетные правила для программы, которая использует порт, выбранный в списке.

Раздел Сетевая активность

Вид

Кнопка, при нажатии на которую открывается меню. Меню содержит следующие пункты:

- **Показывать локальные соединения** – в списке отображается информация о соединениях вашего компьютера с другими компьютерами в локальной сети.
- **Показывать соединения Kaspersky Anti-Virus** – в списке отображается информация о соединениях, установленных Kaspersky Anti-Virus.

Сетевая активность

Содержит активные сетевые соединения, установленные на вашем компьютере в данный момент.

Для каждого соединения указана следующая информация:

- название процесса (программы, службы, сервера), который инициировал соединение;
- направление соединения (входящее / исходящее);
- протокол, по которому выполняется соединение;
- настройки соединения (удаленный порт и IP-адрес);
- объем переданной / принятой информации в килобайтах.

По правой клавише мыши на элементе списка открывается контекстное меню, из которого можно перейти к настройке сетевых правил.

Меню содержит следующие пункты:

- **Сетевые правила программы**. При выборе этого пункта меню открывается окно **Правила программы** на закладке **Сетевые правила**. В этом окне вы можете настроить сетевое правило для программы, выбранной в списке.
- **Все сетевые правила**. При выборе этого пункта меню открывается окно **Пакетные правила**. В этом окне вы можете настроить пакетные правила для программы, выбранной в списке.

Блокировать любую сетевую активность

По ссылке Сетевой экран запрещает сетевую активность всем процессам.

В нижней части окна отображается график объема входящего и исходящего трафика для процесса, выбранного в списке. График показывает объем трафика в режиме реального времени. Объем трафика указывается в килобайтах.

Раздел Сетевой трафик

Период

Список содержит интервалы времени для просмотра распределения сетевого трафика.

Возможные значения:

- **За сегодня**. В списке отображается распределение сетевого трафика за текущие сутки.
- **За вчера**. В списке отображается распределение сетевого трафика за вчерашние сутки.
- **За месяц**. В списке отображается распределение сетевого трафика за текущий месяц.
- **За год**. В списке отображается распределение сетевого трафика за текущий год.

Сетевой трафик

Содержит информацию обо всех входящих и исходящих соединениях между вашим компьютером и другими компьютерами.

Для каждой программы (компьютера, службы, сервера, процесса) указан объем входящего и исходящего трафика.

По двойному щелчку на программе в списке открывается окно **Правила программы** на закладке **Сетевые правила**. В этом окне вы можете настроить сетевые правила для выбранной программы.

По правой клавише мыши на элементе списка открывается контекстное меню, из которого можно перейти к настройке сетевых правил.

Меню содержит следующие пункты:

- **Сетевые правила программы**. При выборе этого пункта открывается окно **Правила программы** на закладке **Сетевые правила**, на которой вы можете настроить сетевое правило для выбранной программы.
- **Все сетевые правила**. При выборе этого пункта открывается окно **Пакетные правила**, в котором вы можете настроить пакетные правила для выбранной программы.

В нижней части окна отображается диаграмма распределения трафика выбранной программы по времени за выбранный период.

Разрыв сетевых соединений

Если в момент завершения работы на компьютере или приостановки защиты были установлены сетевые соединения, контролируемые программой, на экран будет выведено уведомление о разрыве этих соединений. Это необходимо для корректного завершения работы программы. Разрыв происходит автоматически по истечении 10 секунд либо при нажатии на кнопку **Да**. Большинство прерванных соединений восстанавливается через некоторое время.

Если во время разрыва соединения вы скачиваете файл без использования менеджера загрузки, передача данных будет прервана. Для получения файла вам потребуется повторно инициировать его загрузку.

Вы можете отменить разрыв соединений. Для этого в окне уведомления нажмите на кнопку **Нет**. При этом программа продолжит свою работу.

Поиск проблем / Поиск изменений

В этом окне отображается процесс анализа настроек браузера Microsoft Internet Explorer или поиск изменений, сделанных мастером настройки браузера ранее.

Процесс может занять некоторое время. Процесс можно прервать, нажав на кнопку **Отмена**.

Поиск проблем завершен / Поиск изменений завершен

Список проблем

Содержит перечисление проблем, которые обнаружила программа Kaspersky Anti-Virus на предыдущем шаге. Найденные проблемы Kaspersky Anti-Virus группирует в зависимости от опасности, которую они представляю:

- *Проблемы, которые настоятельно рекомендуется устранить*. Уязвимости браузера, представляющие серьезную угрозу безопасности компьютера.
- *Проблемы, которые рекомендуется устранить*. Уязвимости браузера, которые могут представлять опасность для компьютера.
- *Проблемы, которые можно устранить*. Неопасные в данный момент уязвимости браузера, которые в дальнейшем могут поставить безопасность компьютера под угрозу.

Если флажок в строке проблемы установлен, Kaspersky Anti-Virus пытается устранить проблему.

Если флажок в строке проблемы снят, Kaspersky Anti-Virus не устраняет проблему.

Если на первом шаге работы мастера настройки браузера был выбран вариант **Отменить изменения**, в списке содержатся устраненные ранее проблемы. Вы можете отменить действия, выполненные для устранения этих проблем.

Настройка браузера

Выполнить диагностику Microsoft Internet Explorer

Kaspersky Anti-Virus запускает анализ настроек браузера Microsoft Internet Explorer.

Отменить изменения

Kaspersky Anti-Virus отменяет изменения, которые были сделаны в результате предыдущей работы мастера настройки браузера.

Этот вариант доступен, если в результате предыдущей работы мастер настройки браузера внес изменения в настройки браузера.

Устранение проблем / Отмена изменений

В этом окне отображается процесс устранения проблем, обнаруженных в ходе анализа настроек браузера. Устранение проблем может занять некоторое время.

Если на первом шаге был выбран вариант **Отменить изменения**, мастер настройки браузера выполняет откат действий, выбранных на предыдущем шаге.

Завершение работы

Готово

Кнопка, при нажатии на которую мастер настройки браузера завершает работу.

Перезагрузить компьютер

Если флажок установлен, компьютер перезагружается после завершения работы мастера.

О дополнительных возможностях безопасного соединения

Дополнительные возможности безопасного соединения доступны вам, если на вашем компьютере установлена и запущена программа Kaspersky Internet Security, Kaspersky Total Security или Kaspersky Security Cloud.

Дополнительные возможности безопасного соединения включают в себя следующее:

- Настройка включения безопасного соединения при посещении следующих категорий сайтов:
  - банковские сайты;
  - платежные системы;
  - интернет-магазины и сайты электронной коммерции;
  - социальные сети.
- Настройка автоматической смены региона. Если вы указали в настройках безопасного соединения разные регионы при подключении к сайтам разных категорий, вы можете указать, надо ли менять регион, когда вы перемещаетесь между сайтами разных категорий.
- Настройка безопасного соединения для отдельных сайтов, например, для сайтов, которые вы часто посещаете.

Вернуться в справку Kaspersky Secure Connection.

Обнаруженные объекты

Устранить

При нажатии на кнопку Kaspersky Anti-Virus запускает обработку обнаруженного объекта.

Кнопка отображается при наличии обнаруженного объекта.

При нажатии на кнопку раскрывается меню, в котором можно выбрать дополнительное действие:

- **Добавить в исключения** – создать исключение, в соответствии с которым объект не должен считаться вредоносным.
- **Игнорировать** – перенести уведомление в раздел **Игнорируемые уведомления**.
- **Перейти к файлу** – открыть папку исходного размещения файла.
- **Посмотреть отчет** – открыть окно **Подробные отчеты** с детальной информацией об обнаруженных объектах и действиях программы в отношении этих объектов.
- **Узнать больше** – открыть веб-страницу с описанием обнаруженного объекта.

Окна уведомлений Kaspersky Anti-Virus

Уведомления программы, появляющиеся в области уведомлений панели задач, информируют о событиях, происходящих в процессе работы программы и требующих вашего внимания.

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

Окно Родительский контроль

Список учетных записей

Содержит учетные записи пользователей компьютера.

В списке отображается следующая информация о пользователе:

- изображение пользователя, установленное в настройках Родительского контроля;
- псевдоним пользователя;
- статус контроля пользователя с помощью Родительского контроля (**Включен** или **Выключен**).

Изображение пользователя

По нажатию на изображение пользователя открывается окно, содержащее статистику использования пользователем интернета и программ. Из этого окна можно перейти к просмотру отчета Родительского контроля, а также к настройке Родительского контроля.

Настроить ограничения

По ссылке открывается окно, в котором вы можете настроить контроль действий пользователя с помощью Родительского контроля.

Посмотреть отчет

По ссылке открывается окно, содержащее статистику использования интернета и программ выбранным пользователем. Из этого окна можно перейти к просмотру отчета Родительского контроля, а также к настройке Родительского контроля.

Переключатель  / 

Переключатель включает / выключает контроль действий пользователя:

 – контроль действий пользователя включен.

 – контроль действий пользователя выключен.

Окно Создайте пароль

Защита паролем

Отображается при переходе к настройкам Родительского контроля, если не задан пароль для ограничения доступа к управлению Kaspersky Anti-Virus. Включает в себя следующие элементы управления:

- **Пароль**. В этом поле вводится пароль.
- **Подтверждение**. В этом поле пароль вводится повторно.
- **Продолжить**. При нажатии на эту кнопку отображается окно **Родительский контроль**, из которого можно перейти к просмотру профилей пользователей и настройке Родительского контроля.
- **Пропустить**. По ссылке отображается окно **Родительский контроль**, доступ к управлению Родительским контролем не ограничивается.

Введите пароль

Отображается при переходе к настройкам Родительского контроля, если доступ к нему защищен паролем. Включает в себя следующие элементы управления:

- Поле ввода пароля.
- **Войти**. При нажатии на эту кнопку открывается окно **Родительский контроль**.
- **Запомнить пароль на эту сессию**. При установке этого флажка Kaspersky Anti-Virus запоминает введенный пароль и в течение текущей сессии больше его не запрашивает.

Об облачной защите

В этом окне вы можете ознакомиться с информацией о Kaspersky Security Network.

Окно My Kaspersky

Отключиться от My Kaspersky

При нажатии на кнопку Kaspersky Anti-Virus отключается от My Kaspersky.

Подключиться к My Kaspersky

При нажатии на кнопку Kaspersky Anti-Virus переходит к авторизации на My Kaspersky.

Перейти на My Kaspersky

При нажатии на кнопку открывается окно браузера на странице сайта My Kaspersky.

Кнопка отображается, если Kaspersky Anti-Virus подключен к сайту.

Окно Активация

В этом окне отображается процесс активации программы.

Отмена

При нажатии на кнопку можно отменить активацию программы.

Окно Анализ установленных программ

Запустить

При нажатии на кнопку запускается анализ установленных программ с целью поиска программ, которые, возможно, имеют нестандартную установку или удаление, редко используются или являются рекламными.

Остановить

При нажатии на кнопку останавливается анализ установленных программ.

Кнопка отображается, если выполняется анализ установленных программ.

Окно Безопасное соединение

Узнать больше

По ссылке открывается окно браузера на странице с информацией о программе Kaspersky Secure Connection.

Скачать и установить

При нажатии на кнопку запускается скачивание и установка программы Kaspersky Secure Connection.

Кнопка отображается, если на вашем компьютере не установлена программа Kaspersky Secure Connection.

Попробовать еще раз

По ссылке можно запустить скачивание и установку Kaspersky Secure Connection, если при предыдущем запуске произошла ошибка.

Ссылка отображается, если не удалось скачать установочный пакет Kaspersky Secure Connection.

Скачать и установить вручную

По ссылке открывается окно браузера со ссылкой на скачивание установочного пакета Kaspersky Secure Connection.

Ссылка отображается, если программе Kaspersky Anti-Virus не удалось автоматически скачать установочный пакет.

Открыть

При нажатии на кнопку открывается окно программы Kaspersky Secure Connection.

Кнопка отображается, если на вашем компьютере установлена программа Kaspersky Secure Connection.

Окно Безопасные платежи

Включить

Включение компонента Безопасные платежи.

Кнопка отображается, если компонент Безопасные платежи выключен.

Включить самозащиту

Включение механизма защиты Kaspersky Anti-Virus от изменения или удаления собственных файлов на диске, процессов в памяти, записей в системном реестре.

Кнопка отображается, если снят флажок **Включить самозащиту** в разделе **Дополнительно**, подраздел **Самозащита** окна настройки программы.

Добавить сайт / Добавить сайт в Безопасные платежи

При нажатии на кнопку в правой части окна отображаются поля ввода, в которых можно указать адрес веб-сайта банка или платежной системы и его описание. Когда пользователь обращается к указанному сайту или платежной системе, Kaspersky Anti-Virus выполняет действие, выбранное в блоке **При посещении этого сайта**.

Экранная клавиатура

По ссылке отображается Экранная клавиатура. Экранная клавиатура защищает от перехвата данные, которые вы вводите с клавиатуры. Экранную клавиатуру можно использовать для ввода персональных данных, например, при регистрации на сайтах или выполнении финансовых операций через интернет.

Чтобы Экранная клавиатура была доступна, после установки Kaspersky Anti-Virus необходимо перезагрузить компьютер.

Список банков и платежных систем

Содержит перечень сайтов банков или платежных систем, для которых вы указали особые настройки Безопасных платежей. По нажатию на элемент списка Kaspersky Anti-Virus выполняет заданное действие. Значок в левой части списка и текст, расположенный в центре списка, обозначают действие, которое будет выполняться:

- Запускать Защищенный браузер.
- Запрашивать действие.
- Не запускать Защищенный браузер, а открывать сайт в обычном браузере.

Справа от каждого элемента списка отображается кнопка . Если вы нажмете на эту кнопку, в правой части окна отобразятся поля ввода. В полях ввода можно изменить настройки использования Безопасных платежей при обращении к сайту банка или платежной системы.

Если список пуст, то Kaspersky Anti-Virus использует базу сайтов банков и платежных систем, рекомендованную специалистами "Лаборатории Касперского". При этом на месте списка отображается кнопка **Добавить сайт в Безопасные платежи**.

Показать все / Скрыть

По ссылке отображается / скрывается часть списка сайтов банков и платежных систем, для которых выбрано действие **Не запускать Защищенный браузер**.

Сайт для Безопасных платежей (URL)

Веб-адрес сайта банка или платежной системы. Вы можете указать веб-адрес или маску веб-адреса.

В блоке **При посещении этого сайта** вы можете выбрать действие, которое Kaspersky Anti-Virus совершает при обращении пользователя к указанному сайту.

Запускать Защищенный браузер

Если Kaspersky Anti-Virus обнаруживает попытку доступа к указанному сайту, то открывает этот сайт в Защищенном браузере. В обычном браузере, использованном для обращения к сайту, отображается сообщение о запуске Защищенного браузера.

Запрашивать действие

Если Kaspersky Anti-Virus обнаруживает попытку доступа к указанному сайту, то предлагает запустить Защищенный браузер либо открыть сайт при помощи обычного браузера.

Не запускать Защищенный браузер

Когда вы обращаетесь к указанному сайту, Kaspersky Anti-Virus не использует Защищенный браузер. Сайт открывается в обычном браузере.

Добавить описание

По ссылке отображается поле ввода, в котором можно ввести описание веб-сайта (например, название банка). Описание отображается в списке веб-сайтов банков и платежных систем в левой части окна.

Описание

Поле ввода, в котором можно изменить описание сайта (например, название банка). Описание отображается в списке сайтов банков и платежных систем в левой части окна.

Добавить / Сохранить

Кнопка, при нажатии на которую введенная информация о веб-сайте банка или платежной системы сохраняется в списке.

Отмена

Кнопка, при нажатии на которую внесенные изменения отменяются.

Удалить

Кнопка, при нажатии на которую выбранный сайт банка или платежной системы удаляется из списка.

Удаление можно отменить, нажав на кнопку **Восстановить** в правой части окна.

Восстановить

Кнопка, при нажатии на которую ранее удаленная запись о веб-сайте банка или платежной системе восстанавливается в списке.

Оставить отзыв

По ссылке открывается окно, в котором вы можете оставить отзыв о работе компонента Безопасные платежи.

Регистрация

Адрес электронной почты

Поле для ввода адреса электронной почты для входа на сайт My Kaspersky.

Пароль

Поле для ввода пароля для входа на сайт My Kaspersky.

Войти

При нажатии на кнопку выполняется вход на сайт My Kaspersky.

Забыли пароль?

Переход к окну восстановления пароля от учетной записи на сайте My Kaspersky, если вы его забыли.

У меня нет учетной записи

При нажатии на кнопку выполняется переход к форме регистрации на сайте My Kaspersky.

Подтвердить вход

Если на сайте My Kaspersky вы настроили двухэтапную проверку, на ваш телефон будет отправлено сообщение с проверочным кодом. Введите проверочным код в поле ввода и нажмите на кнопку **Подтвердить вход**.

Двухэтапная проверка доступна не во всех регионах. Подробнее смотрите в справке My Kaspersky.

При переходе к регистрации на My Kaspersky в окне отображаются следующие поля:

Адрес электронной почты

Поле для ввода адреса электронной почты для регистрации на My Kaspersky.

Пароль

Поле для ввода пароля для регистрации на My Kaspersky.

Повторите пароль

Поле для подтверждения пароля для My Kaspersky.

Ваше имя

Поле для ввода вашего имени. Это поле отображается не во всех регионах.

Ваша фамилия

Поле для ввода вашей фамилии. Это поле отображается не во всех регионах.

Где вы купили программу?

В этом поле можно выбрать магазин, в котором вы приобрели программу Kaspersky Anti-Virus.

Я соглашаюсь предоставить "Лаборатории Касперского" адрес своей электронной почты для получения персональных маркетинговых предложений

Если флажок установлен, вы будете получать новости от "Лаборатории Касперского" на указанный адрес электронной почты.

Я подтверждаю, что разрешаю АО "Лаборатория Касперского" использовать мой адрес электронной почты, имя и фамилию, чтобы оповещать меня по электронной почте о персонализированных специальных предложениях, обзорах, опросах, напоминать о незавершенных заказах, отправлять актуальные новости и события

Если флажок установлен, вы будете получать на указанный адрес электронной почты специальные предложения и новости от "Лаборатории Касперского". Этот флажок доступен, если вы используете программу на территории Европейского союза.

В некоторых регионах флажок называется **Я подтверждаю, что разрешаю АО "Лаборатория Касперского" использовать мой адрес электронной почты, чтобы оповещать меня по электронной почте о персонализированных специальных предложениях, обзорах, опросах, напоминать о незавершенных заказах, отправлять актуальные новости и события**.

Создать

При нажатии на кнопку выполняется регистрация учетной записи My Kaspersky. На указанный вами при регистрации адрес электронной почты придет письмо, содержащее ссылку для активации учетной записи My Kaspersky.

Состав полей при создании учетной записи формируется специалистами «Лаборатории Касперского» и может меняться.

Окно Выбор ключа в реестре

Выбрать

При нажатии на кнопку поля в окне **Добавление ключа реестра** заполняются значениями выбранного ключа.

Окно Выбор папки хранения сейфа

В этом окне можно выбрать папку, в которой будет храниться создаваемый сейф.

Выбрать

При нажатии на кнопку можно подтвердить, что указанный путь верный.

Окно Выбор файла или папки

Выбрать

При нажатии на кнопку путь к файлу или папке отображается в окне **Добавление файла или папки** в поле **Путь**.

Окно Группа доверия для неизвестных программ

В этом окне можно выбрать группу доверия для неизвестных программ.

Выбрать группу доверия автоматически

Если выбран этот вариант, Kaspersky Anti-Virus помещает неизвестные программы в одну из групп доверия на основании правил, заданных специалистами "Лаборатории Касперского".

Выбрать группу доверия вручную

Если выбран этот вариант, вы можете самостоятельно выбрать группу доверия, в которую необходимо помещать неизвестные программы.

Окно Группа доверия для программ, запущенных до начала работы Kaspersky Anti-Virus

В этом окне можно выбрать группу доверия для неизвестных программ, запущенных до начала работы Kaspersky Anti-Virus.

Список групп доверия

В списке можно указать группу доверия, в которую нужно помещать неизвестные программы, запущенные до начала работы Kaspersky Anti-Virus. Сетевая активность таких программ будет ограничиваться в соответствии с правилами выбранной группы доверия. По умолчанию сетевая активность программ, запущенных до начала работы Kaspersky Anti-Virus, ограничивается в соответствии с правилами, заданными специалистами "Лаборатории Касперского".

Окно Добавление / изменение исключения Защиты от сбора данных

Маска веб-адреса

В поле вы можете указать IP-адрес или веб-адрес (URL) сайта, на котором вы хотите разрешить сбор данных о ваших действиях.

Окно Добавление / Изменение категории

Название категории

В этом поле можно указать название категории ресурсов, доступ к которым со стороны программ должен анализировать и контролировать Контроль программ.

Окно Добавление / Изменение ключа реестра

Выбрать

При нажатии на кнопку открывается окно **Выбор ключа в реестре**, где вы можете выбрать ключ реестра, доступ к которому должен контролировать Контроль программ.

Название

В поле можно указать название ресурса с ключом реестра.

Путь к ключу

В поле можно указать путь к ключу реестра.

Защитить значение ключа

Если флажок установлен, от изменения защищается только значение ключа, указанное в поле **Значение ключа**.

Если флажок снят, то защищаются все значения этого ключа реестра.

Если в поле **Значение ключа** не указано никакого значения, то защищается значение ключа реестра по умолчанию.

Флажок автоматически устанавливается при выборе ключа реестра.

Значение ключа

В поле можно указать значение ключа реестра, которое Контроль программ должен защищать от изменения.

Поле доступно, если установлен флажок **Защитить значение ключа**.

Добавить

При нажатии на кнопку ключ реестра добавляется в список ресурсов.

Окно Добавление / Изменение нецензурного слова

Маска нецензурного слова

Слово или маска слова, наличие которого в сообщении является признаком спама.

Весовой коэффициент нецензурного слова

Числовое значение, выражающее вероятность того, что письмо, содержащее нецензурное слово, является спамом. Чем выше весовой коэффициент, тем выше вероятность того, что письмо, в котором содержится нецензурное слово, является спамом.

Анти-Спам определяет письмо как спам, если сумма весовых коэффициентов нецензурных слов и запрещенных фраз в письме превышает установленное значение.

Статус

В блоке **Статус** вы можете указать, должен ли Анти-Спам проверять сообщения на наличие нецензурного слова:

- **Активно**. Анти-Спам проверяет сообщения на наличие нецензурного слова.
- **Неактивно**. Анти-Спам не проверяет сообщения на наличие нецензурного слова.

Окно Добавление / Изменение файла или папки

Название

В поле можно указать название ресурса с файлом или папкой, доступ к которым должен контролировать Контроль программ.

Путь

В поле вы можете вручную указать путь к файлу или папке.

При вводе пути вручную вы можете использовать маску. Маска `\*` позволяет указать, что нужно контролировать доступ ко всем файлам в выбранной папке. Маска `\*<расширение>` позволяет указать, что нужно контролировать доступ ко всем файлам с определенным расширением в выбранной папке.

Выбрать

При нажатии на кнопку открывается окно, где вы можете выбрать файл или папку.

Добавить

При нажатии на кнопку папка или файл добавляется в список ресурсов.

Окно завершения активации

Это окно открывается, если программа активирована успешно.

Готово

При нажатии на кнопку завершается процедура активации программы. Выполняется переход в окно лицензирования.

Окно Завершение регистрации на сайте My Kaspersky

Готово

При нажатии на кнопку выполняется подключение программы к сайту My Kaspersky.

Окно Запрещенные и разрешенные программы

В этом окне отображается список программ, которым разрешено или запрещено изменять настройки операционной системы. Пустой список означает, что вы еще не разрешали и не запрещали программам изменять настройки операционной системы.

Список программ

Список программ содержит следующую информацию:

- **Программа**. В графе отображается название программы.
- **Имя файла**. В графе отображается название исполняемого файла программы.
- **Путь**. В графе отображается путь к исполняемому файлу программы на жестком диске вашего компьютера.
- **Издатель**. В графе отображается цифровая подпись издателя программы.
- **Изменения**. В графе отображается, запрещено или разрешено программе изменять настройки операционной системы, браузеров, а также настройки сети.

Окно Защита приватности

Доступ к веб-камере разрешен / запрещен

В блоке представлена информация о состоянии компонента Защита веб-камеры.

Если каким-либо программам запрещен доступ к веб-камере, в блоке отображается ссылка **<N> программам запрещен доступ к веб-камере**. По ссылке открывается окно **Программы, которым запрещен доступ к веб-камере**.

Защита от сбора данных включена / выключена

В блоке представлена информация о состоянии компонента Защита от сбора данных. Компонент защищает от сбора информации о вашей активности на сайтах.

По кнопке **Включить** можно включить компонент. Кнопка отображается, если компонент Защита от сбора данных выключен.

Вы можете настроить работу компонента, выбрав один из вариантов действия.

- **Только собирать статистику**. При выборе этого варианта компонент Защита от сбора данных работает в *режиме обнаружения*, предоставляя вам возможность просмотреть отчеты об обнаруженных попытках сбора данных.

- **Запретить сбор данных**. При выборе этого варианта компонент Защита от сбора данных работает в *режиме блокировки*, обнаруживая и блокируя попытки сбора данных. Информация о попытках сбора данных записывается в отчет.

По кнопке **Выключить** можно выключить компонент. Кнопка отображается, если компонент Защита от сбора данных включен.

Окно Интернет-магазин

В этом окне вы можете ознакомиться с предложениями интернет-магазина и приобрести лицензии на использование программ "Лаборатории Касперского". Если вы приобрели лицензию ранее, вы можете продлить срок ее действия.

Для некоторых программ вы можете выбрать нужный срок действия лицензии и количество компьютеров, на которые вы хотите установить программу, а также включить автоматическое продление подписки.

Для доступа в интернет-магазин через интерфейс Kaspersky Anti-Virus программе требуется установить безопасное соединение с сервером "Лаборатории Касперского" по протоколу HTTPS.

Окно Исключения

Исключения

В список **Исключения** попадают пропущенные вами обновления установленных программ. Вы можете пропустить как отдельное обновление, так и все обновления для программы, установленной на компьютере.

Список **Исключения** состоит из следующих граф:

- **Программа** – в графе отображается название программы.
- **Пропускать** – графа может содержать следующие значения:
  - **Версия обновления** – отображается, если вы пропустили отдельное обновление для установленной программы.
  - **Все обновления** – отображается, если вы решили не обновлять программу.

Удалить из списка

При нажатии на кнопку выбранные программы удаляются из списка исключений. Кнопка доступна, если программа выбрана в списке.

Kaspersky Anti-Virus будет сообщать о наличии обновлений для программ, удаленных из списка.

Окно Исключения Защиты от сбора данных

Список исключений

Список включает в себя адреса сайтов, на которых разрешен сбор данных о ваших действиях. На указанных сайтах компонент Защита от сбора данных обнаруживает попытки сбора данных, но не блокирует их, даже если в настройках компонента указано блокировать сбор данных этими категориями сервисов отслеживания.

Вы можете добавить в список веб-адрес или маску веб-адреса.

Изменить

Открывает окно, в котором можно изменить выбранный веб-адрес / маску веб-адреса.

Удалить

Удаляет из списка выбранный веб-адрес / маску веб-адреса.

Добавить

Открывает окно, в котором можно добавить веб-адрес / маску веб-адреса.

Окно Исключения

Исключения

В список попадают программы, которые вы скрыли из списка обнаруженных программ, сформированного в результате анализа установленных программ. В списке отображается название программы и название компании-производителя программы.

Удалить из списка

При нажатии на кнопку выбранная программа удаляется из списка исключений. Кнопка доступна, если программа выбрана в списке.

Программы, удаленные из списка исключений, отображаются в списке обнаруженных программ, сформированном в результате анализа установленных программ.

Окно Использование программ

Программа

В графе отображаются программы и группы программ, использование которых вы можете ограничить.

Использование

В графе указано, разрешено или запрещено пользователю работать с программой или группой программ:

- **Разрешено** – пользователь может работать с этой программой или группой программ.
- **Заблокировано** – пользователю запрещено работать с этой программой или группой программ.
- **Ограничено** – пользователь может работать с этой программой или группой программ ограниченное количество времени.

Вы можете разрешить, запретить или ограничить использование программы или группы программ для выбранного пользователя, выбрав нужный пункт раскрывающегося списка.

Путь

В графе отображается путь к исполняемому файлу программы.

Правила

По кнопке открывается окно, где вы можете ограничить использование выбранной программы по времени.

Удалить

Нажатие на кнопку удаляет выбранную программу из списка. После удаления программы из списка Kaspersky Anti-Virus перестает контролировать использование программы, пользователь может работать с этой программой без ограничений.

Добавить программу

По кнопке открывается окно, в котором вы можете выбрать исполняемый файл программы для добавления в список. Родительский контроль помещает программу в подходящую категорию в списке.

Окно Карантин

Список объектов на карантине

Содержит перечень файлов, помещенных на карантин. Карантин предназначен для хранения резервных копий файлов, которые были удалены или изменены в процессе лечения.

Файл

Графа, в которой отображается имя файла, помещенного на карантин.

По правой клавише мыши открывается контекстное меню, из которого можно перейти к действиям с файлом, помещенным на карантин: восстановлению, удалению, открытию файла в его исходной папке.

Путь

Графа, в которой отображается путь к файлу.

Обнаружено

Графа, в которой отображается тип обнаруженного объекта, например, *Сетевая атака*.

Дата

Графа, в которой отображается дата и время помещения файла на карантин.

Восстановить

При нажатии на кнопку Kaspersky Anti-Virus возвращает файл, выбранный в списке, в папку, в которой он находился до помещения на карантин.

Удалить

Кнопка, при нажатии на которую Kaspersky Anti-Virus удаляет файл, выбранный в списке.

Удалить все файлы

При нажатии на кнопку Kaspersky Anti-Virus удаляет все резервные копии файлов, помещенные на карантин.

Kaspersky Anti-Virus 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 Anti-Virus 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.

Окно Категории

В этом окне вы можете выбрать категории уязвимостей сетей Wi-Fi. Если для уязвимости установлен флажок, программа будет предупреждать вас о том, что вы подключаетесь к сети Wi-Fi, в которой есть эта уязвимость.

Сеть без пароля

В сети, не защищенной паролем, все данные передаются в открытом виде без шифрования, поэтому они легко доступны для злоумышленников. Установите флажок, чтобы программа показывала уведомление о том, что вы подключаетесь к сети Wi-Fi без пароля.

Слабое шифрование

Если в сети используется слабое шифрование, злоумышленники могут легко взломать такую сеть и перехватить ваши данные. Установите флажок, чтобы программа показывала уведомление о том, что вы подключаетесь к сети Wi-Fi со слабым шифрованием.

Распространенное имя сети

Если у сети распространенное имя, злоумышленники могут легко подобрать пароль к такой сети с помощью специальных программ для взлома. Установите флажок, чтобы программа показывала уведомление о том, что вы подключаетесь к сети Wi-Fi с распространенным именем.

Сеть с включенным WPS

WPS – это протокол для упрощенной настройки Wi-Fi сети, который может содержать уязвимость и, как следствие, быть неустойчивым к взлому. Установите флажок, чтобы программа показывала уведомление о том, что вы подключаетесь к сети Wi-Fi с включенным WPS.

Публичная сеть

Даже если публичная сеть защищена паролем, это не гарантирует безопасность. Если вместе с вами к публичной сети подключится злоумышленник, он сможет перехватить ваши данные с помощью специальных программ. Установите флажок, чтобы программа показывала уведомление о том, что вы подключаетесь к публичной сети Wi-Fi.

Окно Нецензурные слова

В этом окне представлен список нецензурных слов. По наличию этих слов Kaspersky Anti-Virus определяет, что сообщение является спамом.

Кнопка

При нажатии на кнопку открывается меню, в котором можно выбрать действие:

- Импортировать и добавить к существующему. При выборе этого действия можно загрузить список нецензурных слов из файла формата CSV. Текущие фразы не удаляются.
- Импортировать и заменить существующий. При выборе этого действия можно загрузить список нецензурных слов из файла формата CSV. Текущие фразы удаляются.
- Экспортировать. При выборе этого действия можно сохранить список нецензурных слов в файле формата CSV.

Нецензурное слово

Графа, в которой отображается слово или словосочетание. Наличие этого слова или словосочетания может означать, что сообщение является спамом.

Вес

В графе отображается весовой коэффициент, присвоенный нецензурному слову. Если в сообщении несколько нецензурных слов, суммарный коэффициент которых превышает 100, такое сообщение считается спамом.

Статус

Графа, в которой указано, использует ли Анти-Спам это слово при проверке сообщений на наличие нецензурных слов.

- **Активно**. Программа проверяет наличие этого слова в сообщениях.
- **Неактивно**. Программа не проверяет наличие этого слова в сообщениях.

Изменить

При нажатии на кнопку открывается окно, в котором можно изменить выбранное в списке нецензурное слово или маску слова.

Удалить

При нажатии на кнопку можно удалить нецензурное слово.

Добавить

При нажатии на кнопку открывается окно, в котором можно добавить в список нецензурное слово или маску слова.

Окно Новости

Список новостей

Новости в окне представлены в виде списка. Для каждой новости указывается ее заголовок, анонс, время появления.

По нажатию на заголовок новости открывается окно с текстом новости.

Окно Новость

Ссылки на Twitter и социальные сети

По ссылкам можно перейти на ваши страницы в социальных сетях или в Twitter для публикации новости. Текст публикации можно дополнить.

Если вход на страницу не был выполнен, сайт социальной сети откроется на странице авторизации.

Ссылки на социальные сети отображаются, если их посещение разрешено.

Кнопки 

Кнопки, с помощью которых можно переходить к предыдущей или следующей новости.

Окно Облачная защита

Узнать больше

При нажатии на кнопку открывается окно с информацией о Kaspersky Security Network.

Принять участие в Kaspersky Security Network

По кнопке открывается окно, где вы можете просмотреть Положение о Kaspersky Security Network и принять или отказаться от участия в Kaspersky Security Network.

Кнопка доступна, если вы отказались от участия в программе Kaspersky Security Network.

В некоторых случаях "Лаборатория Касперского" может вводить временные ограничения на запросы репутации файлов из Kaspersky Security Network. В случае действия временных ограничений на запрос информации из Kaspersky Security Network в левой части окна отображается соответствующее уведомление.

Окно Обновление баз

Обновить

Кнопка, при нажатии на которую запускается обновление баз и программных модулей.

Последнее обновление: <время последнего обновления>

По ссылке открывается окно **Подробные отчеты**, в котором можно просмотреть информацию о выполненных обновлениях баз и программных модулей.

Режим запуска: <название режима запуска>

По ссылке открывается окно **Настройки обновления**. В окне можно настроить режим запуска обновлений.

Кнопка 

При нажатии на кнопку обновление отменяется, и базы и программные модули остаются в прежнем состоянии.

Кнопка отображается во время обновления баз и программных модулей.

Загружено: <совокупный размер загруженных файлов>

По ссылке открывается окно **Подробные отчеты**, в котором можно просмотреть информацию о выполненных обновлениях баз и программных модулей.

Ссылка отображается во время обновления баз и программных модулей.

Обзор вирусной активности в мире

По ссылке открывается окно браузера на странице securelist.com, содержащей обзор вирусной активности на текущий момент.

Окно Обновление программ

Окно содержит список доступных обновлений для программ, установленных на компьютере.

Обновить все

При нажатии на кнопку Kaspersky Anti-Virus скачивает и устанавливает все доступные обновления для программ, которые отображаются в списке.

Обновить

При нажатии на кнопку Kaspersky Anti-Virus скачивает и устанавливает обновление для выбранной программы.

Кнопка

При нажатии на кнопку раскрывается меню, в котором можно выбрать следующие пункты:

- **Не обновлять эту программу** – Kaspersky Anti-Virus помещает программу в список исключений и не отображает уведомления о наличии обновлений для этой программы.
- **Пропустить это обновление** – Kaspersky Anti-Virus помещает обновление для программы в список исключений и не отображает уведомление о нем.
- **Открыть сайт производителя** – в браузере, установленном в операционной системе по умолчанию, открывается веб-сайт компании-производителя программы. На веб-сайте вы можете ознакомиться с обновлением и скачать его вручную.

Окно Обновление программ

Начать поиск

При нажатии на кнопку запускается поиск обновлений для программ, установленных на компьютере.

Остановить

При нажатии на кнопку поиск обновлений для установленных программ останавливается.

Кнопка отображается во время поиска обновлений.

Окно Настройки Менеджера программ

Включить / выключить Менеджер программ

Включение Менеджера программ. Если переключатель включен, программа Kaspersky Anti-Virus контролирует установку и удаление дополнительных программ, а также показ шагов установки, содержащих рекламу.

Во время установки программ автоматически снимать флажки установки дополнительных программ. Предупреждать при попытке установить дополнительные программы

Если флажок установлен, при установке программ на ваш компьютер Kaspersky Anti-Virus блокирует установку дополнительных программ.

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

Функциональность помощника по установке ограничена в Microsoft Windows XP (x64). Функциональность помощника по установке может быть недоступна для некоторых программ по установке.

Не отображать шаги установки, которые могут содержать рекламу или предложения об установке дополнительных программ

Если флажок установлен, при установке программ на ваш компьютер Kaspersky Anti-Virus блокирует показ рекламы или предложений об установке дополнительных программ.

Выполнять анализ установленных программ и расширений браузеров

Если флажок установлен, Kaspersky Anti-Virus будет регулярно анализировать установленные программы и расширения браузеров с точки зрения возможных причин для их удаления.

Выбрать категории объектов

По ссылке открывается окно, в котором вы можете выбрать категории установленных программ и расширений браузеров, которые Kaspersky Anti-Virus будет анализировать с точки зрения возможных причин для их удаления.

Настроить расписание

По ссылке открывается окно, в котором вы можете указать, в какие дни и в какое время Kaspersky Anti-Virus будет проводить анализ установленных программ и расширений браузеров.

Исключения

По ссылке открывается окно **Исключения**. В окне представлены программы, которые вы добавили в список исключений, нажав на кнопку **Игнорировать** в списке обнаруженных программ компонента Очистка компьютера.

Окно Настройки обновления программ

Включить поиск обновлений для программ

Если флажок установлен, Kaspersky Anti-Virus ищет обновления для установленных программ и предлагает скачать и установить их.

Задать режим поиска обновлений

По ссылке открывается окно, в котором вы можете задать режим поиска обновлений для программ, установленных на вашем компьютере.

Автоматически скачивать и устанавливать обновления, если не требуется принимать новое лицензионное соглашение

Если флажок установлен, Kaspersky Anti-Virus автоматически ищет обновления для установленных программ, а также скачивает и устанавливает найденные обновления, если для этого от вас не требуется принять новое лицензионное соглашение.

Искать обновления для программ

В настройке требуется выбрать, какие обновления программ будет скачивать и устанавливать Kaspersky Anti-Virus:

- **Важные обновления, которые повышают безопасность компьютера** – Kaspersky Anti-Virus устанавливает для программ только важные обновления, которые устраняют уязвимости и повышают безопасность вашего компьютера.
- **Все обновления для известных программ** – Kaspersky Anti-Virus устанавливает для программ все обновления.

Исключения

По ссылке открывается окно **Исключения** со списком исключений. В список исключений попадают пропущенные вами обновления установленных программ. Вы можете пропустить как отдельное обновление, так и все обновления для программы, установленной на компьютере.

Окно Настройки обновления

Задать режим запуска обновлений баз

По ссылке открывается окно **Режим запуска обновлений баз**. В окне можно сформировать расписание, в соответствии с которым Kaspersky Anti-Virus будет запускать задачу обновления.

Настроить источники обновлений

По ссылке открывается окно **Источник обновлений**. В окне можно выбрать источник обновлений баз программы.

Настройки учетной записи

По ссылке открывается окно **Настройки учетной записи**. В окне можно указать данные учетной записи пользователя (логин и пароль), от имени которого будет запускаться задача обновления.

Окно Поиск уязвимостей

Начать поиск

Кнопка, при нажатии на которую запускается поиск уязвимостей.

Остановить

Кнопка, при нажатии на которую поиск уязвимостей останавливается.

Кнопка отображается, если запущен поиск уязвимостей.

<N> уязвимых программ

По ссылке открывается окно **Уязвимые программы** со списком уязвимых программ, обнаруженных при проверке. Ссылка отображается, если был запущен поиск уязвимостей.

<N> уязвимостей в операционной системе

По ссылке открывается окно **Уязвимости операционной системы** со списком уязвимостей в операционной системе, обнаруженных при проверке. Ссылка отображается, если был запущен поиск уязвимостей.

Окно Приостановка защиты

Приостановить на указанное время

Режим возобновления работы компонентов защиты, при котором защита автоматически включается через указанный вами промежуток времени.

Промежуток времени вы можете указать в раскрывающемся списке ниже.

Приостановить до перезапуска программы

Режим возобновления работы компонентов защиты, при котором защита включается после перезапуска программы или перезагрузки операционной системы (при условии, что включен автоматический запуск программы).

Приостановить

Режим возобновления работы компонентов защиты, при котором защита включится только тогда, когда вы сами решите возобновить ее.

Окно Проверка пароля

Пароль

Пароль, ограничивающий доступ к управлению Kaspersky Anti-Virus.

Запомнить пароль на эту сессию

Если флажок установлен, Kaspersky Anti-Virus запоминает введенный пароль и больше не запрашивает его во время текущего сеанса работы.

Окно Программы, которым запрещен доступ к веб-камере

В окне отображаются программы, которым вы запретили доступ к веб-камере.

Разрешить доступ к веб-камере

При нажатии на кнопку программе, выбранной в списке, разрешается доступ к веб-камере.

Окно Регистрация на сайте My Kaspersky

Адрес электронной почты

Поле для ввода адреса электронной почты для регистрации на My Kaspersky.

Пароль

Поле для ввода пароля для регистрации на My Kaspersky.

Повторите пароль

Поле для подтверждения пароля для My Kaspersky.

Я соглашаюсь предоставить "Лаборатории Касперского" адрес своей электронной почты для получения персональных маркетинговых предложений

Если флажок установлен, вы будете получать новости от "Лаборатории Касперского" на указанный адрес электронной почты.

Создать

При нажатии на кнопку выполняется регистрация учетной записи My Kaspersky. На указанный вами при регистрации адрес электронной почты придет письмо, содержащее ссылку для активации учетной записи My Kaspersky.

Окно Режим Безопасных программ

В блоке **Режим Безопасных программ** можно включить или выключить режим Безопасных программ.

Узнать больше

Ссылка, по которой открывается окно браузера на сайте Службы технической поддержки с подробной информацией о режиме Безопасных программ.

Включить

После нажатия на кнопку начинается запуск режима Безопасных программ. Перед запуском режима Безопасных программ Kaspersky Anti-Virus анализирует программы, установленные на вашем компьютере. В процессе анализа Kaspersky Anti-Virus определяет, целесообразно ли использовать режим Безопасных программ на вашем компьютере.

Кнопка отображается, если режим Безопасных программ выключен. Кнопка не отображается во время анализа установленных программ.

Остановить

При нажатии на кнопку Kaspersky Anti-Virus останавливает анализ программ, установленных на вашем компьютере.

Кнопка отображается во время анализа программ, который Kaspersky Anti-Virus выполняет перед запуском режима Безопасных программ.

<количество> запусков

По ссылке открывается окно **История вызова модулей**. В этом окне можно просмотреть информацию о модулях программ, запуск которых был заблокирован или разблокирован.

Ссылка отображается, если включен режим Безопасных программ.

Управление программами

По ссылке открывается окно **Управление программами**. В этом окне можно указать группы доверия программ, разрешить или запретить запуск программ, а также перейти к настройке разрешений для отдельной программы.

Выключить

По ссылке вы можете выключить режим Безопасных программ.

Ссылка отображается, если режим Безопасных программ включен.

Включить и проверить все установленные программы

По ссылке запускается анализ операционной системы и установленных программ и открывается окно **Анализ установленных программ**. В этом окне отображается информация о текущих результатах анализа операционной системы и установленных программ и о времени, оставшемся до окончания анализа.

Ссылка отображается, если режим Безопасных программ выключен.

Окно Рекомендуемая настройка

Включить защиту от рекламных предложений, чтобы устанавливать только нужные программы и блокировать дополнительные установки

Если флажок установлен, Kaspersky Anti-Virus блокирует показ рекламы во время установки на компьютер какого-либо программного обеспечения. При этом блокируется также установка предлагаемых в рекламе дополнительных программ.

Готово

При нажатии на кнопку вы переходите в главное окно программы.

Окно Удаление программ

В окне представлен список программ, которые, возможно, имеют нестандартную установку или удаление, редко используются или являются рекламными.

Скрыть

При нажатии на кнопку строка с информацией об обнаруженной программе перестает отображаться в списке. Kaspersky Anti-Virus добавляет эту программу в список исключений.

Удалить

При нажатии на кнопку запускается процесс удаления обнаруженной программы.

Окно Отчеты

Список событий за день

Список содержит события, которые программа Kaspersky Anti-Virus зафиксировала в течение суток.

В состав списка могут входить события следующих типов:

- обнаруженные объекты;
- обновления баз и программных модулей;
- произведенные проверки.

Для событий каждого типа отображается ссылка, по которой можно открыть окно с подробным описанием этих событий.

Период

Период, за который формируется отчет.

Можно сформировать отчеты за следующие периоды:

- за сутки;
- за последнюю неделю;
- за последний месяц;
- за все время.

Список событий за выбранный период

Список содержит события, которые программа Kaspersky Anti-Virus зафиксировала в течение выбранного периода.

В состав списка могут входить события следующих типов:

- обнаруженные объекты;
- обновления баз и программных модулей;
- произведенные проверки.

Для событий каждого типа отображается ссылка, по которой можно открыть окно с подробным описанием этих событий.

Подробные отчеты

По ссылке открывается окно **Подробные отчеты**, в котором отображается детальная информация о событиях Kaspersky Anti-Virus.

Окно Подробные отчеты

Список компонентов и задач

Список компонентов и задач расположен в левой части окна. В списке можно выбрать компонент программы или задачу, отчет о работе которых нужно отобразить в списке событий.

Период

Период, за который формируется отчет.

Можно сформировать отчеты за следующие периоды:

- за сутки;
- за последнюю неделю;
- за последний месяц;
- за все время.

Экспорт

При нажатии на кнопку открывается окно для выбора файла, в котором будет сохранена информация из отчета.

Список событий

Список событий расположен в левой части окна. Список содержит информацию о событиях, произошедших во время работы компонентов программы и / или при выполнении задач.

В правой части окна **Подробные отчеты** отображаются детальные сведения о событии, выбранном в списке. Если ни одно событие не выбрано, в правой части окна не отображается информация.

На операционной системе Windows 10 RS3 и выше во время полной или выборочной проверки Kaspersky Anti-Virus не проверяет файлы, хранящиеся в облачных хранилищах, например, OneDrive. Эти файлы проверяются Файловым Антивирусом во время их открытия или изменения.

Окно Настройки учетной записи

Запускать обновления баз с правами

Выбор учетной записи, с правами которой Kaspersky Anti-Virus будет запускать задачи обновления. Функция доступна для запуска задачи обновления Kaspersky Anti-Virus как вручную, так и по сформированному расписанию.

Возможны следующие варианты:

- **Текущего пользователя**. Задачи обновления будут запускаться с правами текущей учетной записи, под которой вы зарегистрированы в операционной системе.
- **Другого пользователя**. Задачи обновления будут запускаться от имени указанного пользователя. При выборе этого варианта вам нужно указать имя и пароль учетной записи в полях **Учетная запись** и **Пароль**.

Окно Поддержка

Блок **Поддержка "Лаборатории Касперского"** содержит информацию, необходимую для обращения в Службу технической поддержки "Лаборатории Касперского": версию Kaspersky Anti-Virus, дату и время выпуска баз программы, версию операционной системы, ключ.

Лицензионный ключ

По ссылке **<ключ>** открывается окно **Информация о лицензии**, в котором приведены сведения о действующей лицензии.

Посмотреть на My Kaspersky

По ссылке открывается сайт My Kaspersky на странице с информацией о коде активации, с помощью которого была активирована программа. Может потребоваться ввести имя пользователя и пароль от вашей учетной записи на My Kaspersky.

Другие версии

По ссылке открывается сайт, с которого вы можете загрузить версию программы, предназначенную для использования в вашем регионе. Ссылка доступна не во всех версиях программы.

Ответы на часто задаваемые вопросы

По ссылке открывается окно браузера на странице интерактивной поддержки. Эта страница содержит ответы на вопросы, которые пользователи чаще всего задают специалистам технической поддержки "Лаборатории Касперского".

Рекомендации по настройке программы

По ссылке открывается окно браузера на странице сайта Службы технической поддержки, где опубликованы статьи о настройке и использовании Kaspersky Anti-Virus.

Сообщество пользователей

По ссылке открывается окно браузера на странице сообщества "Лаборатории Касперского", где вы можете просматривать опубликованные темы, оставлять свои комментарии, создавать новые темы, пользоваться поиском.

Мониторинг проблем

По ссылке открывается окно **Мониторинг проблем**. В этом окне можно собрать техническую информацию о работе программы и создать отчет о состоянии системы.

Окно Мониторинг проблем

Запись событий

Текущий статус записи событий (включена / выключена). Показывает, ведется или нет отчет о состоянии операционной системы и о работе программы.

Раскрывающийся список

В раскрывающемся списке можно выбрать события, информацию о которых Kaspersky Anti-Virus будет сохранять в отчете о состоянии операционной системы и работе программы.

Возможные значения:

- **Ошибки**. Kaspersky Anti-Virus сохраняет в отчете сведения об ошибках, возникающих в работе программы.
- **Важные**. Kaspersky Anti-Virus сохраняет в отчете сведения о событиях, важных для обеспечения безопасности компьютера (например, об обнаружении возможно зараженного объекта или подозрительной активности в операционной системе).
- **Рекомендуемые**. Kaspersky Anti-Virus сохраняет в отчете сведения о важных событиях, а также о событиях, не имеющих первостепенной важности для обеспечения безопасности компьютера.
- **Все**. Kaspersky Anti-Virus составляет подробный отчет обо всех событиях, которые могут быть использованы для диагностики работы программы.

Настройка доступна, если запись событий включена.

Включить запись

При нажатии на кнопку включается запись отчета о состоянии операционной системы и работе программы.

Кнопка доступна, если запись событий выключена.

Кнопка 

При нажатии на кнопку Kaspersky Anti-Virus прекращает вести отчет о состоянии операционной системы и работе программы.

Кнопка доступна, если запись событий включена.

Как создать отчет об операционной системе

По ссылке в окне браузера по умолчанию открывается статья в Базе знаний, где вы можете получить информацию о том, как создать отчет об операционной системе.

Отправить отчет в Службу технической поддержки

По ссылке открывается окно **Отправка отчета**. Это окно позволяет отправить на FTP-сервер "Лаборатории Касперского" отчет о состоянии операционной системы и работе программы.

Удалить все служебные данные и отчеты

По ссылке можно удалить все файлы трассировки и отчеты. Если по ссылке не удалось удалить все файлы трассировки, необходимо перезагрузить компьютер и снова пройти по ссылке **Удалить все служебные данные и отчеты**.

Ссылка активна, если запись событий выключена.

Отправка отчета

Информация об операционной системе

Флажок позволяет добавить в отчет, отсылаемый на сервер Службы технической поддержки, информацию о состоянии операционной системы.

Полученные для анализа данные

Флажок позволяет добавить файлы трассировок и дампов в отчет, отсылаемый на сервер Службы технической поддержки. В этих файлах сохранена история выполнения программой всех команд, а также информация о состоянии программы.

По ссылке **<количество файлов>**, **<объем данных>** рядом с флажком открывается окно **Полученные для анализа данные**. В окне отображаются список файлов и суммарный объем информации, которая будет передана на сервер Службы технической поддержки.

Сохранить отчет на компьютере

По ссылке открывается окно для сохранения файла отчета.

Введите номер запроса

Номер, присвоенный вашему запросу при обращении в Службу технической поддержки через сайт My Kaspersky.

Отправить отчет

Кнопка, при нажатии на которую выбранные файлы загружаются на FTP-сервер Службы технической поддержки.

Окно Полученные для анализа данные

Список файлов данных

Список файлов, которые Kaspersky Anti-Virus включает в отчет, отсылаемый на сервер Службы технической поддержки. В состав списка входят файлы трассировок и дампов. В этих файлах сохранена история выполнения программой всех команд, а также информация о состоянии программы.

Если флажок в строке файла установлен, то файл будет загружен на сервер Службы технической поддержки. Перед загрузкой подготовленные файлы данных будут упакованы в архив.

Если флажок в строке файла снят, то файл не будет загружен на сервер Службы технической поддержки.

Файл

Графа, в которой указывается название файла, готового для отправки на сервер Службы технической поддержки.

Размер

Объем информации, который будет передан на сервер Службы технической поддержки, если указанный файл включен в состав отчета. Kaspersky Anti-Virus помещает файл в отчет, если установлен флажок в строке этого файла.

Запуск скрипта

Текст скрипта для выполнения

Текст скрипта, полученный от Службы технической поддержки.

Специалисты "Лаборатории Касперского" не рекомендуют самостоятельно вносить изменения в скрипт.

Выполнить

Кнопка, при нажатии на которую скрипт выполняется.

Выполнение скрипта AVZ

В этом окне отображается процесс выполнения скрипта AVZ. Выполнение скрипта может занять некоторое время.

Результат выполнения скрипта

Ошибка

Сообщение об ошибке. Выводится, если в скрипте AVZ были найдены ошибки. При этом работа мастера выполнения скрипта AVZ останавливается.

Готово

Кнопка, при нажатии на которую мастер выполнения скрипта AVZ завершает работу.

Результат выполнения скрипта

Закрыть

Кнопка, при нажатии на которую мастер выполнения скрипта AVZ завершает работу.

Изменить

По кнопке можно заново ввести скрипт и повторить попытку выполнения скрипта.

Окно Уязвимости операционной системы

Уязвимости операционной системы

Содержит перечень уязвимостей в операционной системе. Все найденные уязвимости Kaspersky Anti-Virus группирует в зависимости от опасности, которую они представляют для операционной системы. Для каждой группы уязвимостей Kaspersky Anti-Virus предлагает набор действий для их устранения. Выделены три группы уязвимостей и действий для их устранения:

- *Настоятельно рекомендуемые действия* помогут избавиться от уязвимостей, представляющих серьезную угрозу безопасности.
- *Рекомендуемые действия* направлены на устранение уязвимостей, которые могут представлять опасность.
- *Дополнительные действия* предназначены для устранения неопасных в данный момент уязвимостей, которые в дальнейшем могут поставить безопасность компьютера под угрозу.

Для каждой уязвимости из списка доступны следующие кнопки:

- **Исправить**

Кнопка, при нажатии на которую Kaspersky Anti-Virus устраняет выбранную уязвимость.

- **Подробнее**

Кнопка, при нажатии на которую открывается сайт Службы технической поддержки с описанием угрозы, связанной с выбранной уязвимостью.

- **Отменить исправление**

Кнопка, при нажатии на которую Kaspersky Anti-Virus отменяет ранее выполненное исправление уязвимости.

Кнопка отображается для тех уязвимостей, которые были ранее исправлены, и в случае, если в списке **Просмотр** установлен флажок **Показать исправленные уязвимости**.

Просмотр

В раскрывающемся списке можно установить флажок **Показать исправленные уязвимости**, который включает / выключает отображение в списке исправленных уязвимостей.

Окно Уязвимые программы

Уязвимые программы

Содержит найденные в программах уязвимости.

Из-за особенностей работы службы обновлений уязвимости некоторых программ могут быть обнаружены повторно.

Для каждой найденной уязвимости доступны следующие кнопки:

- **Подробнее**

Кнопка, при нажатии на которую открывается сайт Службы технической поддержки с описанием угрозы. На сайте вы можете скачать нужное обновление для вашей версии программы и установить его.

- **Добавить в исключения**

Кнопка, при нажатии на которую Kaspersky Anti-Virus добавляет программу в доверенную зону.

Раздел Быстрая проверка

При быстрой проверке производится проверка системной памяти, загрузочных секторов диска и объектов, которые загружаются при запуске операционной системы.

Запустить

По ссылке запускается обновление баз и программных модулей.

Ссылка отображается, если базы и программные модули давно не обновлялись.

Запустить проверку

Кнопка, при нажатии на которую запускается проверка.

Остановить

Кнопка, при нажатии на которую проверка останавливается.

Кнопка отображается, если запущена проверка.

Возобновить проверку

По ссылке Kaspersky Anti-Virus возобновляет проверку, которая ранее была приостановлена.

Полный отчет

По ссылке открывается окно **Подробные отчеты** с детальной информацией о выполненной проверке. Ссылка отображается, если проверка выполнена или остановлена.

Расписание проверки

По ссылке раскрывается меню, содержащее следующие пункты:

- **Полная проверка** — открывает окно, в котором вы можете настроить расписание полной проверки.
- **Быстрая проверка** — открывает окно, в котором вы можете настроить расписание быстрой проверки.
- **Поиск уязвимостей** — открывает окно, в котором вы можете настроить расписание поиска уязвимостей.

Раздел Выборочная проверка

Запустить

По ссылке запускается обновление баз и программных модулей.

Ссылка отображается, если базы и программные модули давно не обновлялись.

Добавить

При нажатии на кнопку открывается окно **Выбор файла или папки для проверки**. В окне вы можете выбрать объекты, которые Kaspersky Anti-Virus должен проверить.

Запустить проверку

Кнопка, при нажатии на которую запускается проверка.

Остановить

Кнопка, при нажатии на которую проверка останавливается.

Кнопка отображается, если запущена проверка.

Список объектов для проверки

Список объектов содержит диски, файлы и папки, которые Kaspersky Anti-Virus проверяет при выполнении задачи выборочной проверки.

Если в список объектов пуст, отображается прямоугольная область, в которую вы можете перетащить объекты для проверки. Также вы можете выбрать объекты в окне **Выбор файла или папки для проверки**. Окно открывается по кнопке **Добавить**.

Рядом с каждым объектом в списке отображается кнопка ×, позволяющая удалить выбранный объект из списка проверки.

Удалить все

По ссылке Kaspersky Anti-Virus удаляет все элементы из списка объектов для проверки. Ссылка не отображается, если список пуст.

Полный отчет

По ссылке открывается окно **Подробные отчеты** с детальной информацией о выполненной проверке. Ссылка отображается, если проверка выполнена или остановлена.

Раздел Полная проверка

По умолчанию программа проверяет следующие объекты: системная память, объекты, исполняемые при старте операционной системы, резервное хранилище, жесткие и съемные диски.

Запустить

По ссылке запускается обновление баз и программных модулей.

Ссылка отображается, если базы и программные модули давно не обновлялись.

Запустить проверку

Кнопка, при нажатии на которую запускается проверка.

Остановить

Кнопка, при нажатии на которую проверка останавливается.

Кнопка отображается, если запущена проверка.

Возобновить проверку

По ссылке Kaspersky Anti-Virus возобновляет проверку, которая ранее была приостановлена.

Полный отчет

По ссылке открывается окно **Подробные отчеты** с детальной информацией о выполненной проверке. Ссылка отображается, если проверка выполнена или остановлена.

Расписание проверки

По ссылке раскрывается меню, содержащее следующие пункты:

- **Полная проверка** — открывает окно, в котором вы можете настроить расписание полной проверки.
- **Быстрая проверка** — открывает окно, в котором вы можете настроить расписание быстрой проверки.
- **Поиск уязвимостей** — открывает окно, в котором вы можете настроить расписание поиска уязвимостей.

По окончании проверки

По ссылке раскрывается список, в котором можно выбрать действие, выполняемое по окончании проверки:

- оставить компьютер включенным;
- выключить компьютер;
- перевести компьютер в режим ожидания;
- перевести компьютер в спящий режим;
- перезагрузить компьютер.

Ссылка отображается, если Kaspersky Anti-Virus выполняет проверку.

Раздел Проверка внешних устройств

Список внешних устройств

В раскрывающемся списке содержатся все мобильные устройства и съемные диски, подключенные к компьютеру.

Список отображается, если к компьютеру подключено хотя бы одно внешнее устройство.

Запустить проверку

Кнопка, при нажатии на которую запускается проверка.

Остановить

Кнопка, при нажатии на которую проверка останавливается.

Кнопка отображается, если запущена проверка.

Полный отчет

По ссылке открывается окно **Подробные отчеты** с детальной информацией о выполненной проверке. Ссылка отображается, если проверка выполнена или остановлена.

Перечисленные выше элементы интерфейса могут отображаться, если к компьютеру подключено хотя бы одно внешнее устройство.

Приостановка работы Файлового Антивируса

Приостановить

Флажок включает / выключает приостановку работы Файлового Антивируса на заданный промежуток времени.

Приостановка работы компонента позволяет снизить нагрузку на систему и обеспечить быстрый допуск к объектам.

Приостановить при запуске указанных программ

Список содержит перечень программ, при запуске которых работа Файлового Антивируса приостанавливается.

Например, можно добавить в список программы, требующие значительных ресурсов системы. После завершения работы такой программы Файловый Антивирус включится автоматически.

Добавить

По ссылке открывается окно для выбора исполняемого файла программы. После выбора исполняемого файла программа добавляется в список программ, при запуске которых приостанавливается работа Файлового Антивируса.

Удалить

По ссылке Kaspersky Anti-Virus удаляет из списка выбранную программу.

Настройки Защиты ввода данных

Узнать больше

По ссылке открывается окно браузера на странице с более подробной информацией о компоненте.

В блоке **Экранная клавиатура** вы можете изменить настройки вызова Экранной клавиатуры.

Открывать Экранную клавиатуру по комбинации клавиш CTRL+ALT+SHIFT+P

Флажок включает / выключает быстрый вызов Экранной клавиатуры по комбинации клавиш **CTRL**+**ALT**+**SHIFT**+**P**.

Показывать значок быстрого вызова в полях ввода

Флажок включает / выключает отображение значка быстрого вызова Экранной клавиатуры в полях ввода данных на сайтах.

По умолчанию флажок снят до первой после установки программы перезагрузки компьютера. После перезагрузки компьютера флажок установлен.

Изменить категории

По ссылке открывается окно **Категории**. В этом окне можно указать, на каких сайтах нужно отображать значок быстрого вызова Экранной клавиатуры в полях ввода. В окне также можно сформировать списки веб-сайтов, на которых нужно включить или выключить отображение значка быстрого вызова Экранной клавиатуры вне зависимости от выбранных категорий сайтов.

В блоке **Защита ввода данных с аппаратной клавиатуры** можно включить защищенный ввод данных с помощью аппаратной клавиатуры, а также указать, ввод каких данных и на каких сайтах требуется защищать.

Защищать ввод данных с аппаратной клавиатуры

Флажок включает / выключает защиту ввода данных с аппаратной клавиатуры.

По умолчанию флажок установлен.

Изменить категории

По ссылке открывается окно **Категории**. В этом окне вы можете указать, на каких сайтах нужно защищать ввод данных с аппаратной клавиатуры, а также сформировать списки сайтов, на которых нужно включить или выключить защиту ввода данных с аппаратной клавиатуры вне зависимости от выбранных категорий сайтов.

Настройки отображения Kaspersky Anti-Virus

В блоке **Значок программы** вы можете выбрать внешний вид значка программы: стандартный значок или зеленый медведь Мидори Кума (талисман "Лаборатории Касперского").

Если вы хотите вернуть традиционный значок программы в виде буквы "K", это можно сделать в окне **О программе** с помощью сочетания клавиш **IDDQD**. Чтобы изменения вступили в силу, требуется перезагрузить компьютер.

В блоке **Значок программы в панели задач** вы можете включить анимацию значка программы в области уведомлений панели задач Windows.

Если анимация включена, то в зависимости от операции, которую выполняет Kaspersky Anti-Virus, вид значка изменяется. Например, если Kaspersky Anti-Virus скачивает обновления, на фоне значка вращается миниатюрный глобус.

Если анимация выключена, значок Kaspersky Anti-Virus отражает только состояние защиты вашего компьютера: если защита включена, значок цветной, если защита приостановлена или выключена – серый.

В блоке **Плавный переход между окнами** вы можете изменить настройки плавного перехода. Плавный переход между окнами выполняется в виде перемещения нового окна поверх старого.

В блоке **Тема оформления** вы можете выбрать тему оформления Kaspersky Anti-Virus, отличающуюся от стандартной. Чтобы выбрать тему оформления, требуется установить флажок **Использовать альтернативную тему оформления** и указать zip-файл или папку с темой оформления в окне, открывающемся по ссылке **Выбрать**.

Применение альтернативных тем оформления доступно не во всех регионах.

Окно Добавление / изменение исключения для аппаратной клавиатуры

Маска веб-адреса

Веб-адрес сайта, который нужно добавить в список. Вы можете указать веб-адрес или маску веб-адреса.

В блоке **Область применения** вы можете указать область, на которую распространяется действие исключения для защиты ввода данных с аппаратной клавиатуры.

Применить ко всему сайту

Защита ввода данных с аппаратной клавиатуры включена для любой страницы сайта, указанного в поле **Маска веб-адреса**.

Применить к указанной странице

Защита ввода данных с аппаратной клавиатуры включена только на веб-странице, указанной в поле **Маска веб-адреса**.

В блоке **Защита ввода с аппаратной клавиатуры** вы можете указать, будет ли Kaspersky Anti-Virus защищать ввод данных с аппаратной клавиатуры для выбранного сайта или веб-страницы.

Защищать

Kaspersky Anti-Virus защищает ввод данных с аппаратной клавиатуры для выбранного сайта или веб-страницы.

Не защищать

Kaspersky Anti-Virus не защищает ввод данных с аппаратной клавиатуры для выбранного сайта или веб-страницы.

Окно Исключения для защиты ввода с аппаратной клавиатуры

Список исключений

Содержит перечень сайтов, для которых установлены исключения из защиты ввода данных с аппаратной клавиатуры.

Маска веб-адреса

Адрес или маска адреса сайта, для которого установлено исключение для защиты ввода данных с аппаратной клавиатуры.

Область

Графа, в которой указана область применения исключения из защиты ввода данных с аппаратной клавиатуры (сайт или указанная страница сайта).

Защита

Графа, в которой указано, защищает ли Kaspersky Anti-Virus ввод данных с аппаратной клавиатуры для выбранного сайта или веб-страницы.

Изменить

При нажатии на кнопку открывается окно настройки исключения из защиты ввода данных с аппаратной клавиатуры. В окне можно изменить адрес сайта и изменить настройки защиты ввода с аппаратной клавиатуры на этом сайте.

Удалить

При нажатии на кнопку программа удаляет выбранный сайт из списка исключений в защите ввода данных с аппаратной клавиатуры.

Добавить

При нажатии на кнопку открывается окно исключения из защиты ввода данных с аппаратной клавиатуры. В окне можно добавить веб-сайт или отдельную веб-страницу, для которых нужно изменить настройки защиты ввода данных с аппаратной клавиатуры.

Раздел Дополнительно

Блок **Обновление** позволяет изменить настройки скачивания и установки баз и программных модулей Kaspersky Anti-Virus.

В блоке **Угрозы и исключения** можно сформировать список объектов, которые Kaspersky Anti-Virus не будет контролировать в процессе работы.

Блок **Самозащита** позволяет включить или выключить защиту файлов Kaspersky Anti-Virus, а также процессов в памяти и записей в системном реестре.

Блок **Сеть** позволяет включить или выключить контроль сетевых портов и проверки защищенных соединений, а также изменить настройки прокси-сервера.

Блок **Уведомления** позволяет включить или выключить отображение уведомлений о событиях в работе программы. Также в этом блоке вы можете настроить отображение актуальных для вас информационных материалов при посещении сайтов "Лаборатории Касперского" и ее партнеров.

Блок **Отчеты и карантин** позволяет изменить настройки хранения файлов, помещенных на карантин, а также настройки сохранения информации об обнаруженных угрозах в отчетах.

Блок **Дополнительные средства защиты и управления** позволяет управлять подключением к Kaspersky Security Network и к сайту My Kaspersky.

Блок **Вид** позволяет настроить настройки отображения уведомлений и вид значка программы.

Окно Добавление / изменение исключения для Экранной клавиатуры

Маска веб-адреса

Веб-адрес сайта, который нужно добавить в список. Вы можете указать веб-адрес или маску веб-адреса.

В блоке **Область применения** вы можете указать, к чему применяются настройки отображения значка Экранной клавиатуры: к сайту целиком или к указанной странице.

Применить ко всему сайту

Значок быстрого вызова Экранной клавиатуры отображается в полях ввода на любой странице сайта, указанного в поле **Маска веб-адреса**.

Применить к указанной странице

Значок быстрого вызова Экранной клавиатуры отображается в полях ввода только на веб-странице, указанной в поле **Маска веб-адреса**.

В блоке **Значок Экранной клавиатуры** вы можете указать, должна или не должна программа показывать значок Экранной клавиатуры на страницах, соответствующих заданной маске веб-адреса.

Показывать значок в окне браузера

Kaspersky Anti-Virus отображает значок быстрого вызова Экранной клавиатуры в полях ввода.

Не показывать значок в окне браузера

Kaspersky Anti-Virus не отображает значок быстрого вызова Экранной клавиатуры в полях ввода.

Окно Исключения для Экранной клавиатуры

Список исключений

Содержит сайты, для которых заданы индивидуальные настройки отображения значка быстрого вызова Экранной клавиатуры.

Маска веб-адреса

Маска веб-адреса, для которого установлены индивидуальные настройки отображения значка Экранной клавиатуры.

Область

В графе указано, к чему применяются настройки отображения значка Экранной клавиатуры: к сайту целиком или к указанной странице.

Значок

В графе отображается информация о том, должна или не должна программа показывать значок Экранной клавиатуры на веб-страницах, соответствующих заданной маске веб-адреса.

Изменить

При нажатии на кнопку открывается окно настройки исключения для Экранной клавиатуры. В окне можно изменить адрес сайта и настройки отображения значка быстрого вызова Экранной клавиатуры на этом сайте.

Удалить

При нажатии на кнопку программа удаляет выбранный сайт из списка исключений для Экранной клавиатуры.

Добавить

При нажатии на кнопку открывается окно добавления исключения для Экранной клавиатуры. В окне можно добавить веб-сайт или конкретную страницу, на которых нужно отображать или не отображать значок быстрого вызова Экранной клавиатуры в полях ввода.

Настройки отчетов и карантина

В блоке **Отчеты** вы можете изменить настройки формирования и хранения отчетов.

Хранить отчеты не более чем

Флажок включает / выключает функцию ограничения срока хранения отчетов. Срок хранения может составлять один день, одну неделю, один или шесть месяцев или один год.

Если флажок установлен, отчеты хранятся в течение срока, выбранного в раскрывающемся списке рядом с флажком. По истечении этого срока Kaspersky Anti-Virus удаляет отчет.

Если флажок снят, срок хранения отчетов не ограничен.

Ограничить размер файла отчетов до

Флажок включает / выключает функцию, которая ограничивает максимальный размер файла отчета. Максимальный размер файла указывается в мегабайтах.

Если флажок установлен, то по умолчанию максимальный размер файла отчета составляет 1024 МБ. Когда файл достигает максимального размера, самые старые записи удаляются из файла по мере добавления новых записей.

Если флажок снят, то размер файла отчета не ограничен.

Записывать в отчет некритические события

Флажок включает / выключает функцию, которая добавляет в отчет информацию обо всех событиях Kaspersky Anti-Virus.

Kaspersky Anti-Virus записывает в отчеты подробную информацию о неудачных обновлениях программы независимо от того, установлен флажок или нет. Программа прекращает запись подробной информации после первого удачного обновления и возобновляет запись при неудачном обновлении.

Очистить

При нажатии на кнопку Kaspersky Anti-Virus удаляет данные из папки отчетов.

По умолчанию Kaspersky Anti-Virus удаляет отчеты задач проверки, отчеты задачи обновления.

В блоке **Карантин** вы можете изменить настройки карантина.

Хранить объекты не более чем

Флажок включает / выключает функцию ограничения срока хранения объектов на карантине. Срок хранения может составлять один день, одну неделю, один или шесть месяцев или один год.

Если флажок установлен, объекты хранятся в течение срока, выбранного в раскрывающемся списке рядом с флажком.

Если флажок снят, срок хранения объектов не ограничен.

Ограничить размер карантина до

Флажок включает / выключает функцию, которая ограничивает максимальный размер карантина. Размер карантина указывается в мегабайтах.

Если флажок установлен, по умолчанию максимальный размер хранилища составляет 100 МБ. При достижении максимального размера самые старые объекты удаляются из хранилища, а новые добавляются.

Если флажок снят, размер хранилища не ограничен.

Настройки дополнительных средств защиты

В блоке **Kaspersky Security Network** вы можете принять или отменить участие в программе Kaspersky Security Network.

Kaspersky Security Network – это облачная база знаний "Лаборатории Касперского", которая содержит информацию о репутации программ и сайтов. 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.

Если вы установили программу на территории Европейского союза, вместо блока **Kaspersky Security Network** в этом окне отображается блок **Положение о Kaspersky Security Network**. Внимательно ознакомьтесь с данным положением. Положение содержит информацию о том, какие персональные данные вы передаете в "Лабораторию Касперского".

Включить

По кнопке открывается окно, где вы можете просмотреть Положение о Kaspersky Security Network и принять или отказаться от участия в Kaspersky Security Network.

Кнопка доступна, если вы отказались от участия в программе Kaspersky Security Network.

Выключить

При нажатии на кнопку прекращается ваше участие в Kaspersky Security Network. Вы можете возобновить участие в Kaspersky Security Network в любое время.

В блоке **Вы подключены к My Kaspersky** вы можете ознакомиться с информацией о сайте, перейти на сайт или отключить компьютер от него. Блок отображается, если компьютер подключен к сайту.

Если вы установили программу на территории Европейского союза, в этом окне также отображается блок **Положение об обработке данных для маркетинговых целей**. Это положение позволяет нам делать более выгодные предложения для вас. Внимательно ознакомьтесь с данным положением. Положение содержит информацию о том, какие персональные данные вы передаете в "Лабораторию Касперского".

Перейти на My Kaspersky

По ссылке открывается окно браузера на странице сайта My Kaspersky.

Отключиться от My Kaspersky

При нажатии на кнопку Kaspersky Anti-Virus отключается от My Kaspersky.

Использовать аппаратную виртуализацию, если она доступна

Если флажок установлен, для работы Защищенного браузера используется аппаратная виртуализация (гипервизор). Программа использует технологию гипервизора для дополнительной защиты от сложных вредоносных программ, которые могут похищать ваши персональные данные с помощью буфера обмена и фишинга. Флажок отображается в 64-разрядной версии Windows 8, Windows 8.1 и Windows 10.

Подробнее о том, что такое аппаратная виртуализация и как она работает, вы можете прочитать по ссылке.

Использовать расширенные возможности аппаратной виртуализации

Если флажок установлен, аппаратная виртуализация начинает работать при старте операционной системы. Также вы получаете больше возможностей по защите с помощью аппаратной виртуализации. В случае замедления быстродействия операционной системы, снимите этот флажок.

Окно Выбор источника обновлений

В этом окне можно указать папку, из которой Kaspersky Anti-Virus будет получать обновления баз и программных модулей.

Источник обновлений

Путь к папке, из которой Kaspersky Anti-Virus будет получать обновления баз и программных модулей. В поле можно указать путь к папке (локальной или сетевой) или FTP-серверу.

Окно Источники обновлений

Список источников обновлений

Список содержит адреса ресурсов, с которых Kaspersky Anti-Virus получает обновления баз и программных модулей. В графе **Источник** могут быть указаны FTP-, HTTP-сайт, путь к сетевой или локальной папке.

В процессе обновления Kaspersky Anti-Virus обращается к списку, выбирает первый по порядку адрес сервера и пытается скачать с него пакет обновлений. Если скачать пакет обновлений с выбранного адреса невозможно, Kaspersky Anti-Virus обращается к следующему адресу в списке и вновь пытается получить пакет обновлений.

Если в графе **Статус** в строке источника обновлений установлено значение *Активно*, то Kaspersky Anti-Virus использует этот источник обновлений.

Если в графе **Статус** в строке источника обновлений установлено значение *Неактивно*, то Kaspersky Anti-Virus не использует этот источник обновлений.

По умолчанию список содержит только источник обновлений **Серверы обновлений "Лаборатории Касперского"**. Этот источник обновлений недоступен для изменения и удаления.

При использовании источников обновлений, отличных от источника **Серверы обновлений "Лаборатории Касперского"**, необходимо убедиться, что обновления баз и программных модулей совместимы с используемой версией Kaspersky Anti-Virus.

Источник

В графе содержится адрес источника обновлений баз и программных модулей.

Статус

В графе отображается статус источника обновлений.

Если в графе **Статус** установлено значение *Активно*, то Kaspersky Anti-Virus использует этот источник обновлений.

Если в графе **Статус** установлено значение *Неактивно*, то Kaspersky Anti-Virus не использует этот источник обновлений.

Удалить

При нажатии на кнопку выбранный источник обновлений удаляется из списка.

Кнопка 

Перемещает выбранный источник обновлений на одну строку выше.

Кнопка 

Перемещает выбранный источник обновлений на одну строку ниже.

Добавить

При нажатии на кнопку открывается окно, в котором можно указать путь к новому источнику обновлений.

Режим запуска обновлений баз

Запускать обновление

В раскрывающемся списке можно указать периодичность запуска задачи обновления, а также настроить расписание запуска задачи:

- **Автоматически (рекомендуется)**. Kaspersky Anti-Virus проверяет наличие пакета обновлений в источнике обновлений с заданной периодичностью. Частота проверки может увеличиваться во время вирусных эпидемий и сокращаться при их отсутствии. Обнаружив пакет обновлений, Kaspersky Anti-Virus скачивает его и устанавливает на компьютер. Мы рекомендуем выбирать этот вариант, так как от этого зависит защита вашего компьютера.
- **Ежедневно**. Запуск задачи осуществляется каждый день. Время запуска задачи указывается в поле **Время**, расположенном ниже.
- **Еженедельно**. Запуск задачи осуществляется в тот день недели, который выбран в списке **День недели**, расположенном ниже. Время запуска задачи указывается в поле **Время**, расположенном ниже.
- **После запуска программы**. Запуск задачи осуществляется через 15 минут после каждого запуска Kaspersky Anti-Virus.
- **Вручную**. Вы сами запускаете задачу обновления в удобное время.

День недели

В раскрывающемся списке можно указать, в какой из дней недели должно запускаться обновление баз и программных модулей.

Этот элемент интерфейса отображается, если в списке **Запускать обновление** выбран элемент **еженедельно**.

Время

В поле ввода можно указать, в какое время должно запускаться обновление баз и программных модулей.

Этот элемент интерфейса отображается, если в списке **Запускать обновление** выбран элемент **еженедельно** или **ежедневно**.

Запускать пропущенные задачи обновления

Если флажок установлен, программа запускает пропущенные задачи. Например, если компьютер был выключен, программа запускает пропущенные задачи после его включения.

Если флажок снят, Kaspersky Anti-Virus не запускает пропущенные задачи, а выполняет следующую задачу по установленному расписанию.

Флажок отображается, если в списке выбрано значение **ежедневно** или **еженедельно**.

Настройки самозащиты

Включить самозащиту

Флажок включает / выключает механизм защиты Kaspersky Anti-Virus от изменения или удаления собственных файлов на диске, процессов в памяти, записей в системном реестре.

Если флажок установлен, также отключается возможность внешнего управления системной службой. Если отключено внешнее управление системной службой, Kaspersky Anti-Virus блокирует любую попытку удаленного управления сервисами программ. При попытке удаленного управления появляется уведомление над значком Kaspersky Anti-Virus в области уведомлений панели задач Microsoft® Windows® (если уведомления не отключены).

Разрешить управление настройками Kaspersky Anti-Virus через программы удаленного управления

Если флажок установлен, доверенные программы удаленного администрирования (такие как TeamViewer, LogMeIn и RemotelyAnywhere) могут изменять настройки Kaspersky Anti-Virus.

Недоверенным программам удаленного администрирования изменение настроек Kaspersky Anti-Virus будет запрещено, даже если флажок установлен.

Настройки сети

В блоке **Учет стоимости подключения** вы можете указать, должна ли программа ограничивать трафик на основе учета стоимости подключения к интернету. Блок отображается при работе в операционной системе Microsoft Windows 8 и выше.

Ограничивать трафик при лимитном подключении

Если флажок установлен, программа ограничивает собственный сетевой трафик в том случае, если подключение к интернету является лимитным. Kaspersky Anti-Virus определяет высокоскоростное мобильное подключение к интернету как лимитное, а подключение по Wi-Fi – как безлимитное.

Флажок отображается при работе в операционной системе Microsoft Windows 8 и выше.

В блоке **Обработка трафика** вы можете указать, должна ли программа внедрять в трафик скрипт при взаимодействии с веб-страницами.

Внедрять в трафик скрипт взаимодействия с веб-страницами

Если флажок установлен, Kaspersky Anti-Virus внедряет в трафик скрипт взаимодействия с веб-страницами. Этот скрипт обеспечивает работу таких компонентов как Проверка ссылок и Защита ввода данных.

В блоке **Контролируемые порты** вы можете выбрать режим контроля портов, в котором Почтовый Антивирус и Веб-Антивирус проверяют потоки данных.

Контролировать все сетевые порты

Режим контроля портов, при котором Почтовый Антивирус и Веб-Антивирус контролируют все открытые порты вашего компьютера.

Контролировать только выбранные порты

Режим контроля портов, при котором Почтовый Антивирус и Веб-Антивирус контролируют выбранные вами порты вашего компьютера.

Список портов, которые обычно используются для передачи почты и веб-трафика, включен в комплект поставки программы.

Выбрать

По ссылке открывается окно **Сетевые порты**. В окне вы можете сформировать списки контролируемых портов, а также программ, для которых Kaspersky Anti-Virus контролирует все порты.

В блоке **Проверка защищенных соединений** вы можете включить / выключить режим проверки защищенных соединений по протоколу SSL.

Сайты

По ссылке открывается окно со списком сайтов. Для этих сайтов не выполняется проверка защищенных соединений.

Не проверять защищенные соединения

Если выбран этот вариант, Kaspersky Anti-Virus не проверяет SSL-трафик.

Проверять защищенные соединения по запросу компонентов защиты

Kaspersky Anti-Virus использует установленный сертификат "Лаборатории Касперского" для проверки SSL-соединений, если этого требуют компоненты защиты Веб-Антивирус и Проверка ссылок.

Если эти компоненты выключены, Kaspersky Anti-Virus не проверяет SSL-соединения.

После того как Kaspersky Anti-Virus проверит SSL-соединение, в сертификатах сайтов может не отображаться название организации, на которую зарегистрирован сайт.

Если вы не хотите, чтобы программа проверяла SSL-соединение с сайтом, вы можете исключить сайт из проверки.

Всегда проверять защищенные соединения

Если выбран этот вариант, Kaspersky Anti-Virus всегда использует установленный сертификат "Лаборатории Касперского" для проверки безопасности соединения.

Соединение с использованием протокола SSL защищает канал обмена данными в интернете. Протокол SSL позволяет идентифицировать обменивающиеся данными стороны на основе электронных сертификатов, шифровать передаваемые данные и обеспечивать их целостность в процессе передачи.

Если при соединении с сервером Kaspersky Anti-Virus обнаружит некорректный сертификат (например, при его подмене злоумышленником), то Kaspersky Anti-Virus выводит на экран уведомление с предложением принять или отвергнуть сертификат либо просмотреть информацию о сертификате. Если Kaspersky Anti-Virus работает в автоматическом режиме защиты, то Kaspersky Anti-Virus без уведомления разрывает соединение, использующее некорректный сертификат.

В случае возникновения ошибок при проверке защищенных соединений

В раскрывающемся списке вы можете выбрать действие, которое выполняет программа, если на каком-либо сайте возникла ошибка проверки защищенных соединений.

- **Игнорировать**. Программа разрывает соединение с сайтом, на котором возникла ошибка проверки.
- **Спрашивать**. Программа показывает вам уведомление с предложением добавить адрес сайта в список сайтов, на которых возникли ошибки проверки. Адрес сайта будет проверен по базе вредоносных объектов.
- **Добавлять сайт в исключения**. Программа добавляет адрес сайта в список сайтов, на которых возникли ошибки проверки. Адрес сайта будет проверен по базе вредоносных объектов.

Сайты с ошибками проверки

По этой ссылке можно перейти в окно **Сайты с ошибками проверки**. В окне можно просмотреть сайты, которые не были проверены из-за того, что при подключении к ним возникли ошибки. Адреса сайтов были проверены по базе вредоносных объектов.

Настроить исключения

По ссылке открывается окно **Исключения**. В этом окне вы можете сформировать список сайтов, которые не будут проверять компоненты защиты Веб-Антивирус и Проверка ссылок.

Дополнительные настройки

По ссылке выполняется переход к окну, в котором можно настроить дополнительные настройки защищенных соединений.

В блоке **Прокси-сервер** вы можете изменить настройки подключения к прокси-серверу, который вы используете для выхода в интернет.

Настройки прокси-сервера, используемые по умолчанию, программа определяет на этапе установки.

Настройка прокси-сервера

По ссылке открывается окно **Настройки прокси-сервера**. В окне вы можете изменить настройки подключения программы к прокси-серверу.

В блоке **Mozilla Firefox и Thunderbird** вы можете выбрать хранилище сертификатов для продуктов Mozilla.

Проверять защищенный трафик в продуктах Mozilla

Если флажок установлен, Kaspersky Anti-Virus проверяет зашифрованный трафик в программах Mozilla. Доступ к некоторым сайтам по протоколу HTTPS может быть заблокирован.

Использовать хранилище сертификатов Windows (рекомендуется)

Выберите этот вариант, если вы хотите использовать для хранения локального доверенного сертификата Kaspersky Anti-Virus хранилище сертификатов Windows.

Использовать хранилище сертификатов Mozilla

Выберите этот вариант, если вы хотите использовать для хранения локального доверенного сертификата Kaspersky Anti-Virus хранилище сертификатов Mozilla.

Защищенные соединения

Блокировать соединения по протоколу SSL 2.0 (рекомендуется)

Флажок запрещает / разрешает установку соединения с удаленным сервером с использованием протокола SSL 2.0.

Если флажок установлен, Kaspersky Anti-Virus блокирует защищенные соединения, устанавливаемые по протоколу SSL 2.0, и отображает уведомление о блокировании соединения.

Если флажок снят, Kaspersky Anti-Virus позволяет устанавливать защищенные соединения по протоколу SSL 2.0 и не контролирует их.

Не рекомендуется использовать протокол SSL 2.0, так как он содержит недостатки, влияющие на безопасность передачи данных.

Не расшифровывать защищенные соединения с EV-сертификатом

Флажок включает / выключает расшифровку защищенных SSL-соединений с сертификатом EV (Extended Validation).

EV-сертификаты подтверждают подлинность сайтов и повышают безопасность соединения. Браузеры сообщают о наличии на сайте EV-сертификата с помощью значка замка в адресной строке браузера. Также браузеры могут полностью или частично окрашивать адресную строку в зеленый цвет.

Если флажок установлен, Kaspersky Anti-Virus не расшифровывает защищенные SSL-соединения с EV-сертификатами.

Если флажок снят, Kaspersky Anti-Virus расшифровывает защищенные SSL-соединения с EV-сертификатом. После расшифровки браузер не сообщает о наличии EV-сертификата на сайте.

Если вы впервые открываете сайт с EV-сертификатом, защищенное соединение будет расшифровано независимо от того, установлен флажок или нет.

Настройки прокси-сервера

Не использовать прокси-сервер

Переключатель включает / выключает использование прокси-сервера для выхода в интернет. Kaspersky Anti-Virus использует подключение к интернету в работе некоторых компонентов защиты, а также для обновления баз и программных модулей.

Автоматически определять настройки прокси-сервера

Kaspersky Anti-Virus определяет настройки прокси-сервера автоматически с помощью протокола WPAD (Web Proxy Auto-Discovery Protocol).

В случае, если по этому протоколу определить адрес не удается, Kaspersky Anti-Virus использует настройки прокси-сервера, указанные в браузере Internet Explorer. Kaspersky Anti-Virus не учитывает настройки прокси-серверов, указанные для других браузеров, установленных на компьютере пользователя.

Использовать указанные настройки прокси-сервера

Kaspersky Anti-Virus использует прокси-сервер, отличный от заданного в настройках соединения браузера.

Адрес

Содержит IP-адрес или символьное имя (URL) прокси-сервера.

Поле доступно, если выбрана настройка **Использовать указанные настройки прокси-сервера** (например, IP-адрес 192.168.0.1).

Порт

Порт прокси-сервера.

Поле доступно, если выбрана настройка **Использовать указанные настройки прокси-сервера**.

Использовать аутентификацию на прокси-сервере

Аутентификация – это проверка регистрационных данных пользователя.

Флажок включает / выключает использование аутентификации на прокси-сервере.

Если флажок установлен, то Kaspersky Anti-Virus попытается выполнить NTLM-, а затем BASIC-аутентификацию.

Если флажок не установлен или настройки прокси-сервера не указаны, то Kaspersky Anti-Virus попытается выполнить NTLM-аутентификацию с использованием учетной записи, от имени которой запущена задача (например, задача обновления).

Если аутентификация на прокси-сервере необходима, а вы не указали имя пользователя и пароль, или указанные данные по каким-либо причинам не были приняты прокси-сервером, откроется окно запроса имени пользователя и пароля. Если аутентификация пройдет успешно, Kaspersky Anti-Virus будет использовать в дальнейшем указанные имя пользователя и пароль. В противном случае Kaspersky Anti-Virus повторно запросит настройки аутентификации.

Имя пользователя

Имя пользователя, которое используется при аутентификации на прокси-сервере.

Пароль

Пароль для введенного имени пользователя.

Не использовать прокси-сервер для локальных адресов

Если флажок установлен, Kaspersky Anti-Virus не использует прокси-сервер при обновлении баз и программных модулей из локальной или сетевой папки.

Если флажок снят, Kaspersky Anti-Virus использует прокси-сервер при обновлении баз и программных модулей из локальной или сетевой папки.

Добавление / изменение сетевого порта

Описание

Поле, в котором указывается название сетевого порта.

Порт

Поле, в котором указывается номер сетевого порта.

Статус

В блоке **Статус** вы можете указать, должен ли Kaspersky Anti-Virus контролировать трафик, проходящий через этот порт.

Если установлено значение *Активно*, то Kaspersky Anti-Virus контролирует трафик, проходящий через порт.

Если установлено значение *Неактивно*, то Kaspersky Anti-Virus добавляет порт в список портов, но исключает порт из проверки.

Сетевые порты

Список

Содержит информацию о портах, соединение с которыми контролирует Kaspersky Anti-Virus.

Если в графе **Статус** в строке порта установлено значение *Активно*, то Kaspersky Anti-Virus контролирует трафик, проходящий через этот порт.

Если в графе **Статус** в строке порта установлено значение *Неактивно*, то Kaspersky Anti-Virus исключает этот порт из проверки, но не удаляет его из списка портов.

Список портов, которые обычно используются для передачи почты и веб-трафика, включен в комплект поставки Kaspersky Anti-Virus. По умолчанию Kaspersky Anti-Virus контролирует трафик, проходящий через все порты из этого списка.

Описание

Графа, в которой указано название порта.

Порт

Графа, в которой указан номер порта.

Статус

Графа, в которой указано, выполняет ли Kaspersky Anti-Virus проверку трафика, проходящего через порт.

Если в графе **Статус** установлено значение *Активно*, то Kaspersky Anti-Virus контролирует трафик, проходящий через порт.

Если в графе **Статус** установлено значение *Неактивно*, то Kaspersky Anti-Virus исключает порт из проверки, но не удаляет его из списка портов.

Изменить

При нажатии на кнопку открывается окно **Сетевой порт**. В окне вы можете изменить номер сетевого порта, выбранного в списке, и его описание.

Удалить

При нажатии на кнопку Kaspersky Anti-Virus удаляет выбранный сетевой порт из списка.

Добавить

При нажатии на кнопку открывается окно **Сетевой порт**. В окне вы можете добавить сетевой порт в список портов.

Контролировать все сетевые порты программ, которые уязвимы для сетевых атак

Если флажок установлен, Kaspersky Anti-Virus контролирует все сетевые порты программ, которые уязвимы для сетевых атак. Список уязвимых программ сформирован специалистами "Лаборатории Касперского".

Если флажок снят, Kaspersky Anti-Virus не контролирует порты, используемые программами, уязвимыми для сетевых атак.

Окно Исключения

Кнопка

При нажатии на кнопку открывается меню, в котором можно выбрать действие:

- **Импортировать и добавить к существующему**. При выборе этого действия можно загрузить список адресов сайтов, которые вы хотите исключить из проверки. Список адресов должен храниться в файле формата CSV. Текущие адреса не удаляются.
- **Импортировать и заменить существующий**. При выборе этого действия можно загрузить список адресов сайтов, которые вы хотите исключить из проверки. Список адресов должен храниться в файле формата CSV. Текущие адреса удаляются.
- **Экспортировать**. При выборе этого действия можно сохранить список адресов сайтов, которые вы исключили из проверки. Программа сохраняет список адресов в файл формата CSV.

Список исключений

Содержит адреса сайтов, которые вы добавили как исключение для компонентов Веб-Антивирус и Проверка ссылок.

Если в графе **Статус** в строке доменного имени установлено значение *Активно*, компоненты не проверяют сайт с этим доменным именем.

Если в графе **Статус** в строке доменного имени установлено значение *Неактивно*, компоненты проверяют сайт с этим доменным именем.

Изменить

Открывает окно, в котором можно изменить выбранное доменное имя и его статус.

Удалить

Удаляет из списка выбранное доменное имя.

Добавить

Открывает окно, в котором можно добавить доменное имя.

Окно Добавление / Изменение доменного имени

Доменное имя

В поле требуется указать доменное имя сайта, который требуется исключить из проверки. Вы можете изменить указанное в поле доменное имя.

Указанное доменное имя отображается в списке исключений. Компоненты программы проверяют доменное имя в зависимости от статуса, который вы выбрали.

Статус

В блоке **Статус** вы можете указать, должны ли компоненты программы проверять это доменное имя. Возможны следующие варианты:

- *Активно*. Компоненты не проверяют это доменное имя.
- *Неактивно*. Компоненты проверяют это доменное имя.

Настройки уведомлений

Уведомлять о событиях

Флажок включает / выключает уведомление о событиях.

Если флажок снят, Kaspersky Anti-Virus не уведомляет вас о событиях, возникающих в ходе работы, но записывает информацию о них в отчет.

Уведомления могут быть реализованы следующими способами:

- всплывающими сообщениями над значком Kaspersky Anti-Virus в области уведомлений панели задач;
- звуковыми оповещениями.

Восстановить все скрытые уведомления

По ссылке вы можете восстановить значения настроек отображения уведомлений. Если ранее вы заблокировали отображение уведомлений, эти уведомления снова будут отображаться.

Если скрытых уведомлений нет, ссылка недоступна.

Сопровождать уведомления звуковыми сигналами

Флажок включает / выключает звуковое сопровождение уведомлений.

По умолчанию уведомления о критических событиях (например, об обнаружении вредоносной программы) сопровождаются звуковым сигналом.

Изменить установленный по умолчанию звуковой сигнал на "визг свиньи" можно в окне **О программе** с помощью сочетания клавиш **IDKFA**.

На операционной системе Microsoft Windows 10 звуковое сопровождение уведомлений не работает.

Получать информационные и рекламные сообщения "Лаборатории Касперского"

Флажок включает / выключает отображение уведомлений о непрочитанных новостях в области уведомлений панели задач.

Если флажок снят, Kaspersky Anti-Virus продолжает получать информационные и рекламные сообщения "Лаборатории Касперского", но не отображает уведомления о них.

Отображать информацию о специальных предложениях

Флажок включает / выключает настройку отображения информации о программах и специальных предложениях на сайтах "Лаборатории Касперского" и сайтах компаний-партнеров.

Если флажок установлен, на сайтах отображаются специальные предложения о покупке программ, подобранные с учетом уже приобретенных вами лицензий на использование программ "Лаборатории Касперского".

Если флажок снят, на сайтах отображаются стандартные предложения о покупке программ.

Получать информацию о специальных предложениях для пользователей социальных сетей

Если флажок установлен, Kaspersky Anti-Virus определяет, являетесь ли вы пользователем социальных сетей, и отображает в новостях информацию о действиях "Лаборатории Касперского" в социальных сетях.

Если флажок снят, Kaspersky Anti-Virus отображает стандартные новости "Лаборатории Касперского".

Получать информационные и рекламные сообщения по истечении срока действия лицензии

Если флажок установлен, по истечении срока действия лицензии программа продолжает скачивать и показывать новые информационные и рекламные сообщения.

Если флажок снят, новые информационные и рекламные сообщения не скачиваются. Программа показывает сообщения, полученные до истечения срока действия лицензии.

Настройки угроз и исключений

В блоке **Типы обнаруживаемых объектов** можно указать типы объектов, которые должен обнаруживать Kaspersky Anti-Virus.

Обнаруживать другие программы, которые могут быть использованы злоумышленниками для нанесения вреда компьютеру или данным пользователя

Флажок включает / выключает обнаружение Kaspersky Anti-Virus программ, с помощью которых злоумышленник может нанести вред вашему компьютеру или хранящимся на нем данным.

В блоке **Исключения** можно сформировать список объектов, которые Kaspersky Anti-Virus не будет контролировать в процессе работы.

Настроить исключения

По ссылке выполняется переход к окну добавления исключений из проверки.

Можно исключать из проверки следующие объекты:

- файл определенного формата;
- группу файлов, определяемую по маске;
- папку или программу;
- процесс программы;
- объект, определяемый по названию или маске названия согласно классификации Вирусной энциклопедии.

Указать доверенные программы

По ссылке открывается окно со списком доверенных программ. Если программа внесена в список доверенных, то Kaspersky Anti-Virus не контролирует используемые этой программой объекты (например, файлы).

В блоке **Лечение активного заражения** можно выключить или выключить применение технологии лечения активного заражения.

Применять технологию лечения активного заражения

Если флажок установлен, то при обнаружении вредоносной активности в операционной системе Kaspersky Anti-Virus предлагает провести специальную расширенную процедуру *лечения активного заражения*. Эта процедура требуется в тех случаях, когда вредоносная программа уже выполняется на компьютере и Kaspersky Anti-Virus не может обезвредить ее другими способами. В процессе лечения активного заражения работа операционной системы приостанавливается, в связи с чем рекомендуется предварительно сохранить важные файлы. После окончания лечения активного заражения компьютер автоматически перезагружается.

Если флажок снят, то технология лечения активного заражения не применяется.

Доверенные программы

Список доверенных программ

Содержит доверенные программы, для которых отменен контроль используемых этими программами объектов (например, файлов).

Если в графе **Статус** в строке программы установлено значение *Активно*, то Kaspersky Anti-Virus исключает из проверки объект, используемый этой программой. При этом Kaspersky Anti-Virus по-прежнему проверяет исполняемый файл и процесс доверенной программы на вирусы и другие программы, представляющие угрозу.

Если в графе **Статус** в строке программы установлено значение *Неактивно*, то Kaspersky Anti-Virus проверяет исполняемый файл доверенной программы, процесс программы и объекты, используемые программой. При этом программа не удаляется из списка доверенных.

Программа

Графа, в которой отображается название доверенной программы.

Путь к файлу

Графа, в которой указан путь к исполняемому файлу программы.

Статус

Графа, в которой указано, выполняет ли Kaspersky Anti-Virus проверку объектов, используемых программой (например, файлов).

Если в графе **Статус** установлено значение *Активно*, то Kaspersky Anti-Virus исключает из проверки объект, используемый программой. При этом Kaspersky Anti-Virus по-прежнему проверяет исполняемый файл и процесс доверенной программы.

Если в графе **Статус** установлено значение *Неактивно*, то Kaspersky Anti-Virus проверяет исполняемый файл доверенной программы, процесс программы и объекты, используемые программой. При этом программа не удаляется из списка доверенных.

Изменить

При нажатии на кнопку открывается окно **Исключения для программы**. В окне вы можете изменить настройки исключений для выбранной программы.

Удалить

При нажатии на кнопку выбранная программа удаляется из списка.

Добавить

При нажатии на кнопку открывается окно выбора программы.

Исключения для программы

Не проверять открываемые файлы

Флажок включает / выключает исключение из проверки всех файлов, которые открываются этой программой.

Если флажок установлен, Kaspersky Anti-Virus исключает из проверки файлы, которые открываются выбранной программой.

Если флажок снят, Kaspersky Anti-Virus проверяет файлы, которые открываются выбранной программой.

Не контролировать активность программы

Флажок включает / выключает исключение из проверки любой активности программы в рамках работы Проактивной защиты.

Если флажок установлен, любая активность программы исключается из проверки компонентами Проактивная защита.

Если флажок снят, Kaspersky Anti-Virus будет проверять любую активность программы.

Не наследовать ограничения родительского процесса (программы)

Если флажок установлен, активность программы контролируется по заданным вами правилам или по правилам группы доверия, в которую входит эта программа.

Если флажок снят, программа наследует правила от родительской программы, которая ее запустила.

Не контролировать активность дочерних программ

Флажок включает / выключает исключение из проверки любой активности любой дочерней программы.

Разрешить взаимодействие с интерфейсом Kaspersky Anti-Virus

Если флажок установлен, программе разрешено управлять программой Kaspersky Anti-Virus, используя ее графический интерфейс. Необходимость разрешить программе управлять интерфейсом Kaspersky Anti-Virus может возникнуть при использовании программы для удаленного доступа к рабочему столу или программы, обеспечивающей работу устройства ввода данных. К таким устройствам относятся, например, сенсорные панели (тачпады), графические планшеты.

Не проверять весь / зашифрованный трафик

Флажок включает / выключает исключение из проверки сетевого трафика программы.

По ссылке можно выбрать вариант исключения сетевого трафика из проверки:

- **Не проверять весь трафик**. Kaspersky Anti-Virus исключает из проверки весь сетевой трафик программы.
- **Не проверять зашифрованный трафик**. Kaspersky Anti-Virus исключает из проверки только трафик программы, передаваемый по протоколу SSL.

Только для указанных IP-адресов

Флажок включает / выключает функцию исключения из проверки сетевого трафика программы для указанных IP-адресов.

IP-адреса, которые нужно исключать из проверки, можно указать в поле ввода, расположенном под флажком.

Если флажок установлен, Kaspersky Anti-Virus исключает из проверки сетевой трафик только для указанных IP-адресов.

Если флажок снят, Kaspersky Anti-Virus исключает из проверки все IP-адреса.

Только для указанных портов

Флажок включает / выключает функцию исключения из проверки сетевого трафика только для указанных портов.

Порты, которые нужно исключать из проверки, можно указать в поле ввода, расположенном под флажком.

Если флажок установлен, Kaspersky Anti-Virus исключает из проверки сетевой трафик только для указанных портов.

Если флажок снят, Kaspersky Anti-Virus исключает из проверки все порты.

Статус

- **Активно**. Если выбран этот вариант, исключения для выбранной программы применяются.
- **Неактивно**. Если выбран этот вариант, исключения для выбранной программы не применяются.

Окно Добавление / изменение исключения

Файл или папка

Файл (или папка), который нужно исключить из проверки.

Объект

Название объекта, который должен быть исключен из проверки. Название объекта указывается в соответствии с классификацией Вирусной энциклопедии.

В блоке **Компоненты защиты** можно указать компоненты защиты (например, Файловый Антивирус или Веб-Антивирус), в работе которых будет учитываться исключение.

По умолчанию новое исключение учитывается в работе всех компонентов защиты.

Комментарий

Дополнительная информация об исключении.

Статус

В блоке **Статус** можно указать статус исключения.

Если установлено значение *Активно*, Kaspersky Anti-Virus исключает из проверки файлы и папки.

Если установлено значение *Неактивно*, Kaspersky Anti-Virus проверяет файлы и папки.

Окно Исключения

Список исключений

Список содержит исключения из проверки.

Можно исключать из проверки следующие объекты:

- файл определенного формата;
- группу файлов, определяемую по маске;
- папку или программу;
- процесс программы;
- объект, определяемый по названию или маске названия согласно классификации Вирусной энциклопедии.

Если в графе **Статус** в строке исключения установлено значение *Активно*, то Kaspersky Anti-Virus исключает объект из проверки.

Если в графе **Статус** в строке исключения установлено значение *Неактивно*, то Kaspersky Anti-Virus проверяет объект.

Файл или папка

Графа, в которой указывается путь к файлу или папке, исключаемым из проверки.

Объект

Графа, в которой указывается маска названия объекта. При обнаружении объекта, соответствующего маске, Kaspersky Anti-Virus применяет исключение.

Для формирования маски можно использовать любые символы, допустимые в названиях файлов, в том числе специальные:

- * — любое количество произвольных символов.
- ? — любой один символ.

Название и расширение файла всегда пишутся через точку.

Примеры масок:

- *.EXE — все файлы с расширением EXE.
- *.EX? — все файлы с расширением EX?, где вместо ? может использоваться любой один символ.
- test — все файлы с именем test.

Компоненты защиты

В графе отображаются названия компонентов защиты, в работе которых учитывается исключение (например, Файловый Антивирус или Веб-Антивирус).

Если исключение учитывается в работе всех компонентов защиты, в графе отображается значение *Любые*.

Статус

В графе отображается статус исключения.

Если установлено значение *Активно*, то Kaspersky Anti-Virus исключает объект из проверки.

Если установлено значение *Неактивно*, то Kaspersky Anti-Virus проверяет объект.

Изменить

При нажатии на эту кнопку открывается окно, в котором вы можете изменить настройки выбранного в списке исключения.

Удалить

Кнопка, при нажатии на которую Kaspersky Anti-Virus удаляет выбранное исключение из списка.

Добавить

При нажатии на эту кнопку открывается окно, в котором вы можете добавить исключение в список исключений.

Раздел Защита

Список компонентов защиты

Содержит компоненты защиты, предназначенные для защиты компьютера от различных видов информационных угроз.

Каждый тип угроз обрабатывается отдельным компонентом защиты. Вы можете включать и выключать компоненты защиты независимо друг от друга, а также настраивать их работу.

Переключатель <компонент включен / выключен>

Переключатель позволяет включать / выключать компоненты защиты программы.

В зависимости от текущего состояния компонента переключатель имеет следующий вид:

 – компонент включен.

 – компонент выключен.

Настройки Защиты веб-камеры

Включить / выключить Защиту веб-камеры

Переключатель включает / выключает компонент Защита веб-камеры.

Запретить всем программам доступ к веб-камере

Если флажок установлен, то запрет на доступ к веб-камере распространяется на все установленные на вашем компьютере программы.

Если флажок снят, то Kaspersky Anti-Virus контролирует доступ программ к веб-камере на основе принадлежности программы к группе доверия:

- **Доверенные** – доступ к веб-камере разрешен.
- **Слабые ограничения** – при попытке доступа к веб-камере Kaspersky Anti-Virus выводит на экран окно с запросом разрешения на доступ этой программы к веб-камере.
- **Сильные ограничения** и **Недоверенные** – доступ к веб-камере запрещен.

Показывать уведомление, когда веб-камеру использует программа, которой это разрешено

Если флажок установлен, Kaspersky Anti-Virus выводит на экран уведомление при доступе к веб-камере программы, которой доступ разрешен. С помощью уведомления вы можете изменить настройки доступа программы к веб-камере, а также отказаться от дальнейшего отображения уведомлений.

Если флажок снят, уведомление не выводится.

Флажок доступен, если снят флажок **Запретить всем программам доступ к веб-камере**.

Раздел Менеджер задач

В разделе отображается список задач проверки, которые были выполнены или выполняются в текущий момент:

- Полная проверка.
- Быстрая проверка.
- Выборочная проверка.
- Проверка внешних устройств.
- Поиск уязвимостей.
- Поиск руткитов.
- Проверка во время простоя.
- Лечение активного заражения.

В верхней части окна отображается информация о текущих задачах: название задачи, индикатор выполнения, время, оставшееся до завершения задачи, информация о количестве проверенных файлов и обнаруженных угроз.

Остановить

При нажатии на кнопку Kaspersky Anti-Virus приостанавливает выполнение задачи. После этого информация о приостановленной задаче отображается в нижней части окна в списке выполненных задач.

В нижней части окна отображается список выполненных задач. Задачи в списке перечислены в порядке их выполнения: в начале списка отображаются задачи, выполненные последними. Каждый элемент списка содержит название задачи, процент ее выполнения, если задача была остановлена, информацию о времени, прошедшем с момента окончания задачи, о количестве проверенных файлов, обнаруженных и устраненных угроз.

Полный отчет

По ссылке открывается окно **Подробные отчеты** с детальной информацией о выполненной проверке. Ссылка отображается, если проверка выполнена или остановлена.

<N> угроз не устранено

По ссылке открывается окно **Центр уведомлений**, в котором вы можете выбрать действие в отношении найденных и не устраненных угроз.

<N> угроз устранено

По ссылке открывается окно **Карантин**, в котором приведен список резервных копий файлов, удаленных или измененных в процессе лечения.

<N> уязвимых программ

По ссылке открывается окно **Уязвимые программы** со списком уязвимых программ, обнаруженных при проверке. Ссылка отображается, если был запущен поиск уязвимостей.

<N> уязвимостей в операционной системе

По ссылке открывается окно **Уязвимости операционной системы** со списком уязвимостей в операционной системе, обнаруженных при проверке. Ссылка отображается, если был запущен поиск уязвимостей.

Раздел Общие

Защита

Переключатель включает / выключает все компоненты защиты Kaspersky Anti-Virus. Отключение компонентов защиты не влияет на выполнение текущих задач проверки и задачи обновления Kaspersky Anti-Virus.

В блоке **Интерактивная защита** вы можете изменить режим взаимодействия Kaspersky Anti-Virus с пользователем.

Автоматически выполнять рекомендуемые действия

Kaspersky Anti-Virus взаимодействует с пользователем в двух режимах:

- **Интерактивный режим защиты**. Kaspersky Anti-Virus уведомляет пользователя обо всех опасных и подозрительных событиях в операционной системе. В этом режиме пользователю предстоит самостоятельно принимать решение о разрешении или запрещении каких-либо действий.
- **Автоматический режим защиты**. При возникновении опасных событий Kaspersky Anti-Virus автоматически применяет действие, рекомендуемое специалистами "Лаборатории Касперского".

При установке флажка включается автоматический режим защиты, при снятии флажка – интерактивный режим защиты.

Удалять вредоносные утилиты, рекламные программы, программы автодозвона и подозрительные упаковщики

Флажок включает / выключает функцию, при включении которой Kaspersky Anti-Virus удаляет вредоносные утилиты, рекламные программы, программы автодозвона и подозрительные упаковщики в автоматическом режиме защиты.

Функция доступна, если установлен флажок **Автоматически выполнять рекомендуемые действия**.

В блоке **Автозапуск** вы можете включить / выключить автоматический запуск Kaspersky Anti-Virus при старте операционной системы.

Запускать Kaspersky Anti-Virus при включении компьютера (рекомендуется)

Флажок включает / выключает автоматический запуск Kaspersky Anti-Virus после загрузки операционной системы.

Установить защиту паролем

По ссылке открывается окно **Защита паролем**. В окне можно настроить защиту доступа к управлению Kaspersky Anti-Virus с помощью пароля.

Ссылка отображается, если пароль еще не был задан.

Изменение пароля

По ссылке открывается окно **Защита паролем**. После ввода текущего пароля можно перейти к изменению настроек защиты паролем.

Ссылка отображается, если пароль был установлен.

Управление настройками

Раскрывающийся список, в котором вы можете выбрать способ изменения настроек программы или сохранения их значений:

- **Импортировать настройки**. Извлечь настройки работы программы из файла формата CFG и применить их.
- **Экспортировать настройки**. Сохранить текущие настройки работы программы в файл формата CFG.
- **Восстановить настройки**. Запустить мастер восстановления настроек программы.

Уровень безопасности

Раскрывающийся список, в котором вы можете выбрать один из предустановленных уровней безопасности. Выбранное значение будет установлено в качестве уровня безопасности для всех компонентов защиты, в настройках которого предусмотрен выбор этого значения.

Вы можете выбрать один из следующих уровней безопасности:

- **Максимальный уровень безопасности**. Рекомендуется при работе в опасной среде.
- **Оптимальный уровень безопасности**. Рекомендуется большинству пользователей.
- **Минимальный уровень безопасности**. Обеспечивает максимальное быстродействие операционной системы.

Начало работы мастера

Далее

Кнопка, при нажатии на которую мастер восстановления настроек Kaspersky Anti-Virus начинает работу.

Обнаружено подозрительное перенаправление

Удалить записи

Kaspersky Anti-Virus удаляет все подозрительные записи из файла hosts.

Пропустить

Kaspersky Anti-Virus не удаляет из файла hosts подозрительные записи, представленные в списке.

Список подозрительных записей

Список содержит адреса вредоносных или неизвестных веб-серверов, на которые производится перенаправление при обращении программы к серверам "Лаборатории Касперского".

Рекомендуется удалять подозрительные записи из файла hosts.

Восстановление настроек

Восстановление настроек

Kaspersky Anti-Virus восстанавливает значения по умолчанию для всех компонентов программы.

Завершение работы мастера

Готово

Кнопка, при нажатии на которую завершается работа мастера восстановления настроек Kaspersky Anti-Virus.

Окно Ввод пароля

Текущий пароль

Текущий пароль, который используется для доступа к управлению Kaspersky Anti-Virus.

Запомнить пароль на эту сессию

Если флажок установлен, Kaspersky Anti-Virus запоминает введенный пароль и больше не запрашивает его во время текущего сеанса работы.

Окно Защита паролем

Ссылка **Изменить или удалить пароль** отображается, если пароль для защиты доступа к функциям Kaspersky Anti-Virus ранее был задан.

Изменить или удалить пароль

По ссылке отображаются поля ввода, в которых можно указать новый пароль и подтвердить его.

Новый пароль

Пароль для доступа к управлению Kaspersky Anti-Virus.

Подтверждение пароля

Повторный ввод пароля, введенного в поле **Новый пароль**.

В блоке **Область действия пароля** вы можете указать, какие функции управления программой нужно защитить паролем.

Настройка программы

Флажок включает / выключает запрос пароля при попытке пользователя сохранить изменения настроек программы.

Завершение работы программы

Флажок включает / выключает запрос пароля при попытке пользователя завершить работу программы.

Удаление программы

Флажок включает / выключает запрос пароля при попытке пользователя удалить программу.

Раздел Проверка

В блоке **Уровень безопасности** с помощью ползунка вы можете выбрать один из трех предустановленных наборов настроек проверки (уровней безопасности), сформированных специалистами "Лаборатории Касперского".

Высокий

Уровень безопасности, который следует использовать в случае, если вероятность заражения компьютера очень высока.

Настройки проверки при этом уровне безопасности отличаются от заданных по умолчанию тем, что Kaspersky Anti-Virus проверяет файлы всех типов. При проверке составных файлов Kaspersky Anti-Virus дополнительно проверяет файлы почтовых форматов.

Рекомендуемый

Уровень безопасности, который подходит для большинства случаев и рекомендован специалистами "Лаборатории Касперского".

Низкий

Уровень безопасности, который подходит для работы с приложениями, требующими значительных ресурсов оперативной памяти, поскольку набор проверяемых файлов на этом уровне безопасности сокращен.

Настройки проверки при этом уровне безопасности отличаются от заданных по умолчанию тем, что Kaspersky Anti-Virus проверяет только новые и измененные файлы. Если для проверки файлов требуется более 180 секунд, то Kaspersky Anti-Virus исключает эти файлы из проверки.

Восстановить рекомендуемый уровень безопасности

По ссылке Kaspersky Anti-Virus устанавливает для всех видов проверки уровень безопасности **Рекомендуемый**.

Ссылка отображается, если для полной, быстрой и выборочной проверки установлены разные уровни безопасности.

Действие при обнаружении угрозы

В раскрывающемся списке можно выбрать действие, которое программа Kaspersky Anti-Virus должна выполнить при обнаружении зараженных или возможно зараженных объектов.

Возможны следующие варианты действий:

- **Выбирать действие автоматически**. При обнаружении зараженных или возможно зараженных объектов Kaspersky Anti-Virus автоматически выполняет действие, рекомендуемое специалистами "Лаборатории Касперского". Для зараженных объектов таким действием будет **Лечить, неизлечимую – удалять**. Действия программы для возможно зараженных объектов зависят от значений основных настроек защиты.

Перед лечением или удалением зараженного объекта Kaspersky Anti-Virus создает его резервную копию на тот случай, если впоследствии понадобится восстановить объект или появится возможность его вылечить.

Этот вариант доступен и установлен по умолчанию, если выбран автоматический режим защиты. Автоматический режим защиты можно включить, установив флажок **Автоматически выполнять рекомендуемые действия** в разделе **Общие** окна настройки программы.

- **Запрашивать по окончании проверки**. Если во время проверки Kaspersky Anti-Virus обнаруживает зараженный или возможно зараженный объект, он уведомляет вас об этом после завершения проверки и запрашивает действия над обнаруженными объектами.

Этот вариант доступен и установлен по умолчанию, если выбран интерактивный режим защиты. Интерактивный режим защиты можно включить, сняв флажок **Автоматически выполнять рекомендуемые действия** в разделе **Общие** окна настройки программы.

- **Запрашивать при обнаружении**. Если во время проверки Kaspersky Anti-Virus обнаруживает зараженный или возможно зараженный объект, он сразу уведомляет вас об этом и запрашивает действие над обнаруженным объектом.

Этот вариант доступен, если выбран интерактивный режим защиты.

- **Лечить**. Kaspersky Anti-Virus пытается вылечить все обнаруженные зараженные объекты. Если лечение невозможно, то Kaspersky Anti-Virus блокирует доступ к этим объектам.
- **Лечить, неизлечимую – удалять**. Kaspersky Anti-Virus пытается вылечить все обнаруженные зараженные объекты. Если лечение невозможно, то Kaspersky Anti-Virus удаляет их.
- **Информировать**. При обнаружении зараженного или возможно зараженного объекта отображается всплывающее уведомление с информацией об обнаруженном объекте.
- **Удалять**. При обнаружении зараженных или возможно зараженных объектов Kaspersky Anti-Virus удаляет их. Перед удалением зараженного или возможно зараженного объекта Kaspersky Anti-Virus создает его резервную копию на случай, если впоследствии понадобится восстановить объект или появится возможность его вылечить.

Восстановить действие по умолчанию для всех видов проверки

По ссылке Kaspersky Anti-Virus устанавливает для всех видов проверки действие при обнаружении угрозы, рекомендуемое по умолчанию.

Ссылка отображается, если для полной, быстрой и выборочной проверки выбраны разные действия при обнаружении угрозы.

Проверка внешних устройств при подключении

В раскрывающемся списке можно выбрать действие, которое программа Kaspersky Anti-Virus должна выполнять при подключении к компьютеру внешних устройств.

Возможны следующие варианты действий:

- **Запрашивать действие**. Когда вы подключаете внешнее устройство, Kaspersky Anti-Virus показывает уведомление, в котором вы можете выбрать действие с этим устройством.
- **Не проверять**. Когда вы подключаете внешнее устройство, Kaspersky Anti-Virus не проверяет его и не запрашивает действие для подключенного устройства.
- **Проверять только корневую папку**. Когда вы подключаете внешнее устройство, Kaspersky Anti-Virus выполняет проверку файлов в корневой папке этого устройства. Этот вариант выбран по умолчанию.
- **Проверять все устройство**. Когда вы подключаете внешнее устройство, Kaspersky Anti-Virus выполняет полную проверку файлов на внешнем устройстве.
- **Проверять все устройство, если его объем менее 64 ГБ**. Когда вы подключаете внешнее устройство объемом более 64 ГБ, Kaspersky Anti-Virus не проверяет его и не запрашивает действие для подключенного устройства. Если объем внешнего устройства менее 64 ГБ, Kaspersky Anti-Virus выполняет полную проверку файлов на внешнем устройстве.

Расписание проверки

В раскрывающемся списке можно выбрать тип проверки и настроить расписание выполнения проверки выбранного типа.

Расширенная настройка

В раскрывающемся списке можно выбрать одно из следующих действий:

- **Настройка полной проверки** – открыть окно **Настройка полной проверки**. В этом окне вы можете установить уровень безопасности при выполнении полной проверки, выбрать действие при обнаружении угрозы во время полной проверки, изменить область полной проверки и задать дополнительные настройки полной проверки.
- **Настройка быстрой проверки** – открыть окно **Настройка быстрой проверки**. В этом окне вы можете установить уровень безопасности при выполнении быстрой проверки, выбрать действие при обнаружении угрозы во время быстрой проверки, изменить область быстрой проверки и задать дополнительные настройки быстрой проверки.
- **Настройка выборочной проверки** – открыть окно **Настройка выборочной проверки**. В этом окне вы можете установить уровень безопасности при выполнении выборочной проверки, выбрать действие при обнаружении угрозы во время выборочной проверки и задать дополнительные настройки выборочной проверки.
- **Область поиска уязвимостей** – открыть окно **Проверка**. В этом окне вы можете указать объекты, которые Kaspersky Anti-Virus будет проверять при выполнении поиска уязвимостей.
- **Запуск проверки с правами пользователя** – открыть окно **Настройки учетной записи**. В этом окне вы можете указать имя и пароль пользователя, от имени которого будет выполняться задача проверки.

Окно Выбор файла или папки для проверки

Объект

Поле содержит путь к файлу или папке, которые нужно добавить в список объектов, включенных в область проверки / защиты. Файл или папку можно выбрать в дереве, расположенном выше поля ввода, или указать вручную.

Окно Дополнительные настройки быстрой проверки

В блоке **Типы файлов** вы можете выбрать типы объектов, которые Kaspersky Anti-Virus должен проверять. Значения настроек, установленные по умолчанию в этом блоке, зависят от выбранного уровня безопасности.

Все файлы

Kaspersky Anti-Virus проверяет файлы любых форматов и расширений.

Файлы, проверяемые по формату

При выборе этого варианта Kaspersky Anti-Virus проверяет только те файлы, в которые может внедриться вирус. Перед началом поиска вирусов в объекте выполняется анализ его внутреннего заголовка для определения формата файла. При проверке также учитывается расширение файла.

Файлы, проверяемые по расширению

В этом случае Kaspersky Anti-Virus проверяет только файлы, в которые может внедриться вирус. При этом формат файла определяется на основании его расширения.

Файлы без расширения проверяются всегда, независимо от того, какой тип файлов выбран в блоке **Типы файлов**.

В блоке **Оптимизация проверки** можно выбрать настройки, которые позволяют сократить время проверки.

Проверять только новые и измененные файлы

Флажок включает / выключает режим проверки только новых файлов и файлов, которые изменились с момента их предыдущего анализа. Такой режим проверки распространяется как на простые, так и на составные файлы.

Пропускать объекты, если их проверка длится более

Флажок включает / выключает ограничение длительности проверки одного объекта. По истечении заданного времени проверка файла будет прекращена, а Kaspersky Anti-Virus исключит такой файл из проверки.

При установке флажка проверка по умолчанию прекращается через 30 секунд.

Блок **Проверка составных файлов** содержит список типов составных файлов, которые Kaspersky Anti-Virus анализирует на присутствие вирусов и других программ, представляющих угрозу. Значения настроек, установленные по умолчанию в этом блоке, зависят от выбранного уровня безопасности и типа проверки (полная проверка, выборочная проверка или быстрая проверка).

Проверять архивы

Флажок включает / выключает проверку архивов форматов RAR, ARJ, ZIP, CAB, LHA, JAR, ICE.

Проверять установочные пакеты

Флажок включает / выключает проверку установочных пакетов.

Проверять OLE-объекты

Флажок включает / выключает функцию, при использовании которой Kaspersky Anti-Virus проверяет вложенные в файл OLE-объекты (например, таблицы Microsoft Office Excel® или макросы, внедренные в файл Microsoft Office Word, вложения почтового сообщения).

Проверять файлы почтовых форматов

Флажок включает / выключает функцию, с помощью которой Kaspersky Anti-Virus проверяет файлы почтовых форматов, а также почтовые базы данных.

Если флажок установлен, Kaspersky Anti-Virus разбирает файл почтового формата и анализирует на наличие вирусов каждый его компонент (тело письма, вложения).

Если флажок снят, Kaspersky Anti-Virus проверяет файл почтового формата как единый объект.

Не распаковывать составные файлы размером более

Если флажок установлен, то Kaspersky Anti-Virus исключает из проверки составные файлы, размер которых больше заданного (кроме файлов больших размеров, извлеченных из архивов).

Если флажок снят, то Kaspersky Anti-Virus проверяет составные файлы любого размера.

В блоке **Методы проверки** вы можете выбрать методы, которые программа Kaspersky Anti-Virus должна использовать при проверке компьютера. Набор настроек, установленных по умолчанию в этом блоке, зависит от выбранного уровня безопасности.

Сигнатурный анализ

При сигнатурном анализе Kaspersky Anti-Virus использует базы, в которых содержатся описания известных угроз и методы их устранения. Защита с помощью сигнатурного анализа обеспечивает минимально допустимый уровень безопасности.

В соответствии с рекомендациями специалистов "Лаборатории Касперского" этот метод анализа всегда включен.

Эвристический анализ

Флажок включает / выключает использование эвристического анализа при проверке компьютера.

Ползунок

Ползунок позволяет регулировать уровень эвристического анализа. Уровень эвристического анализа обеспечивает баланс между тщательностью поиска угроз, степенью загрузки ресурсов операционной системы и временем проверки.

Существуют следующие уровни эвристического анализа:

- **Поверхностный**. Эвристический анализатор выполняет меньше действий, содержащихся в исполняемом файле. При таком режиме вероятность обнаружить угрозу снижается. Проверка требует меньше ресурсов системы и проходит быстрее.
- **Средний**. Эвристический анализатор выполняет то количество действий в исполняемом файле, которое рекомендовано специалистами "Лаборатории Касперского".
- **Глубокий**. Эвристический анализатор выполняет больше действий, содержащихся в исполняемом файле. При таком режиме вероятность обнаружить угрозу возрастает. Проверка требует больше ресурсов системы и занимает больше времени.

Ползунок доступен, если установлен флажок **Эвристический анализ**.

В блоке **Технологии проверки** вы можете выбрать технологию проверки файлов.

Технология iSwift

Технология, представляющая собой развитие технологии iChecker для компьютеров с файловой системой NTFS.

Технология iSwift имеет ограничение: она привязана к конкретному местоположению файла в файловой системе и применима только к объектам, расположенным в файловой системе NTFS.

Флажок включает / выключает использование технологии iSwift.

Технология iChecker

Технология, позволяющая увеличить скорость проверки за счет исключения из нее некоторых файлов. Файлы исключаются из проверки по специальному алгоритму, учитывающему дату выпуска баз Kaspersky Anti-Virus, дату предыдущей проверки файла, а также изменение настроек проверки.

Технология iChecker имеет ограничение: она не работает с файлами больших размеров, а кроме того, применима только к файлам с известной программе структурой (например, к файлам формата EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP, RAR).

Флажок включает / выключает использование технологии iChecker.

Окно Дополнительные настройки выборочной проверки

В блоке **Типы файлов** вы можете выбрать типы объектов, которые Kaspersky Anti-Virus должен проверять. Значения настроек, установленные по умолчанию в этом блоке, зависят от выбранного уровня безопасности.

Все файлы

Kaspersky Anti-Virus проверяет файлы любых форматов и расширений.

Файлы, проверяемые по формату

При выборе этого варианта Kaspersky Anti-Virus проверяет только те файлы, в которые может внедриться вирус. Перед началом поиска вирусов в объекте выполняется анализ его внутреннего заголовка для определения формата файла. При проверке также учитывается расширение файла.

Файлы, проверяемые по расширению

В этом случае Kaspersky Anti-Virus проверяет только файлы, в которые может внедриться вирус. При этом формат файла определяется на основании его расширения.

Файлы без расширения проверяются всегда, независимо от того, какой тип файлов выбран в блоке **Типы файлов**.

В блоке **Оптимизация проверки** можно выбрать настройки, которые позволяют сократить время проверки.

Проверять только новые и измененные файлы

Флажок включает / выключает режим проверки только новых файлов и файлов, которые изменились с момента их предыдущего анализа. Такой режим проверки распространяется как на простые, так и на составные файлы.

Пропускать объекты, если их проверка длится более

Флажок включает / выключает ограничение длительности проверки одного объекта. По истечении заданного времени проверка файла будет прекращена, а Kaspersky Anti-Virus исключит такой файл из проверки.

При установке флажка проверка по умолчанию прекращается через 30 секунд.

Блок **Проверка составных файлов** содержит список типов составных файлов, которые Kaspersky Anti-Virus анализирует на присутствие вирусов и других программ, представляющих угрозу. Значения настроек, установленные по умолчанию в этом блоке, зависят от выбранного уровня безопасности и типа проверки (полная проверка, выборочная проверка или быстрая проверка).

Проверять архивы

Флажок включает / выключает проверку архивов форматов RAR, ARJ, ZIP, CAB, LHA, JAR, ICE.

Проверять установочные пакеты

Флажок включает / выключает проверку установочных пакетов.

Проверять OLE-объекты

Флажок включает / выключает функцию, при использовании которой Kaspersky Anti-Virus проверяет вложенные в файл OLE-объекты (например, таблицы Microsoft Office Excel® или макросы, внедренные в файл Microsoft Office Word, вложения почтового сообщения).

Проверять файлы почтовых форматов

Флажок включает / выключает функцию, с помощью которой Kaspersky Anti-Virus проверяет файлы почтовых форматов, а также почтовые базы данных.

Если флажок установлен, Kaspersky Anti-Virus разбирает файл почтового формата и анализирует на наличие вирусов каждый его компонент (тело письма, вложения).

Если флажок снят, Kaspersky Anti-Virus проверяет файл почтового формата как единый объект.

Не распаковывать составные файлы размером более

Если флажок установлен, то Kaspersky Anti-Virus исключает из проверки составные файлы, размер которых больше заданного (кроме файлов больших размеров, извлеченных из архивов).

Если флажок снят, то Kaspersky Anti-Virus проверяет составные файлы любого размера.

В блоке **Методы проверки** вы можете выбрать методы, которые программа Kaspersky Anti-Virus должна использовать при проверке компьютера. Набор настроек, установленных по умолчанию в этом блоке, зависит от выбранного уровня безопасности.

Сигнатурный анализ

При сигнатурном анализе Kaspersky Anti-Virus использует базы, в которых содержатся описания известных угроз и методы их устранения. Защита с помощью сигнатурного анализа обеспечивает минимально допустимый уровень безопасности.

В соответствии с рекомендациями специалистов "Лаборатории Касперского" этот метод анализа всегда включен.

Эвристический анализ

Флажок включает / выключает использование эвристического анализа при проверке компьютера.

Ползунок

Ползунок позволяет регулировать уровень эвристического анализа. Уровень эвристического анализа обеспечивает баланс между тщательностью поиска угроз, степенью загрузки ресурсов операционной системы и временем проверки.

Существуют следующие уровни эвристического анализа:

- **Поверхностный**. Эвристический анализатор выполняет меньше действий, содержащихся в исполняемом файле. При таком режиме вероятность обнаружить угрозу снижается. Проверка требует меньше ресурсов системы и проходит быстрее.
- **Средний**. Эвристический анализатор выполняет то количество действий в исполняемом файле, которое рекомендовано специалистами "Лаборатории Касперского".
- **Глубокий**. Эвристический анализатор выполняет больше действий, содержащихся в исполняемом файле. При таком режиме вероятность обнаружить угрозу возрастает. Проверка требует больше ресурсов системы и занимает больше времени.

Ползунок доступен, если установлен флажок **Эвристический анализ**.

В блоке **Технологии проверки** вы можете выбрать технологию проверки файлов.

Технология iSwift

Технология, представляющая собой развитие технологии iChecker для компьютеров с файловой системой NTFS.

Технология iSwift имеет ограничение: она привязана к конкретному местоположению файла в файловой системе и применима только к объектам, расположенным в файловой системе NTFS.

Флажок включает / выключает использование технологии iSwift.

Технология iChecker

Технология, позволяющая увеличить скорость проверки за счет исключения из нее некоторых файлов. Файлы исключаются из проверки по специальному алгоритму, учитывающему дату выпуска баз Kaspersky Anti-Virus, дату предыдущей проверки файла, а также изменение настроек проверки.

Технология iChecker имеет ограничение: она не работает с файлами больших размеров, а кроме того, применима только к файлам с известной программе структурой (например, к файлам формата EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP, RAR).

Флажок включает / выключает использование технологии iChecker.

Окно Дополнительные настройки полной проверки

В блоке **Типы файлов** вы можете выбрать типы объектов, которые Kaspersky Anti-Virus должен проверять. Значения настроек, установленные по умолчанию в этом блоке, зависят от выбранного уровня безопасности.

Все файлы

Kaspersky Anti-Virus проверяет файлы любых форматов и расширений.

Файлы, проверяемые по формату

При выборе этого варианта Kaspersky Anti-Virus проверяет только те файлы, в которые может внедриться вирус. Перед началом поиска вирусов в объекте выполняется анализ его внутреннего заголовка для определения формата файла. При проверке также учитывается расширение файла.

Файлы, проверяемые по расширению

В этом случае Kaspersky Anti-Virus проверяет только файлы, в которые может внедриться вирус. При этом формат файла определяется на основании его расширения.

Файлы без расширения проверяются всегда, независимо от того, какой тип файлов выбран в блоке **Типы файлов**.

В блоке **Оптимизация проверки** можно выбрать настройки, которые позволяют сократить время проверки.

Проверять только новые и измененные файлы

Флажок включает / выключает режим проверки только новых файлов и файлов, которые изменились с момента их предыдущего анализа. Такой режим проверки распространяется как на простые, так и на составные файлы.

Пропускать объекты, если их проверка длится более

Флажок включает / выключает ограничение длительности проверки одного объекта. По истечении заданного времени проверка файла будет прекращена, а Kaspersky Anti-Virus исключит такой файл из проверки.

При установке флажка проверка по умолчанию прекращается через 30 секунд.

Блок **Проверка составных файлов** содержит список типов составных файлов, которые Kaspersky Anti-Virus анализирует на присутствие вирусов и других программ, представляющих угрозу. Значения настроек, установленные по умолчанию в этом блоке, зависят от выбранного уровня безопасности и типа проверки (полная проверка, выборочная проверка или быстрая проверка).

Проверять архивы

Флажок включает / выключает проверку архивов форматов RAR, ARJ, ZIP, CAB, LHA, JAR, ICE.

Проверять установочные пакеты

Флажок включает / выключает проверку установочных пакетов.

Проверять OLE-объекты

Флажок включает / выключает функцию, при использовании которой Kaspersky Anti-Virus проверяет вложенные в файл OLE-объекты (например, таблицы Microsoft Office Excel® или макросы, внедренные в файл Microsoft Office Word, вложения почтового сообщения).

Проверять файлы почтовых форматов

Флажок включает / выключает функцию, с помощью которой Kaspersky Anti-Virus проверяет файлы почтовых форматов, а также почтовые базы данных.

Если флажок установлен, Kaspersky Anti-Virus разбирает файл почтового формата и анализирует на наличие вирусов каждый его компонент (тело письма, вложения).

Если флажок снят, Kaspersky Anti-Virus проверяет файл почтового формата как единый объект.

Не распаковывать составные файлы размером более

Если флажок установлен, то Kaspersky Anti-Virus исключает из проверки составные файлы, размер которых больше заданного (кроме файлов больших размеров, извлеченных из архивов).

Если флажок снят, то Kaspersky Anti-Virus проверяет составные файлы любого размера.

В блоке **Методы проверки** вы можете выбрать методы, которые программа Kaspersky Anti-Virus должна использовать при проверке компьютера. Набор настроек, установленных по умолчанию в этом блоке, зависит от выбранного уровня безопасности.

Сигнатурный анализ

При сигнатурном анализе Kaspersky Anti-Virus использует базы, в которых содержатся описания известных угроз и методы их устранения. Защита с помощью сигнатурного анализа обеспечивает минимально допустимый уровень безопасности.

В соответствии с рекомендациями специалистов "Лаборатории Касперского" этот метод анализа всегда включен.

Эвристический анализ

Флажок включает / выключает использование эвристического анализа при проверке компьютера.

Ползунок

Ползунок позволяет регулировать уровень эвристического анализа. Уровень эвристического анализа обеспечивает баланс между тщательностью поиска угроз, степенью загрузки ресурсов операционной системы и временем проверки.

Существуют следующие уровни эвристического анализа:

- **Поверхностный**. Эвристический анализатор выполняет меньше действий, содержащихся в исполняемом файле. При таком режиме вероятность обнаружить угрозу снижается. Проверка требует меньше ресурсов системы и проходит быстрее.
- **Средний**. Эвристический анализатор выполняет то количество действий в исполняемом файле, которое рекомендовано специалистами "Лаборатории Касперского".
- **Глубокий**. Эвристический анализатор выполняет больше действий, содержащихся в исполняемом файле. При таком режиме вероятность обнаружить угрозу возрастает. Проверка требует больше ресурсов системы и занимает больше времени.

Ползунок доступен, если установлен флажок **Эвристический анализ**.

В блоке **Технологии проверки** вы можете выбрать технологию проверки файлов.

Технология iSwift

Технология, представляющая собой развитие технологии iChecker для компьютеров с файловой системой NTFS.

Технология iSwift имеет ограничение: она привязана к конкретному местоположению файла в файловой системе и применима только к объектам, расположенным в файловой системе NTFS.

Флажок включает / выключает использование технологии iSwift.

Технология iChecker

Технология, позволяющая увеличить скорость проверки за счет исключения из нее некоторых файлов. Файлы исключаются из проверки по специальному алгоритму, учитывающему дату выпуска баз Kaspersky Anti-Virus, дату предыдущей проверки файла, а также изменение настроек проверки.

Технология iChecker имеет ограничение: она не работает с файлами больших размеров, а кроме того, применима только к файлам с известной программе структурой (например, к файлам формата EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP, RAR).

Флажок включает / выключает использование технологии iChecker.

Окно Настройка быстрой проверки

В блоке **Уровень безопасности** с помощью ползунка вы можете выбрать один из трех предустановленных наборов настроек быстрой проверки (уровней безопасности), сформированных специалистами "Лаборатории Касперского". Этот уровень безопасности будет применяться при быстрой проверке независимо от того, какой уровень безопасности выбран для проверки в целом (в разделе **Проверка** окна **Настройка**).

Высокий

Уровень безопасности, который следует использовать в случае, если вероятность заражения компьютера высока.

Настройки быстрой проверки при этом уровне безопасности отличаются от заданных по умолчанию тем, что Kaspersky Anti-Virus проверяет файлы всех типов. При проверке составных файлов Kaspersky Anti-Virus дополнительно проверяет файлы почтовых форматов.

Рекомендуемый

Уровень безопасности, который подходит для большинства случаев быстрой проверки и рекомендован специалистами "Лаборатории Касперского".

Низкий

Уровень безопасности, который подходит для работы с программами, требующими значительных ресурсов оперативной памяти, поскольку набор проверяемых файлов на этом уровне безопасности сокращен.

Настройки быстрой проверки при этом уровне безопасности отличаются от заданных по умолчанию тем, что Kaspersky Anti-Virus проверяет только новые и измененные файлы. Если для проверки файла требуется более 180 секунд, то Kaspersky Anti-Virus исключает этот файл из проверки.

Восстановить рекомендуемый уровень безопасности

По ссылке Kaspersky Anti-Virus устанавливает для быстрой проверки уровень безопасности **Рекомендуемый**.

Ссылка отображается, если вы изменили настройки в окне **Дополнительные настройки быстрой проверки**.

Действие при обнаружении угрозы

В раскрывающемся списке можно выбрать действие, которое программа Kaspersky Anti-Virus должна выполнить при обнаружении зараженных или возможно зараженных объектов.

Возможны следующие варианты действий:

- **Выбирать действие автоматически**. При обнаружении зараженных или возможно зараженных объектов Kaspersky Anti-Virus автоматически выполняет действие, рекомендуемое специалистами "Лаборатории Касперского". Для зараженных объектов таким действием будет **Лечить, неизлечимую – удалять**. Действия программы для возможно зараженных объектов зависят от значений основных настроек защиты.

Перед лечением или удалением зараженного объекта Kaspersky Anti-Virus создает его резервную копию на тот случай, если впоследствии понадобится восстановить объект или появится возможность его вылечить.

Этот вариант доступен и установлен по умолчанию, если выбран автоматический режим защиты. Автоматический режим защиты можно включить, установив флажок **Автоматически выполнять рекомендуемые действия** в разделе **Общие** окна настройки программы.

- **Запрашивать по окончании проверки**. Если во время проверки Kaspersky Anti-Virus обнаруживает зараженный или возможно зараженный объект, он уведомляет вас об этом после завершения проверки и запрашивает действия над обнаруженными объектами.

Этот вариант доступен и установлен по умолчанию, если выбран интерактивный режим защиты. Интерактивный режим защиты можно включить, сняв флажок **Автоматически выполнять рекомендуемые действия** в разделе **Общие** окна настройки программы.

- **Запрашивать при обнаружении**. Если во время проверки Kaspersky Anti-Virus обнаруживает зараженный или возможно зараженный объект, он сразу уведомляет вас об этом и запрашивает действие над обнаруженным объектом.

Этот вариант доступен, если выбран интерактивный режим защиты.

- **Лечить**. Kaspersky Anti-Virus пытается вылечить все обнаруженные зараженные объекты. Если лечение невозможно, то Kaspersky Anti-Virus блокирует доступ к этим объектам.
- **Лечить, неизлечимую – удалять**. Kaspersky Anti-Virus пытается вылечить все обнаруженные зараженные объекты. Если лечение невозможно, то Kaspersky Anti-Virus удаляет их.
- **Информировать**. При обнаружении зараженного или возможно зараженного объекта отображается всплывающее уведомление с информацией об обнаруженном объекте.
- **Удалять**. При обнаружении зараженных или возможно зараженных объектов Kaspersky Anti-Virus удаляет их. Перед удалением зараженного или возможно зараженного объекта Kaspersky Anti-Virus создает его резервную копию на случай, если впоследствии понадобится восстановить объект или появится возможность его вылечить.

Изменить область быстрой проверки

По ссылке открывается окно **Область быстрой проверки**. В этом окне вы можете указать, какие объекты необходимо проверять при выполнении быстрой проверки.

Дополнительные настройки

По ссылке открывается окно **Дополнительные настройки быстрой проверки**. В этом окне вы можете задать настройки быстрой проверки различных типов файлов, настройки оптимизации быстрой проверки, выбрать методы и технологии для быстрой проверки.

Окно Настройка выборочной проверки

В блоке **Уровень безопасности** с помощью ползунка вы можете выбрать один из трех предустановленных наборов настроек выборочной проверки (уровней безопасности), сформированных специалистами "Лаборатории Касперского". Этот уровень безопасности будет применяться при выборочной проверке независимо от того, какой уровень безопасности выбран для проверки в целом (в разделе **Проверка** окна **Настройка**).

Высокий

Уровень безопасности, который следует использовать в случае, если вероятность заражения компьютера высока.

Настройки выборочной проверки при этом уровне безопасности отличаются от заданных по умолчанию тем, что Kaspersky Anti-Virus проверяет файлы всех типов. При выборочной проверке составных файлов Kaspersky Anti-Virus дополнительно проверяет файлы почтовых форматов.

Рекомендуемый

Уровень безопасности, который подходит для большинства случаев выборочной проверки и рекомендован специалистами "Лаборатории Касперского".

Низкий

Уровень безопасности, который подходит для работы с программами, требующими значительных ресурсов оперативной памяти, поскольку набор проверяемых файлов на этом уровне безопасности сокращен.

Настройки выборочной проверки при этом уровне безопасности отличаются от заданных по умолчанию тем, что Kaspersky Anti-Virus проверяет только новые и измененные файлы. Если для выборочной проверки файла требуется более 180 секунд, то Kaspersky Anti-Virus исключает этот файл из выборочной проверки.

Восстановить рекомендуемый уровень безопасности

По ссылке Kaspersky Anti-Virus устанавливает для выборочной проверки уровень безопасности **Рекомендуемый**.

Ссылка отображается, если вы изменили настройки в окне **Дополнительные настройки выборочной проверки**.

Действие при обнаружении угрозы

В раскрывающемся списке можно выбрать действие, которое программа Kaspersky Anti-Virus должна выполнить при обнаружении зараженных или возможно зараженных объектов.

Возможны следующие варианты действий:

- **Выбирать действие автоматически**. При обнаружении зараженных или возможно зараженных объектов Kaspersky Anti-Virus автоматически выполняет действие, рекомендуемое специалистами "Лаборатории Касперского". Для зараженных объектов таким действием будет **Лечить, неизлечимую – удалять**. Действия программы для возможно зараженных объектов зависят от значений основных настроек защиты.

Перед лечением или удалением зараженного объекта Kaspersky Anti-Virus создает его резервную копию на тот случай, если впоследствии понадобится восстановить объект или появится возможность его вылечить.

Этот вариант доступен и установлен по умолчанию, если выбран автоматический режим защиты. Автоматический режим защиты можно включить, установив флажок **Автоматически выполнять рекомендуемые действия** в разделе **Общие** окна настройки программы.

- **Запрашивать по окончании проверки**. Если во время проверки Kaspersky Anti-Virus обнаруживает зараженный или возможно зараженный объект, он уведомляет вас об этом после завершения проверки и запрашивает действия над обнаруженными объектами.

Этот вариант доступен и установлен по умолчанию, если выбран интерактивный режим защиты. Интерактивный режим защиты можно включить, сняв флажок **Автоматически выполнять рекомендуемые действия** в разделе **Общие** окна настройки программы.

- **Запрашивать при обнаружении**. Если во время проверки Kaspersky Anti-Virus обнаруживает зараженный или возможно зараженный объект, он сразу уведомляет вас об этом и запрашивает действие над обнаруженным объектом.

Этот вариант доступен, если выбран интерактивный режим защиты.

- **Лечить**. Kaspersky Anti-Virus пытается вылечить все обнаруженные зараженные объекты. Если лечение невозможно, то Kaspersky Anti-Virus блокирует доступ к этим объектам.
- **Лечить, неизлечимую – удалять**. Kaspersky Anti-Virus пытается вылечить все обнаруженные зараженные объекты. Если лечение невозможно, то Kaspersky Anti-Virus удаляет их.
- **Информировать**. При обнаружении зараженного или возможно зараженного объекта отображается всплывающее уведомление с информацией об обнаруженном объекте.
- **Удалять**. При обнаружении зараженных или возможно зараженных объектов Kaspersky Anti-Virus удаляет их. Перед удалением зараженного или возможно зараженного объекта Kaspersky Anti-Virus создает его резервную копию на случай, если впоследствии понадобится восстановить объект или появится возможность его вылечить.

Дополнительные настройки

По ссылке открывается окно **Дополнительные настройки выборочной проверки**. В этом окне вы можете задать настройки выборочной проверки различных типов файлов, настройки оптимизации выборочной проверки, выбрать методы и технологии для выборочной проверки.

Окно Настройка полной проверки

В блоке **Уровень безопасности** с помощью ползунка вы можете выбрать один из трех предустановленных наборов настроек полной проверки (уровней безопасности), сформированных специалистами "Лаборатории Касперского". Этот уровень безопасности будет применяться при полной проверке независимо от того, какой уровень безопасности выбран для проверки в целом (в разделе **Проверка** окна **Настройка**).

Высокий

Уровень безопасности, который следует использовать в случае, если вероятность заражения компьютера высока.

Настройки полной проверки при этом уровне безопасности отличаются от заданных по умолчанию тем, что Kaspersky Anti-Virus проверяет файлы всех типов. При проверке составных файлов Kaspersky Anti-Virus дополнительно проверяет файлы почтовых форматов.

Рекомендуемый

Уровень безопасности, который подходит для большинства случаев полной проверки и рекомендован специалистами "Лаборатории Касперского".

Низкий

Уровень безопасности, который подходит для работы с программами, требующими значительных ресурсов оперативной памяти, поскольку набор проверяемых файлов на этом уровне безопасности сокращен.

Настройки полной проверки при этом уровне безопасности отличаются от заданных по умолчанию тем, что Kaspersky Anti-Virus проверяет только новые и измененные файлы. Если для проверки файла требуется более 180 секунд, то Kaspersky Anti-Virus исключает этот файл из проверки.

Восстановить рекомендуемый уровень безопасности

По ссылке Kaspersky Anti-Virus устанавливает для полной проверки уровень безопасности **Рекомендуемый**.

Ссылка отображается, если вы изменили настройки в окне **Дополнительные настройки полной проверки**.

Действие при обнаружении угрозы

В раскрывающемся списке можно выбрать действие, которое программа Kaspersky Anti-Virus должна выполнить при обнаружении зараженных или возможно зараженных объектов.

Возможны следующие варианты действий:

- **Выбирать действие автоматически**. При обнаружении зараженных или возможно зараженных объектов Kaspersky Anti-Virus автоматически выполняет действие, рекомендуемое специалистами "Лаборатории Касперского". Для зараженных объектов таким действием будет **Лечить, неизлечимую – удалять**. Действия программы для возможно зараженных объектов зависят от значений основных настроек защиты.

Перед лечением или удалением зараженного объекта Kaspersky Anti-Virus создает его резервную копию на тот случай, если впоследствии понадобится восстановить объект или появится возможность его вылечить.

Этот вариант доступен и установлен по умолчанию, если выбран автоматический режим защиты. Автоматический режим защиты можно включить, установив флажок **Автоматически выполнять рекомендуемые действия** в разделе **Общие** окна настройки программы.

- **Запрашивать по окончании проверки**. Если во время проверки Kaspersky Anti-Virus обнаруживает зараженный или возможно зараженный объект, он уведомляет вас об этом после завершения проверки и запрашивает действия над обнаруженными объектами.

Этот вариант доступен и установлен по умолчанию, если выбран интерактивный режим защиты. Интерактивный режим защиты можно включить, сняв флажок **Автоматически выполнять рекомендуемые действия** в разделе **Общие** окна настройки программы.

- **Запрашивать при обнаружении**. Если во время проверки Kaspersky Anti-Virus обнаруживает зараженный или возможно зараженный объект, он сразу уведомляет вас об этом и запрашивает действие над обнаруженным объектом.

Этот вариант доступен, если выбран интерактивный режим защиты.

- **Лечить**. Kaspersky Anti-Virus пытается вылечить все обнаруженные зараженные объекты. Если лечение невозможно, то Kaspersky Anti-Virus блокирует доступ к этим объектам.
- **Лечить, неизлечимую – удалять**. Kaspersky Anti-Virus пытается вылечить все обнаруженные зараженные объекты. Если лечение невозможно, то Kaspersky Anti-Virus удаляет их.
- **Информировать**. При обнаружении зараженного или возможно зараженного объекта отображается всплывающее уведомление с информацией об обнаруженном объекте.
- **Удалять**. При обнаружении зараженных или возможно зараженных объектов Kaspersky Anti-Virus удаляет их. Перед удалением зараженного или возможно зараженного объекта Kaspersky Anti-Virus создает его резервную копию на случай, если впоследствии понадобится восстановить объект или появится возможность его вылечить.

Изменить область полной проверки

По ссылке открывается окно **Область полной проверки**. В этом окне вы можете указать, какие объекты необходимо проверять при выполнении полной проверки.

Дополнительные настройки

По ссылке открывается окно **Дополнительные настройки полной проверки**. В этом окне вы можете задать настройки полной проверки различных типов файлов, настройки оптимизации полной проверки, выбрать методы и технологии для полной проверки.

Окно Проверка

Список объектов

Содержит список дисков, папок и других объектов, которые Kaspersky Anti-Virus проверяет при выполнении выбранной задачи: полной проверки, быстрой проверки или поиска уязвимостей.

Если флажок в строке объекта установлен, то Kaspersky Anti-Virus проверяет объект при выполнении задачи.

Если флажок в строке объекта снят, то Kaspersky Anti-Virus исключает этот объект из проверки.

Добавить

При нажатии на кнопку открывается окно для выбора файла или папки, которую нужно добавить в список объектов для проверки. Выбранный объект для проверки добавляется в конец списка.

Кнопка

При нажатии на кнопку выбранный объект удаляется из списка.

Кнопка отображается справа от объектов, которые были добавлены вручную. Удалить объекты проверки, присутствующие в списке по умолчанию, невозможно.

Настройки учетной записи

Запуск от имени

Выбор учетной записи, с правами которой Kaspersky Anti-Virus будет запускать задачи проверки. Функция доступна для запуска проверки Kaspersky Anti-Virus как вручную, так и по расписанию.

Возможны следующие варианты выбора:

- **Текущего пользователя**. Задачи проверки будут запускаться с правами текущей учетной записи.
- **Другого пользователя**. Задачи проверки будут запускаться от имени указанного пользователя. При выборе этого варианта нужно указать имя и пароль учетной записи в полях **Учетная запись** и **Пароль**.

Расписание проверки и поиска уязвимостей

Запускать проверку

В раскрывающемся списке можно выбрать режим запуска проверки. Проверку можно запускать вручную или по расписанию с указанной периодичностью.

Возможны следующие варианты запуска:

Вручную. Режим запуска, при котором запуск задачи по расписанию отключен. Вы запускаете проверку вручную в удобное для вас время.

- **Каждый день**. Запуск задачи осуществляется каждый день в определенное время.

Для этого значения доступно поле ввода **Время**. В поле ввода можно указать время запуска задачи.

- **Каждый рабочий день**. Запуск задачи осуществляется по рабочим дням в определенное время.

Для этого значения доступно поле ввода **Время**. В поле ввода можно указать время запуска задачи.

- **Каждый выходной**. Запуск задачи осуществляется по выходным дням в определенное время.

Для этого значения доступно поле ввода **Время**. В поле ввода можно указать время запуска задачи.

- **Еженедельно**. Запуск задачи осуществляется в определенные дни недели.

Для этого значения доступны следующие настройки:

- **День недели**. В раскрывающемся списке можно выбрать день недели, в который будет запускаться задача проверки.
- **Время**. В поле ввода можно указать время запуска задачи проверки.
- **Ежемесячно**. Запуск задачи осуществляется в определенные дни месяца.

Для этого значения доступны следующие настройки:

- **День месяца**. В раскрывающемся списке можно выбрать первый или последний день месяца, в который будет запускаться задача проверки.
- **Время**. В поле ввода можно указать время запуска задачи проверки.

Запускать проверку по расписанию на следующий день, если компьютер был выключен

Если флажок установлен, программа запускает пропущенные задачи. Например, если компьютер был выключен, программа запускает пропущенные задачи после его включения.

Если флажок снят, Kaspersky Anti-Virus не запускает пропущенные задачи, а выполняет следующую задачу по установленному расписанию.

Флажок отображается, если в списке выбрано значение **ежедневно** или **еженедельно**.

Выполнять проверку по расписанию только в случае, когда компьютер заблокирован или включена экранная заставка

Флажок включает / выключает функцию Kaspersky Anti-Virus, которая приостанавливает запуск задачи до того момента, пока вы не закончите работу на компьютере. Таким образом, задача проверки не будет занимать ресурсы компьютера во время работы.

Если флажок установлен, Kaspersky Anti-Virus запустит проверку по расписанию после того, как будет включена экранная заставка или компьютер будет заблокирован.

Флажок не отображается, если в списке **Запускать проверку** выбрано значение **вручную**.

Раздел Производительность

Не запускать задачи по расписанию при работе от аккумулятора

Проверка на вирусы и другие программы, представляющие угрозу, и обновление баз и программных модулей иногда требуют значительного количества ресурсов компьютера и времени.

Флажок включает / выключает режим экономии питания аккумулятора портативного компьютера, при котором выполнение задач проверки и задач обновления откладывается. По мере необходимости вы можете самостоятельно обновлять базы и программные модули Kaspersky Anti-Virus или запускать проверку на вирусы и другие программы, представляющие угрозу.

Использовать Игровой режим

Если флажок установлен, Kaspersky Anti-Virus не запускает задачи проверки и обновления, не отображает уведомления, когда вы играете или работаете с программами в полноэкранном режиме.

Уступать ресурсы операционной системе при запуске компьютера

Флажок контролирует использование ресурсов операционной системы программой Kaspersky Anti-Virus.

Если флажок установлен, при запуске операционной системы включаются только критически важные компоненты защиты Kaspersky Anti-Virus. После загрузки операционной системы защита включается полностью.

Если флажок снят, все компоненты защиты включаются одновременно при запуске операционной системы.

Предотвращать заражение во время перезагрузки операционной системы

Если флажок установлен, при завершении работы операционной системы Kaspersky Anti-Virus работает в режиме, в котором уделяется особое внимание проверке файлов, появившихся на диске во время перезагрузки операционной системы. Если какие-то из этих файлов являются вредоносными, после перезагрузки операционной системы программа обезвредит их.

Предотвращение заражения при перезагрузке не работает, если в настройках Файлового Антивируса выбрано действие **Блокировать** при обнаружении угрозы.

Откладывать выполнение задач проверки компьютера при высокой нагрузке на центральный процессор и дисковые системы

Когда Kaspersky Anti-Virus выполняет задачи проверки, может увеличиваться нагрузка на центральный процессор и дисковые подсистемы, что замедляет работу других программ. При возникновении такой ситуации Kaspersky Anti-Virus может приостанавливать выполнение задач проверки и высвобождать ресурсы операционной системы для программ пользователя.

Флажок включает / выключает механизм, который приостанавливает выполнение задач проверки. Это позволяет ограничить нагрузку на центральный процессор и дисковые подсистемы.

Выполнять задачи во время простоя компьютера

Флажок включает / выключает запуск задач проверки (системной памяти, системного раздела, объектов автозапуска) и задачу обновления в то время, когда компьютер заблокирован или включена экранная заставка.

Если компьютер работает от аккумулятора, Kaspersky Anti-Virus не выполняет задачи во время простоя компьютера.

Если флажок снят, Kaspersky Anti-Virus не выполняет задачи проверки и задачу обновления во время простоя компьютера.

Выполнять поиск программ, предназначенных для скрытия следов вредоносной программы в системе (руткитов)

Флажок включает / выключает периодический поиск руткитов в операционной системе в фоновом режиме.

Если флажок снят, Kaspersky Anti-Virus не выполняет периодический поиск руткитов.

Приостановить работу Файлового Антивируса

По ссылке открывается окно **Приостановка Файлового Антивируса**. В окне можно указать период времени, в который работа Файлового Антивируса будет приостанавливается, а также сформировать список программ, при работе которых Файловый Антивирус будет приостановлен.

Настройки IM-Антивируса

Включить / выключить IM-Антивирус

Переключатель включает / выключает IM-Антивирус.

Если переключатель включен, IM-Антивирус запускается при старте операционной системы, находится в оперативной памяти компьютера и проверяет входящие и исходящие сообщения, переданные с помощью IM-клиентов (ICQ, Jabber, Mail.Ru Агент). IM-Антивирус не проверяет сообщения, передаваемые через Yahoo! Messenger™, и сообщения, передаваемые через Mail.Ru Агент в офлайн-режиме.

Вы можете найти информацию об ограничениях работы компонента IM-Антивирус в разделе Ограничения и предупреждения.

Настройки Анти-Баннера

Включить / выключить Анти-Баннер

Переключатель включает / выключает использование Анти-Баннера.

Если переключатель включен, Анти-Баннер блокирует отображение баннеров на просматриваемых вами сайтах и в интерфейсе некоторых компьютерных программ. По умолчанию Анти-Баннер блокирует на сайтах баннеры из списка известных баннеров. Список входит в состав баз Kaspersky Anti-Virus.

Список фильтров

По ссылке открывается окно **Список фильтров**, в котором вы можете с помощью специальных фильтров детально указать, какие именно баннеры нужно блокировать.

Сайты с разрешенными баннерами

По ссылке открывается окно со списком сайтов, на которых вы разрешили отображение баннеров.

Запрещенные баннеры

По ссылке открывается окно **Запрещенные баннеры**. В этом окне вы можете сформировать список баннеров, запрещенных для отображения.

Разрешенные баннеры

По ссылке открывается окно **Разрешенные баннеры**. В этом окне вы можете сформировать список баннеров, разрешенных для отображения.

Разрешить баннеры на сайтах "Лаборатории Касперского"

Если флажок установлен, Анти-Баннер не блокирует баннеры на сайтах "Лаборатории Касперского" и сайтах партнеров компании, на которых размещена реклама "Лаборатории Касперского". Список этих сайтов доступен по ссылке **Сайты "Лаборатории Касперского"**.

Сайты "Лаборатории Касперского"

По ссылке открывается окно со списком сайтов "Лаборатории Касперского".

Ссылка доступна, если установлен флажок **Разрешить баннеры на сайтах "Лаборатории Касперского"**.

Окно Добавление / изменение баннера

Маска веб-адреса (URL)

IP-адрес, веб-адрес (URL) или маска веб-адреса.

При вводе маски веб-адреса можно использовать символы `*` и `?`, где `*` – любая последовательность символов, а `?` – любой один символ.

Статус

В блоке **Статус** вы можете указать, должен ли Анти-Баннер использовать этот адрес при проверке баннеров.

Возможны следующие варианты:

- **Активно**. Анти-Баннер использует этот адрес при проверке баннеров.
- **Неактивно**. Анти-Баннер не использует этот адрес при проверке баннеров.

Окно Добавление / изменение сайта

Сайт

Веб-адрес (URL) сайта.

Статус

В блоке **Статус** вы можете указать, должен ли Анти-Баннер разрешать отображение баннеров на указанном сайте.

Возможны следующие варианты:

- **Активно**. Анти-Баннер разрешает отображение баннеров на указанном сайте.
- **Неактивно**. Анти-Баннер не разрешает отображение баннеров на указанном сайте.

Окно Запрещенные баннеры

Кнопка

При нажатии на кнопку открывается меню со следующими пунктами:

- **Импортировать и добавить к существующему**. При выборе этого пункта открывается окно, позволяющее загрузить список запрещенных адресов из файла формата CSV. Текущие адреса не будут удалены.
- **Импортировать и заменить существующий**. При выборе этого пункта открывается окно, позволяющее загрузить список запрещенных адресов из файла формата CSV. Текущие адреса будут удалены.
- **Экспортировать**. При выборе этого пункта открывается окно, позволяющее сохранить список запрещенных адресов в файле формата CSV.

Список запрещенных баннеров

Содержит адреса или маски адресов запрещенных баннеров. Анти-Баннер блокирует баннер, если его адрес есть в списке запрещенных баннеров.

Вы можете добавить в список адрес или маску адреса.

Если в графе **Статус** в строке адреса установлено значение *Активно*, Анти-Баннер использует этот адрес при проверке баннеров.

Если в графе **Статус** в строке адреса установлено значение *Неактивно*, Анти-Баннер не использует этот адрес при проверке баннеров.

Маска веб-адреса (URL)

Графа, в которой указан адрес или маска адреса запрещенного баннера.

Статус

Графа, в которой указано, использует ли Анти-Баннер этот адрес при проверке баннеров.

Если в строке адреса установлено значение *Активно*, Анти-Баннер использует этот адрес при проверке баннеров.

Если в строке адреса установлено значение *Неактивно*, Анти-Баннер не использует этот адрес при проверке баннеров.

Изменить

Кнопка, при нажатии на которую открывается окно для изменения адреса или маски адреса баннера в списке запрещенных баннеров.

Удалить

Кнопка, при нажатии на которую Анти-Баннер удаляет выбранный адрес баннера или маску адреса из списка.

Добавить

Кнопка, при нажатии на которую открывается окно для добавления адреса или маски адреса баннера в список запрещенных баннеров.

Окно Разрешенные баннеры

Кнопка

При нажатии на кнопку открывается меню со следующими пунктами:

- **Импортировать и добавить к существующему**. При выборе этого пункта можно загрузить список разрешенных адресов из файла формата CSV. Текущие адреса не удаляются.
- **Импортировать и заменить существующий**. При выборе этого пункта можно загрузить список разрешенных адресов из файла формата CSV. Текущие адреса удаляются.
- **Экспортировать**. При выборе этого пункта можно сохранить список адресов в файле формата CSV. Вы можете экспортировать как весь список адресов, так и адреса, выбранные из списка.

Список разрешенных баннеров

Содержит адреса или маски адресов разрешенных баннеров. Анти-Баннер не блокирует баннер, если его адрес есть в списке разрешенных баннеров.

Вы можете добавить в список адрес или маску адреса.

Если в графе **Статус** в строке адреса установлено значение *Активно*, Анти-Баннер использует этот адрес при проверке баннеров.

Если в графе **Статус** в строке адреса установлено значение *Неактивно*, Анти-Баннер не использует этот адрес при проверке баннеров.

Маска веб-адреса (URL)

Графа, в которой указана адрес или маска адреса разрешенного баннера.

Статус

Графа, в которой указано, использует ли Анти-Баннер этот адрес при проверке баннеров.

Если в строке адреса установлено значение *Активно*, Анти-Баннер использует этот адрес при проверке баннеров.

Если в строке адреса установлено значение *Неактивно*, Анти-Баннер не использует этот адрес при проверке баннеров.

Изменить

Кнопка, при нажатии на которую открывается окно для изменения адреса или маски адреса баннера в списке разрешенных баннеров.

Удалить

Кнопка, при нажатии на которую Анти-Баннер удаляет выбранный адрес или маску адреса баннера из списка разрешенных баннеров.

Добавить

Кнопка, при нажатии на которую открывается окно для добавления адреса или маски адреса баннера в список разрешенных баннеров.

Окно Сайты с разрешенными баннерами

Кнопка

При нажатии на кнопку открывается меню со следующими пунктами:

- **Импортировать и добавить к существующему**. При выборе этого пункта можно загрузить список разрешенных адресов из файла формата CSV. Текущие адреса не удаляются.
- **Импортировать и заменить существующий**. При выборе этого пункта можно загрузить список разрешенных адресов из файла формата CSV. Текущие адреса удаляются.
- **Экспортировать**. При выборе этого пункта можно сохранить список адресов в файле формата CSV. Вы можете экспортировать как весь список адресов, так и адреса, выбранные из списка.

Список сайтов с разрешенными баннерами

Содержит адреса сайтов, на которых вы разрешили отображение баннеров. Анти-Баннер не блокирует баннеры на сайте, если его адрес есть в списке.

Вы можете добавить в список адрес или маску адреса.

Если в графе **Статус** в строке адреса установлено значение *Активно*, Анти-Баннер разрешает отображение баннеров на этом сайте.

Если в графе **Статус** в строке адреса установлено значение *Неактивно*, Анти-Баннер блокирует баннеры на этом сайте.

Изменить

Кнопка, при нажатии на которую открывается окно для изменения адреса или маски адреса сайта, выбранного в списке.

Удалить

Кнопка, при нажатии на которую Анти-Баннер удаляет выбранный адрес или маску адреса сайта из списка.

Добавить

Кнопка, при нажатии на которую открывается окно для добавления адреса или маски адреса сайта в список.

Окно Сайты "Лаборатории Касперского"

В окне представлен список сайтов "Лаборатории Касперского" и сайты партнеров компании, на которых размещена реклама "Лаборатории Касперского".

Список составляют и обновляют специалисты "Лаборатории Касперского". В программе список обновляется автоматически при обновлении баз и программных модулей.

Настройки Анти-Спама

Включить / выключить Анти-Спам

Переключатель включает / выключает Анти-Спам.

Если переключатель включен, Анти-Спам обнаруживает нежелательную почту (спам) и обрабатывает ее в соответствии с правилами вашего почтового клиента.

Уровень безопасности

В блоке **Уровень безопасности** вы можете выбрать один из предустановленных наборов настроек Анти-Спама (уровней безопасности). Решение о том, какой уровень безопасности выбрать, вы принимаете в зависимости от условий работы и сложившейся ситуации.

Доступны следующие уровни безопасности:

- **Высокий**. Уровень безопасности, при котором Анти-Спам использует максимальный уровень фильтрации спама.

Высокий уровень безопасности рекомендуется устанавливать при работе в опасной среде (например, при использовании бесплатного почтового сервиса).

При установке высокого уровня безопасности может возрасти частота распознавания полезной почты как спама.

- **Рекомендуемый**. Уровень безопасности, при котором обеспечивается оптимальный баланс между производительностью и безопасностью. Он подходит для большинства случаев.

- **Низкий**. Уровень безопасности, при котором Анти-Спам использует минимальный уровень фильтрации спама.

Низкий уровень безопасности рекомендуется устанавливать при работе в безопасной среде (например, при использовании защищенной корпоративной почты).

При установке низкого уровня безопасности может снизиться частота распознавания обычной почты как спама и возможного спама.

Восстановить рекомендуемый уровень безопасности

По ссылке Kaspersky Anti-Virus устанавливает уровень безопасности **Рекомендуемый**. Ссылка отображается, если вы изменили настройки в окне **Дополнительные настройки Анти-Спама** в блоке **Считать спамом следующие сообщения**.

Расширенная настройка

По ссылке открывается окно дополнительных настроек Анти-Спама.

Дополнительные настройки Анти-Спама

В блоке **Считать спамом следующие сообщения** вы можете задать условия фильтрации сообщений, в соответствии с которыми Анти-Спам признает сообщение спамом.

С элементами фишинга

Флажок включает / выключает проверку почтовых сообщений на наличие элементов фишинга в тексте или ссылок, присутствующих в списке фишинговых веб-адресов.

Если флажок установлен, Анти-Спам считает спамом сообщение, в котором есть ссылка из списка фишинговых веб-адресов.

Если флажок снят, Анти-Спам не проверяет ссылки из сообщения по списку фишинговых веб-адресов.

Со ссылками из базы вредоносных веб-адресов

Флажок включает / выключает проверку ссылок, содержащихся в почтовых сообщениях, на принадлежность к списку вредоносных веб-адресов.

От запрещенных отправителей

Флажок включает / выключает фильтрацию сообщений по списку запрещенных отправителей, сообщения от которых Анти-Спам считает спамом.

Выбрать

Кнопка, расположенная справа от флажка **От запрещенных отправителей**. При нажатии на нее открывается окно **Запрещенные отправители**, в котором вы можете сформировать список запрещенных отправителей.

При создании списка вы можете задавать как адреса, так и маски адресов запрещенных отправителей.

Кнопка доступна, если установлен флажок **От запрещенных отправителей**.

С запрещенными фразами

Флажок включает / выключает фильтрацию сообщений по списку запрещенных фраз, наличие которых в сообщении указывает на то, что письмо является спамом.

Выбрать

По ссылке открывается окно **Запрещенные фразы**, в котором вы можете сформировать список запрещенных фраз.

При создании списка вы можете задавать как отдельные фразы, так и маски запрещенных фраз.

Ссылка доступна, если установлен флажок **С запрещенными фразами**.

С нецензурными словами

Ссылка, по которой открывается окно **Нецензурные слова**. В окне вы можете сформировать список нецензурных слов. Наличие этих слов в сообщении свидетельствует о том, что письмо является спамом.

Ссылка доступна, если установлен флажок **С нецензурными словами**.

В блоке **Считать полезными следующие сообщения** вы можете задать признаки, при наличии которых Анти-Спам считает сообщение полезным.

От разрешенных отправителей

Флажок включает / выключает проверку адреса отправителя по списку разрешенных отправителей.

Если флажок установлен, Анти-Спам считает полезными письма от разрешенных отправителей.

Если флажок снят, Анти-Спам не считает полезными письма от разрешенных отправителей. Фильтрация сообщений по списку разрешенных отправителей не производится.

Выбрать

По ссылке открывается окно **Разрешенные отправители**, в котором вы можете сформировать список разрешенных отправителей.

При создании списка вы можете задавать как адреса, так и маски адресов разрешенных отправителей.

Ссылка доступна, если установлен флажок **От разрешенных отправителей**.

С разрешенными фразами

Флажок включает / выключает проверку сообщения по списку разрешенных фраз.

Если флажок установлен, Анти-Спам считает полезным сообщение, в котором есть фразы из этого списка.

Если флажок снят, Анти-Спам не фильтрует сообщения по списку разрешенных фраз и не считает полезными сообщения, в которых есть фразы из этого списка.

Выбрать

По ссылке открывается окно **Разрешенные фразы**, в котором вы можете сформировать список разрешенных фраз.

При создании списка вы можете задавать как отдельные фразы, так и маски разрешенных фраз.

Ссылка доступна, если установлен флажок **С разрешенными фразами**.

В блоке **Действия с сообщениями** вы можете указать, какие метки должны добавляться к теме сообщения, которому Анти-Спам присвоил статус *Спам* или *Возможный спам*.

Добавлять метку [!! SPAM] к теме сообщения, признанного спамом

Флажок включает / выключает автоматическое добавление текстовой метки в тему сообщений, которым Анти-Спам присвоил статус *Спам*.

Текст метки указывается в поле справа от флажка. По умолчанию Анти-Спам добавляет метку **[!! SPAM]**.

Добавлять метку [?? Probable SPAM] к теме сообщения, признанного возможным спамом

Флажок включает / выключает автоматическое добавление текстовой метки в тему сообщений, которым Анти-Спам присвоил статус *Возможный спам*.

Текст метки указывается в поле справа от флажка. По умолчанию Анти-Спам добавляет метку **[?? Probable Spam]**.

Окно Добавление / изменение запрещенной фразы

Маска фразы

Фраза или маска фразы, наличие которой в сообщении является признаком спама.

Весовой коэффициент фразы

Числовое значение, выражающее вероятность того, что письмо, содержащее запрещенную фразу, является спамом. Чем выше весовой коэффициент, тем выше вероятность того, что письмо, в котором содержится запрещенная фраза, является спамом.

Анти-Спам определяет письмо как спам, если сумма весовых коэффициентов запрещенных фраз в письме превышает установленное значение.

Статус

В блоке **Статус** вы можете указать, должен ли Анти-Спам проверять сообщения на наличие запрещенной фразы:

- **Активно**. Анти-Спам проверяет сообщения на наличие запрещенной фразы.
- **Неактивно**. Анти-Спам не проверяет сообщения на наличие запрещенной фразы.

Окно Запрещенные отправители

Кнопка

При нажатии на кнопку открывается меню, в котором можно выбрать действие:

- **Импортировать и добавить к существующему**. При выборе этого действия можно загрузить список запрещенных отправителей из файла формата CSV. Текущий список отправителей не удаляется.
- **Импортировать и заменить существующий**. При выборе этого действия можно загрузить список запрещенных отправителей из файла формата CSV. Текущий список отправителей удаляется.
- **Экспортировать**. При выборе этого действия можно сохранить список запрещенных отправителей в файле формата CSV.

Список Запрещенные отправители

Содержит список адресов, сообщения с которых Анти-Спам считает спамом.

Вы можете добавить в список адрес или маску адреса.

Если в графе **Статус** в строке адреса установлено значение *Активно*, Анти-Спам считает адрес запрещенным.

Если в графе **Статус** в строке адреса установлено значение *Неактивно*, Анти-Спам исключает выбранный адрес из списка.

Адрес отправителя

Графа, в которой указывается адрес или маска адреса электронной почты запрещенного отправителя.

Статус

Графа, в которой указано, считает ли Анти-Спам сообщения, присылаемые с этого адреса, спамом.

Если в строке адреса установлено значение *Активно*, Анти-Спам считает сообщения с этого адреса спамом.

Если в строке адреса установлено значение *Неактивно*, Анти-Спам исключает выбранный адрес из списка.

Изменить

При нажатии на кнопку открывается окно для изменения выбранного в списке адреса или маски адреса.

Удалить

При нажатии на кнопку Анти-Спам удаляет из списка выбранный адрес или маску адреса.

Добавить

При нажатии на кнопку открывается окно добавления в список адреса или маски адреса.

Окно Запрещенные фразы

Кнопка

При нажатии на кнопку открывается меню, в котором можно выбрать действие:

- **Импортировать и добавить к существующему**. При выборе этого действия можно загрузить список запрещенных фраз из файла формата CSV. Текущие фразы не удаляются.
- **Импортировать и заменить существующий**. При выборе этого действия можно загрузить список запрещенных фраз из файла формата CSV. Текущие фразы удаляются.
- **Экспортировать**. При выборе этого действия можно сохранить список запрещенных фраз в файле формата CSV.

Список запрещенных фраз

Содержит ключевые фразы, которые указывают на то, что содержащее их письмо является спамом.

Вы можете добавить в список фразу или маску фразы.

Если в графе **Статус** в строке фразы установлено значение *Активно*, Анти-Спам использует фразу при фильтрации сообщений.

Если в графе **Статус** в строке фразы установлено значение *Неактивно*, Анти-Спам исключает фразу из списка и не использует ее при фильтрации сообщений.

Изменить

При нажатии на кнопку открывается окно, в котором можно изменить выбранную в списке фразу или маску фразы.

Удалить

При нажатии на кнопку Анти-Спам удаляет из списка выбранную фразу или маску фразы.

Добавить

При нажатии на кнопку открывается окно, в котором можно добавить в список фразу или маску фразы.

Окно Добавление / изменение адреса электронной почты

Маска адреса электронной почты

В окне вы можете указать адрес или маску адреса электронной почты.

При вводе маски вы можете использовать символы * и ? (где * – любая последовательность символов, а ? – любой один символ).

Статус

В блоке **Статус** вы можете указать, должен ли Анти-Спам блокировать сообщения, отправленные с этого адреса, при проверке сообщений по списку разрешенных / запрещенных отправителей:

- **Активно**. Анти-Спам блокирует сообщения, отправленные с этого адреса.
- **Неактивно**. Анти-Спам не блокирует сообщения, отправленные с этого адреса.

Окно Добавление / изменение разрешенной фразы

Маска фразы

Фраза или маска фразы, наличие которой в сообщении свидетельствует о том, что письмо не является спамом.

Весовой коэффициент фразы

Числовое значение, выражающее вероятность того, что письмо, содержащее разрешенную фразу, не является спамом. Чем выше весовой коэффициент, тем выше вероятность того, что письмо, в котором содержится разрешенная фраза, не является спамом.

Анти-Спам не определяет письмо как спам, если сумма весовых коэффициентов разрешенных фраз в письме превышает установленное значение.

Статус

В блоке **Статус** вы можете указать, должен ли Анти-Спам проверять сообщения на наличие разрешенной фразы:

- **Активно**. Анти-Спам проверяет сообщения на наличие разрешенной фразы.
- **Неактивно**. Анти-Спам не проверяет сообщения на наличие разрешенной фразы.

Окно Разрешенные отправители

Кнопка

При нажатии на кнопку открывается меню, в котором можно выбрать действие:

- **Импортировать и добавить к существующему**. При выборе этого действия можно загрузить список разрешенных отправителей из файла формата CSV. Текущий список отправителей не удаляется.
- **Импортировать и заменить существующий**. При выборе этого действия можно загрузить список разрешенных отправителей из файла формата CSV. Текущий список отправителей удаляется.
- **Экспортировать**. При выборе этого действия можно сохранить список разрешенных отправителей в файле формата CSV.

Список Разрешенные отправители

Содержит список адресов отправителей, сообщения от которых Анти-Спам считает полезными.

Вы можете добавить в список адрес или маску адреса.

Если в графе **Статус** в строке адреса установлено значение *Активно*, Анти-Спам считает письмо от этого отправителя полезным.

Если в графе **Статус** в строке адреса установлено значение *Неактивно*, Анти-Спам не считает все письма от этого отправителя полезными и проверяет эти письма на основе стандартных методов проверки.

Адрес отправителя

Графа, в которой указывается адрес или маска адреса электронной почты разрешенного отправителя.

Статус

Графа, в которой указано, считает ли Анти-Спам сообщения, присылаемые с этого адреса, полезными.

Если в строке адреса установлено значение *Активно*, Анти-Спам считает сообщения с этого адреса полезными.

Если в строке адреса установлено значение *Неактивно*, Анти-Спам исключает выбранный адрес из списка.

Изменить

Кнопка, по которой открывается окно, в котором вы можете изменить адрес или маску адреса в списке разрешенных отправителей.

Удалить

Кнопка, по которой Анти-Спам удаляет из списка выбранный адрес или маску адреса.

Добавить

При нажатии на кнопку открывается окно, в котором вы можете добавить адрес или маску адреса в список разрешенных отправителей.

Добавлять получателей моих писем в разрешенные отправители

Если флажок установлен, программа добавляет получателей ваших писем в список разрешенных отправителей.

Окно Разрешенные фразы

Кнопка

При нажатии на кнопку открывается меню, в котором можно выбрать действие:

- **Импортировать и добавить к существующему**. При выборе этого действия можно загрузить список разрешенных фраз из файла формата CSV. Текущие фразы не удаляются.
- **Импортировать и заменить существующий**. При выборе этого действия можно загрузить список разрешенных фраз из файла формата CSV. Текущие фразы удаляются.
- **Экспортировать**. При выборе этого действия можно сохранить список разрешенных фраз в файле формата CSV.

Список разрешенных фраз

Содержит ключевые фразы, наличие которых в сообщении считается признаком полезного письма.

Вы можете добавить в список фразу или маску фразы.

Если в графе **Статус** в строке фразы установлено значение *Активно*, Анти-Спам использует фразу при фильтрации сообщений.

Если в графе **Статус** в строке фразы установлено значение *Неактивно*, Анти-Спам не использует фразу при фильтрации сообщений.

Изменить

Кнопка, при нажатии на которую открывается окно, в котором вы можете изменить выбранную в списке фразу или маску фразы.

Удалить

При нажатии на кнопку Анти-Спам удаляет из списка выбранную фразу или маску фразы.

Добавить

При нажатии на кнопку открывается окно, в котором вы можете добавить в список фразу или маску фразы.

Настройки Безопасных платежей

Включить / выключить Безопасные платежи

Переключатель включает / выключает Безопасные платежи.

Если переключатель включен, Kaspersky Anti-Virus отслеживает все обращения к веб-сайтам банков или платежных систем и выполняет действие, заданное по умолчанию или настроенное пользователем. По умолчанию в режиме Безопасных платежей Kaspersky Anti-Virus запрашивает подтверждение пользователя на запуск Защищенного браузера.

Если переключатель выключен, Kaspersky Anti-Virus разрешает обращение к веб-сайтам банков или платежных систем с использованием обычного браузера.

Узнать больше

По ссылке открывается окно браузера на странице с более подробной информацией о компоненте.

В блоке **При первом обращении к сайтам банков или платежных систем** вы можете выбрать действие, которое Kaspersky Anti-Virus совершает при первом обращении к сайтам банков и платежных систем.

Запускать Защищенный браузер

Если Kaspersky Anti-Virus обнаруживает попытку доступа к указанному сайту, то открывает этот сайт в Защищенном браузере. В обычном браузере, использованном для обращения к сайту, отображается сообщение о запуске Защищенного браузера.

Запрашивать действие

Если Kaspersky Anti-Virus обнаруживает попытку доступа к указанному сайту, то предлагает запустить Защищенный браузер либо открыть сайт при помощи обычного браузера.

Не запускать Защищенный браузер

Когда вы обращаетесь к указанному сайту, Kaspersky Anti-Virus не использует Защищенный браузер. Сайт открывается в обычном браузере.

Блок **Дополнительно** позволяет настроить дополнительные настройки работы Безопасных платежей.

Для перехода к сайтам из окна Безопасных платежей использовать <браузер>

В раскрывающемся списке можно выбрать браузер, в котором Kaspersky Anti-Virus будет открывать сайты банков или платежных систем, выбранные из окна Безопасные платежи.

Безопасные платежи доступны при работе с браузерами Microsoft Internet Explorer, Microsoft Edge на базе Chromium, Mozilla Firefox, Google Chrome и Яндекс.Браузер.

По умолчанию Безопасные платежи используют браузер, установленный в операционной системе в качестве браузера по умолчанию.

Создать ярлык для Безопасных платежей

По ссылке на рабочем столе создается ярлык для запуска Безопасных платежей. Ярлык позволяет открыть окно со списком сайтов банков или платежных систем, при обращении к которым используется Защищенный браузер.

В 64-разрядной версии Windows 8, Windows 8.1 и Windows 10 для защиты браузера используется аппаратная виртуализация.

Настройки Веб-Антивируса

Включить / выключить Веб-Антивирус

Переключатель включает / выключает Веб-Антивирус.

Если переключатель включен, Веб-Антивирус защищает информацию, поступающую на компьютер по HTTP- и FTP-протоколам, и предотвращает запуск на компьютере опасных скриптов.

Если переключатель выключен, Веб-Антивирус отключен.

Узнать больше

По ссылке открывается окно браузера на странице с более подробной информацией о компоненте.

В блоке **Уровень безопасности** вы можете выбрать один из предустановленных наборов настроек (уровней безопасности) Веб-Антивируса.

Высокий

Уровень безопасности, при котором Веб-Антивирус максимально контролирует скрипты и объекты, поступающие по HTTP- и FTP-протоколам. Веб-Антивирус детально проверяет все объекты, используя полный набор баз программы, а также проверяет вложенные архивы, размер которых не превышает 1 МБ. Веб-Антивирус проводит глубинный эвристический анализ.

Рекомендуемый

Уровень безопасности, при котором обеспечивается оптимальная защита и скорость проверки веб-трафика и скриптов. Веб-Антивирус проверяет вложенные архивы, размер которых не превышает 1 МБ, и проводит эвристический анализ среднего уровня.

Низкий

Уровень безопасности, при котором обеспечивается максимальная скорость проверки веб-трафика и скриптов. Веб-Антивирус не проверяет архивы и проводит поверхностный эвристический анализ.

Восстановить рекомендуемый уровень безопасности

По ссылке Kaspersky Anti-Virus устанавливает уровень безопасности **Рекомендуемый**. Ссылка отображается, если вы изменили настройки проверки ссылок в окне **Дополнительные настройки Веб-Антивируса** в блоке **Дополнительно**.

Действие при обнаружении угрозы

В раскрывающемся списке можно выбрать действие, которое Веб-Антивирус должен выполнять при обнаружении зараженного или возможно зараженного объекта:

- **Выбирать действие автоматически**. Веб-Антивирус выбирает действие автоматически на основе установленных настроек. Если веб-ресурс находится в списке исключений или не содержит зараженных или возможно зараженных объектов, то Веб-Антивирус разрешает доступ к нему. Если в результате проверки Веб-Антивирус обнаруживает, что веб-ресурс содержит зараженный или возможно зараженный объект, он блокирует доступ к веб-ресурсу.

  Значение выбрано по умолчанию, если установлен автоматический режим защиты. Если установлен интерактивный режим защиты, настройка недоступна.

- **Блокировать**. Веб-Антивирус блокирует доступ к веб-ресурсу, на котором обнаружен зараженный или возможно зараженный объект, и выводит на экран окно уведомления о блокировке.

- **Разрешать**. Веб-Антивирус разрешает доступ к веб-ресурсу.

Расширенная настройка

По ссылке открывается окно **Дополнительные настройки Веб-антивируса**. В окне можно изменить настройки установки и активации плагинов программы в браузерах, настройки модуля проверки ссылок и настройки проверки ссылок по базам фишинговых и вредоносных веб-адресов.

Окно Доверенные веб-адреса

Кнопка

При нажатии на кнопку открывается меню, в котором можно выбрать действие:

- **Импортировать и добавить к существующему**. При выборе этого действия можно загрузить список доверенных веб-адресов из файла формата CSV. Текущие адреса не удаляются.
- **Импортировать и заменить существующий**. При выборе этого действия можно загрузить список доверенных веб-адресов из файла формата CSV. Текущие адреса удаляются.
- **Экспортировать**. При выборе этого действия можно сохранить список доверенных веб-адресов в файле формата CSV.

Список доверенных веб-адресов

Список включает в себя веб-адреса, содержимому которых вы доверяете. Веб-Антивирус не проверяет содержимое веб-адресов из этого списка. Вы можете добавить в список как доверенный веб-адрес, так и его маску.

Если в графе **Статус** в строке веб-адреса установлено значение *Активно*, Веб-Антивирус не проверяет содержимое веб-страниц с этим веб-адресом.

Если в графе **Статус** в строке веб-адреса установлено значение *Неактивно*, Веб-Антивирус проверяет содержимое веб-страниц с этим веб-адресом.

Изменить

Открывает окно, в котором можно изменить выбранный веб-адрес / маску веб-адреса.

Удалить

Удаляет из списка выбранный веб-адрес / маску веб-адреса.

Добавить

Открывает окно, в котором можно добавить веб-адрес / маску веб-адреса.

Окно Дополнительные настройки Веб-Антивируса

В блоке **Расширение Kaspersky Protection** вы можете указать настройки установки и активации расширения программы для браузеров.

Автоматически активировать расширение Kaspersky Protection в браузерах

Если флажок установлен, при запуске браузеров, поддерживаемых программой, в браузерах автоматически активируется расширение Kaspersky Protection.

Если флажок снят, автоматическая активация расширения Kaspersky Protection при запуске браузеров не выполняется.

В блоке **Проверка ссылок** вы можете указать сайты, на которых необходимо проверять ссылки, и сайты, которые необходимо исключить из проверки.

Проверять ссылки

Флажок включает / выключает проверку ссылок на веб-страницах на принадлежность к вредоносным и фишинговым веб-адресам.

На всех сайтах, кроме указанных

Режим проверки ссылок, при котором Веб-Антивирус проверяет все ссылки на веб-странице и информирует вас о степени опасности интернет-ресурса до того, как вы обратились к нему. Веб-Антивирус не проверяет содержимое веб-адресов, которые добавлены в список доверенных веб-адресов.

По ссылке **Настроить исключения** открывается окно, в котором вы можете сформировать список доверенных веб-адресов, содержимое которых Веб-Антивирус не проверяет.

Настроить исключения

По ссылке открывается окно **Настроить исключения**. В нем вы можете сформировать список доверенных веб-адресов, содержимому которых вы доверяете. Веб-Антивирус не будет проверять ссылки на этих сайтах на принадлежность к вредоносным и фишинговым веб-адресам.

Ссылка доступна, если выбран вариант **На всех сайтах, кроме указанных**.

Только на указанных сайтах

Режим проверки ссылок, при котором Веб-Антивирус анализирует содержимое только тех веб-адресов, которые добавлены в список проверяемых адресов. По результатам проверки Веб-Антивирус информирует вас о степени опасности интернет-ресурсов на указанных веб-адресах до того, как вы обратились к ним.

По ссылке **Настроить проверяемые сайты** открывается окно **Проверяемые сайты**. В нем вы можете сформировать список веб-адресов, которые Веб-Антивирус должен проверять.

Настроить проверяемые сайты

По ссылке открывается окно **Проверяемые сайты**. В нем вы можете сформировать список веб-адресов, которые Веб-Антивирус должен проверять.

Ссылка доступна, если выбран вариант **Только на указанных сайтах**.

Настроить проверку ссылок

Кнопка, при нажатии на которую открывается окно **Проверка ссылок**. В окне можно выбрать режим проверки ссылок и категории проверяемых сайтов.

Настроить доверенные веб-адреса

По ссылке открывается окно **Доверенные веб-адреса**. В этом окне вы можете сформировать список веб-адресов, содержимому которых вы доверяете.

В блоке **Дополнительно** вы можете выбрать способы проверки ссылок Веб-Антивирусом.

Проверять веб-адрес по базе вредоносных веб-адресов

Флажок включает / выключает проверку ссылок на принадлежность к списку вредоносных веб-адресов, в том числе веб-адресов, по которым доступны вредоносные программы-майнеры.

Список формируется специалистами "Лаборатории Касперского" и входит в комплект поставки программы.

Проверять веб-адрес по базе фишинговых веб-адресов

Флажок включает / выключает проверку ссылок на принадлежность к списку фишинговых веб-адресов.

В состав баз Kaspersky Anti-Virus включены известные в настоящее время сайты, которые используются для фишинг-атак. Специалисты "Лаборатории Касперского" пополняют список адресами, предоставляемыми международной организацией по борьбе с фишингом (The Anti-Phishing Working Group). Список пополняется при обновлении баз Kaspersky Anti-Virus.

Использовать эвристический анализ

Флажок включает / выключает использование эвристического анализа при проверке объектов.

Проверять веб-адрес по базе веб-адресов, на которых находятся рекламные программы

Если флажок установлен, Kaspersky Anti-Virus проверяет веб-адрес, по которому идет обращение, по базе веб-адресов, на которых находятся рекламные программы. Когда вы обращаетесь по веб-адресам этой категории, программа показывает уведомление о том, что веб-адрес может быть использован для показа рекламы.

Примером такой программы может быть программа, которая в процессе вашей работы с интернетом перенаправляет поисковый запрос на рекламный сайт. Таким образом, вы попадаете не на тот интернет-ресурс, который наилучшим образом соответствует вашему запросу, а на рекламный сайт.

Проверять веб-адрес по базе веб-адресов, на которых находятся легальные программы, которые могут быть использованы злоумышленниками для нанесения вреда компьютеру или вашим данным

Если флажок установлен, Kaspersky Anti-Virus проверяет веб-адрес, по которому идет обращение, по базе веб-адресов, на которых находятся легальные программы, которые могут быть использованы злоумышленниками для нанесения вреда компьютеру или вашим данным. Когда вы обращаетесь по веб-адресам этой категории, программа показывает уведомление о том, что веб-адрес может быть использован злоумышленниками для нанесения вреда компьютеру или вашим данным.

Примером программы из этой категории может быть программа удаленного администрирования, которую легально используют системные администраторы для диагностики и устранения неполадок. Злоумышленник может без вашего ведома установить такую программу на ваш компьютер, получить к нему доступ и использовать в своих целях.

Окно Исключения

Кнопка

При нажатии на кнопку открывается меню, в котором можно выбрать действие:

- **Импортировать и добавить к существующему**. При выборе этого действия можно загрузить список доверенных веб-адресов из файла формата CSV. Текущие адреса не удаляются.
- **Импортировать и заменить существующий**. При выборе этого действия можно загрузить список доверенных веб-адресов из файла формата CSV. Текущие адреса удаляются.
- **Экспортировать**. При выборе этого действия можно сохранить список доверенных веб-адресов в файле формата CSV.

Исключения

Список включает в себя адреса сайтов, содержимому которых вы доверяете. Веб-Антивирус не проверяет ссылки на веб-страницах сайтов из этого списка на принадлежность к вредоносным и фишинговым веб-адресам. Вы можете добавить в список как веб-адрес, так и его маску.

Если в графе **Статус** в строке веб-адреса установлено значение *Активно*, Веб-Антивирус не проверяет ссылки на веб-страницах с этим веб-адресом.

Если в графе **Статус** в строке веб-адреса установлено значение *Неактивно*, Веб-Антивирус проверяет ссылки на веб-страницах с этим веб-адресом.

Изменить

Открывает окно, в котором можно изменить выбранный веб-адрес / маску веб-адреса.

Удалить

Удаляет из списка выбранный веб-адрес / маску веб-адреса.

Добавить

Открывает окно, в котором можно добавить веб-адрес / маску веб-адреса.

Окно Добавление / Изменение веб-адреса

Маска веб-адреса (URL)

Веб-адрес / маска веб-адреса ресурса (например, веб-адрес `www.virus.com`).

При формировании маски можно использовать символ `*` – который заменяет любую последовательность символов. Например, маской `*abc*` обозначается любой веб-адрес, содержащий последовательность `abc`. Этой маске соответствует, например, веб-адрес `www.virus.com/download_virus/page_0-9abcdef.html`. В случае необходимости экранирования символа * можно использовать комбинацию **. При обработке данной комбинации символ * будет трактоваться как * (asterisk), а не как любое количество символов.

Статус

В блоке **Статус** вы можете указать, должен ли Веб-Антивирус проверять этот веб-адрес.

Возможны следующие варианты:

- **Активно**. Веб-Антивирус не проверяет этот веб-адрес.
- **Неактивно**. Веб-Антивирус проверяет этот веб-адрес.

Окно Проверка ссылок

В блоке **Проверяемые ссылки** вы можете выбрать, какие ссылки должен проверять Веб-Антивирус.

Любые ссылки

При выборе этого варианта Веб-Антивирус проверяет любые ссылки на всех типах веб-страниц.

Только ссылки в результатах поиска

При выборе этого варианта Веб-Антивирус проверяет только ссылки на веб-страницах с результатами поиска при использовании поисковых систем.

Отображать информацию о категориях содержимого сайтов

Флажок включает / выключает отображение информации о категориях содержимого сайта в комментарии к ссылке.

Категории сайтов

С помощью флажков можно выбрать категории сайтов, информацию о которых Веб-Антивирус должен отображать в комментарии к ссылке.

Если флажок установлен, Веб-Антивирус отображает информацию о категории ссылки в комментарии.

Если флажок снят, Веб-Антивирус не отображает информацию о категории сайта в комментарии к ссылке.

Окно Проверяемые сайты

Кнопка

При нажатии на кнопку открывается меню, в котором можно выбрать действие:

- **Импортировать и добавить к существующему**. При выборе этого действия можно загрузить список доверенных веб-адресов из файла формата CSV. Текущие адреса не удаляются.
- **Импортировать и заменить существующий**. При выборе этого действия можно загрузить список доверенных веб-адресов из файла формата CSV. Текущие адреса удаляются.
- **Экспортировать**. При выборе этого действия можно сохранить список доверенных веб-адресов в файле формата CSV.

Список проверяемых веб-адресов

Список включает в себя адреса сайтов, содержимому которых вы не доверяете. Веб-Антивирус анализирует информацию на страницах с этими веб-адресами на присутствие опасных объектов.

Вы можете добавить в список веб-адрес или маску веб-адреса.

Если в графе **Статус** в строке адреса сайта установлено значение *Активно*, Веб-Антивирус проверяет содержимое веб-страницы на наличие опасных объектов.

Если в графе **Статус** в строке адреса сайта установлено значение *Неактивно*, Веб-Антивирус не проверяет содержимое веб-страницы.

Изменить

Открывает окно, в котором можно изменить выбранный веб-адрес / маску веб-адреса.

Удалить

Удаляет из списка выбранный веб-адрес / маску веб-адреса.

Добавить

Открывает окно, в котором можно добавить веб-адрес / маску веб-адреса.

Окно Сайты "Лаборатории Касперского" и ее партнеров

В окне представлен список сайтов "Лаборатории Касперского" и ее партнеров.

Список составляют и обновляют специалисты "Лаборатории Касперского". В программе список обновляется автоматически при обновлении баз и программных модулей.

Настройки Защиты от сетевых атак

Включить / выключить Защиту от сетевых атак

Переключатель включает / выключает Защиту от сетевых атак.

Если переключатель включен, компонент Защита от сетевых атак запускается при старте операционной системы и отслеживает во входящем трафике активность, характерную для сетевых атак. Обнаружив попытку атаки на ваш компьютер, Kaspersky Anti-Virus блокирует любую сетевую активность атакующего компьютера в отношении вашего компьютера.

Если переключатель выключен, использование Защиты от сетевых атак выключено.

Добавлять атакующий компьютер в список блокирования на <время>

Флажок включает / выключает функцию блокирования атакующего компьютера на промежуток времени, указанный в поле ввода рядом с флажком. Время указывается в минутах.

Окно Категории

Все поля ввода данных для Безопасных платежей

Флажок включает / выключает отображение значка быстрого вызова Экранной клавиатуры в полях ввода на сайтах, открытых в Защищенном браузере при работе компонента Безопасные платежи.

Банки

Флажок включает / выключает отображение значка быстрого вызова Экранной клавиатуры в полях ввода на сайтах банков.

Электронная коммерция

Флажок включает / выключает отображение значка быстрого вызова Экранной клавиатуры в полях ввода на сайтах платежных систем.

Средства интернет-коммуникации

Флажок включает / выключает отображение значка быстрого вызова Экранной клавиатуры в полях сайтов, предназначенных для интернет-коммуникации, например, социальных сетей, сайтов знакомств, почтовых служб.

Настройка исключений

По ссылке открывается окно **Исключения для Экранной клавиатуры**. В окне можно изменить настройки отображения значка Экранной клавиатуры для определенных сайтов.

Окно Категории

Поля ввода паролей на всех сайтах

Флажок включает / выключает защиту ввода данных с аппаратной клавиатуры в поля, предназначенные для ввода паролей, на сайтах всех категорий.

Все поля ввода данных для Безопасных платежей

Флажок включает / выключает защиту ввода данных с аппаратной клавиатуры на сайтах, открытых в Защищенном браузере при работе компонента Безопасные платежи.

Банки

Флажок включает / выключает защиту ввода данных с аппаратной клавиатуры на сайтах банков.

Электронная коммерция

Флажок включает / выключает защиту ввода данных с аппаратной клавиатуры на сайтах платежных систем.

Средства интернет-коммуникации

Флажок включает / выключает защиту ввода данных с аппаратной клавиатуры во время использования различных средств интернет-коммуникации, например, социальных сетей, сайтов знакомств, почтовых служб.

Настройка исключений

По ссылке открывается окно **Исключения для защиты ввода с аппаратной клавиатуры**. В окне можно изменить настройки защиты ввода данных с аппаратной клавиатуры для определенных сайтов.

Настройки Контроля программ

Включить / выключить Контроль программ

Переключатель включает / выключает Контроль программ.

Узнать больше

По ссылке открывается окно браузера на странице с более подробной информацией о компоненте.

В блоке **Настройка ограничений для программ** можно настраивать включение программы в группу программ.

Доверять программам, имеющим цифровую подпись

Если флажок установлен, Контроль программ считает доверенными программы, имеющие цифровую подпись. Контроль программ помещает такие программы в группу **Доверенные** и не проверяет их активность.

Если флажок снят, Контроль программ не считает программы с обычной цифровой подписью доверенными и проверяет их активность. Программы доверенных поставщиков программного обеспечения (например, Microsoft) Контроль программ считает доверенными независимо от того, установлен флажок или снят.

Загружать правила для программ из Kaspersky Security Network (KSN)

Если флажок установлен, для определения группы доверия программы Контроль программ отправляет запрос в базу Kaspersky Security Network.

Если флажок снят, Контроль программ не ищет информацию в базе Kaspersky Security Network для определения группы доверия, к которой относится программа.

Изменить группу доверия для неизвестных программ

По ссылке открывается окно **Группа доверия для неизвестных программ**. В окне можно выбрать группу доверия, в которую будут помещаться неизвестные программы.

Можно выбрать один из следующих вариантов:

- Доверенные;
- Слабые ограничения;
- Сильные ограничения;
- Недоверенные.

Изменить группу доверия для программ, запущенных до начала работы Kaspersky Anti-Virus

По ссылке открывается окно **Группа доверия для программ, запущенных до начала работы Kaspersky Anti-Virus**. В окне можно изменить группу доверия для программ, запущенных до начала работы Kaspersky Anti-Virus. Сетевая активность программ, запущенных до начала работы Kaspersky Anti-Virus, будет контролироваться в соответствии с правилами выбранной вами группы доверия.

По умолчанию программы, запущенные до начала работы Kaspersky Anti-Virus, помещаются в одну из групп доверия на основании правил, заданных специалистами "Лаборатории Касперского".

Управление программами

По ссылке открывается окно **Управление программами**. В нем вы можете отредактировать список правил для программ.

Управление ресурсами

По ссылке открывается окно **Управление ресурсами**. В нем вы можете сформировать список персональных данных, а также список настроек и ресурсов операционной системы, доступ к которым контролирует Контроль программ.

Настройки Мониторинга активности

Включить / выключить

Переключатель включает / выключает Мониторинг активности.

Если переключатель включен, Мониторинг активности собирает и сохраняет данные о всех событиях, которые происходят в операционной системе (например, изменение файла, изменение ключей в реестре, запуск драйверов, попытка завершить работу компьютера). Эти данные используются, чтобы отследить вредоносную и другую активность программ (в том числе программ-вымогателей) и восстановить состояние операционной системы до появления в ней программы (отменить последствия вредоносной или другой активности программы). В некоторых случаях отменить последствия действий программ невозможно, например, если программа была обнаружена компонентом Контроль программ.

Мониторинг активности собирает данные из разных источников, в том числе и от других компонентов Kaspersky Anti-Virus. Мониторинг активности анализирует активность программ и предоставляет собранную информацию о событиях другим компонентам Kaspersky Anti-Virus.

В блоке **Защита от эксплойтов** вы можете настроить действия программы при запуске исполняемых файлов из уязвимых программ.

Контролировать попытки выполнить несанкционированные операции

Флажок включает / выключает функцию защиты от эксплойтов.

Если флажок установлен, Kaspersky Anti-Virus отслеживает исполняемые файлы, запускаемые уязвимыми программами. Если Kaspersky Anti-Virus обнаруживает, что попытка запустить исполняемый файл из уязвимой программы не была инициирована пользователем, то он выполняет действие, выбранное в раскрывающемся списке **При обнаружении угрозы**.

При обновлении Kaspersky Anti-Virus с версии более ранней, чем Kaspersky Anti-Virus 2018, эта настройка принимает значение по умолчанию.

При обнаружении угрозы

В раскрывающемся списке можно выбрать действие, которое должен выполнять Мониторинг активности в случае запуска исполняемых файлов из контролируемых уязвимых программ.

Список содержит следующие варианты действий:

- **Выбирать действие автоматически**. Мониторинг активности автоматически выполняет действие, указанное в настройках программы и добавляет информацию о выбранном действии в отчет.

В автоматическом режиме защиты этот вариант выбран по умолчанию. В интерактивном режиме защиты этот вариант недоступен.

- **Запрашивать действие**. Мониторинг активности запрашивает действие у пользователя.

В интерактивном режиме защиты этот вариант выбран по умолчанию. В автоматическом режиме защиты этот вариант недоступен.

- **Разрешать действие**. Мониторинг активности разрешает запуск исполняемого файла.
- **Запрещать действие**. Мониторинг активности блокирует запуск исполняемого файла.

При обнаружении вредоносной или другой активности программы

В раскрывающемся списке можно выбрать действие, которое должен выполнять Мониторинг активности, если в результате анализа активности была замечена вредоносная или другая активность программы.

Список содержит следующие варианты действий:

- **Запрашивать действие**. Мониторинг активности запрашивает действие у пользователя.

В интерактивном режиме защиты этот вариант выбран по умолчанию. В автоматическом режиме защиты этот вариант недоступен.

- **Выбирать действие автоматически**. Мониторинг активности автоматически выполняет над программой действие, рекомендуемое специалистами "Лаборатории Касперского".

В автоматическом режиме защиты этот вариант выбран по умолчанию. В интерактивном режиме защиты этот вариант недоступен.

- **Удалять программу**. Мониторинг активности удаляет программу.
- **Завершать работу программы**. Мониторинг активности завершает все процессы программы.
- **Пропускать**. Мониторинг активности не предпринимает никаких действий с программой.

[При возможности отменить последствия вредоносной или другой активности программы]

В раскрывающемся списке можно выбрать действие, которое Мониторинг активности должен выполнять при наличии возможности отменить последствия вредоносной или другой активности программы.

Список содержит следующие варианты действий:

- **Запрашивать действие**. Если в результате работы Мониторинга активности, Файлового Антивируса или выполнения задачи проверки подтверждается необходимость отмены последствий, Мониторинг активности запрашивает действие у пользователя.

В интерактивном режиме защиты этот вариант выбран по умолчанию. В автоматическом режиме защиты этот вариант недоступен.

- **Выбирать действие автоматически**. Если по результатам анализа активности программы Мониторинг активности признает ее вредоносной, то он выполняет отмену последствий активности программы и уведомляет об этом пользователя.

Мониторинг активности добавляет информацию о событии и результатах обработки в отчет.

В автоматическом режиме защиты этот вариант выбран по умолчанию. В интерактивном режиме защиты этот вариант недоступен.

- **Выполнять откат**. Мониторинг активности выполняет отмену последствий вредоносной или другой активности программы.
- **Не выполнять откат**. Мониторинг активности сохраняет информацию о вредоносной или другой активности программы, но не выполняет отмену действий программы.

В блоке **Защита от программ блокировки экрана** вы можете настроить действия Kaspersky Anti-Virus при активизации программ блокировки экрана. Программы блокировки экрана – это вредоносные программы, которые ограничивают возможность работы на компьютере, блокируя экран, клавиатуру, доступ к панели задач и ярлыкам. Программы блокировки экрана могут требовать выкуп за возврат возможности работы с операционной системой. С помощью функции защита от программ блокировки экрана можно завершить работу программы блокировки экрана по нажатию определенной комбинации клавиш.

[Распознавать и закрывать программы блокировки экрана]

Флажок включает / выключает использование функции защиты от программ блокировки экрана.

Если флажок установлен, при обнаружении действий программы блокировки экрана вы можете остановить ее работу по нажатию комбинации клавиш, указанной в раскрывающемся списке под флажком.

При обновлении Kaspersky Anti-Virus с версии более ранней, чем Kaspersky Anti-Virus 2018, эта настройка принимает значение по умолчанию.

Для закрытия программы блокировки экрана вручную использовать комбинацию клавиш

В раскрывающемся списке можно выбрать клавишу или комбинацию клавиш, при нажатии которой функция защиты от программ блокировки экрана обнаруживает и удаляет программу блокировки экрана.

Окно Веб-маяки

В окне представлен список веб-маяков.

Список составляют и обновляют специалисты "Лаборатории Касперского". В программе список обновляется автоматически при обновлении баз и программных модулей.

Окно Дополнительные настройки Почтового Антивируса

В блоке **Область защиты** вы можете выбрать типы почтовых сообщений, которые должен проверять Почтовый Антивирус. Значения настроек, установленные по умолчанию в этом блоке, зависят от выбранного уровня безопасности.

Входящие и исходящие сообщения

Почтовый Антивирус проверяет и входящие, и исходящие сообщения.

Только входящие сообщения

Почтовый Антивирус проверяет только входящие сообщения.

В блоке **Эвристический анализ** вы можете включить использование эвристического анализа при проверке сообщений, а также указать уровень эвристического анализа. Значения настроек, установленные по умолчанию в этом блоке, зависят от выбранного уровня безопасности.

Использовать эвристический анализ

Флажок включает / выключает использование эвристического анализа при проверке объектов.

Ползунок

Ползунок позволяет регулировать уровень эвристического анализа. Уровень эвристического анализа обеспечивает баланс между тщательностью поиска угроз, степенью загрузки ресурсов операционной системы и временем проверки.

Существуют следующие уровни эвристического анализа:

- **Поверхностный**. Эвристический анализатор выполняет меньше действий, содержащихся в исполняемом файле. При таком режиме вероятность обнаружить угрозу снижается. Проверка требует меньше ресурсов системы и проходит быстрее.
- **Средний**. Эвристический анализатор выполняет то количество действий в исполняемом файле, которое рекомендовано специалистами "Лаборатории Касперского".
- **Глубокий**. Эвристический анализатор выполняет больше действий, содержащихся в исполняемом файле. При таком режиме вероятность обнаружить угрозу возрастает. Проверка требует больше ресурсов системы и занимает больше времени.

Ползунок доступен, если установлен флажок **Использовать эвристический анализ**.

В блоке **Проверка составных файлов** вы можете изменить настройки проверки архивов. Значения настроек, установленные по умолчанию в этом блоке, зависят от выбранного уровня безопасности.

Не проверять вложенные архивы

Флажок включает / выключает функцию, при использовании которой Почтовый Антивирус не проверяет архивы, вложенные в сообщение.

Не проверять архивы размером более

Флажок включает / выключает функцию, при использовании которой Почтовый Антивирус ограничивает максимальный размер проверяемых архивов. Эта функция позволяет ускорить проверку сообщений.

Максимальный размер задается в мегабайтах. По умолчанию задано значение 8 МБ.

Если флажок установлен, Почтовый Антивирус исключает из проверки архивы, размер которых больше заданного.

Если флажок снят, Почтовый Антивирус проверяет архивы любого размера.

В блоке **Встраивание в операционную систему** вы можете выбрать проверяемые протоколы и включить интеграцию плагинов Почтового Антивируса в почтовый клиент Microsoft Outlook®.

Проверять трафик POP3, SMTP, NNTP, IMAP

Если флажок установлен, Почтовый Антивирус проверяет поток почтовых сообщений по протоколам POP3 / SMTP / NNTP / IMAP до их скачивания на компьютер.

Если флажок снят, Почтовый Антивирус проверяет почтовые сообщения только после их скачивания на компьютер.

Подключить плагин для Microsoft Outlook

Флажок включает / выключает интеграцию плагина Почтового Антивируса в Microsoft Office Outlook. Эта функция позволяет быстро перейти к настройке Почтового Антивируса из почтового клиента Microsoft Office Outlook, а также изменить настройки проверки почтовых сообщений на присутствие опасных объектов.

Окно Дополнительные настройки Файлового Антивируса

В блоке **Типы файлов** вы можете выбрать тип файлов, который должен проверять Файловый Антивирус. Значения настроек, установленные по умолчанию в этом блоке, зависят от выбранного уровня безопасности.

Все файлы

Файловый Антивирус проверяет все файлы без исключения (любых форматов и расширений).

Файлы без расширения Файловый Антивирус считает исполняемыми и проверяет их всегда, независимо от того, файлы какого типа вы выбрали для проверки.

Файлы, проверяемые по формату

При выборе этого варианта Файловый Антивирус проверяет только файлы, в которые может внедриться вирус. Перед началом поиска вирусов в файле выполняется анализ его внутреннего заголовка на предмет формата файла (TXT, DOC, EXE и так далее). При проверке также учитывается расширение файла.

Файлы без расширения Файловый Антивирус считает исполняемыми. Файловый Антивирус проверяет их всегда, независимо от того, файлы какого типа вы выбрали для проверки.

Файлы, проверяемые по расширению

В этом случае Файловый Антивирус проверяет только потенциально заражаемые файлы. При этом формат файла определяется на основании его расширения.

Файлы без расширения Файловый Антивирус считает исполняемыми и проверяет их всегда, независимо от того, файлы какого типа вы выбрали для проверки.

Изменить область защиты

По ссылке открывается окно **Область защиты Файлового Антивируса**.

Блок **Методы проверки** предназначен для выбора методов, которые Файловый Антивирус должен использовать при проверке компьютера. Значения настроек, установленные по умолчанию в этом блоке, зависят от выбранного уровня безопасности.

Сигнатурный анализ

При сигнатурном анализе используются базы Kaspersky Anti-Virus, содержащие описания известных угроз и методы их устранения. Защита с помощью сигнатурного анализа обеспечивает минимально допустимый уровень безопасности.

В соответствии с рекомендациями специалистов "Лаборатории Касперского" этот метод анализа всегда включен.

Эвристический анализ

Флажок включает / выключает использование эвристического анализа при проверке компьютера.

Ползунок

Изменяет уровень эвристического анализа. Уровень эвристического анализа обеспечивает баланс между тщательностью поиска угроз, степенью загрузки ресурсов операционной системы и временем проверки.

Существуют следующие уровни эвристического анализа:

- **Поверхностный**. Эвристический анализатор выполняет меньше действий, содержащихся в исполняемом файле. При таком режиме вероятность обнаружить угрозу снижается. Проверка требует меньше ресурсов системы и проходит быстрее.
- **Средний**. Эвристический анализатор выполняет то количество инструкций в исполняемом файле, которое рекомендовано специалистами "Лаборатории Касперского".
- **Глубокий**. Эвристический анализатор выполняет больше действий, которые содержатся в исполняемом файле. При таком режиме вероятность обнаружить угрозу возрастает. Проверка требует больше ресурсов системы и занимает больше времени.

Блок **Оптимизация проверки** предназначен для выбора способов, которые позволяют сократить время проверки. Значение настройки, установленное по умолчанию в этом блоке, зависит от выбранного уровня безопасности.

Проверять только новые и измененные файлы

Флажок включает / выключает режим проверки только новых файлов и файлов, которые изменились с момента предыдущего их анализа. Файловый Антивирус проверяет как простые, так и составные файлы.

Блок **Проверка составных файлов** содержит список составных файлов, которые Файловый Антивирус анализирует на присутствие вирусов. Значение настройки, установленное по умолчанию в этом блоке, зависит от выбранного уровня безопасности.

Проверять архивы

Флажок включает / выключает проверку архивов форматов RAR, ARJ, ZIP, CAB, LHA, JAR, ICE.

Проверять установочные пакеты

Флажок включает / выключает проверку установочных пакетов.

Проверять вложенные OLE-объекты

Флажок включает / выключает функцию, при использовании которой Kaspersky Anti-Virus проверяет вложенные в файл OLE-объекты (например, таблицы Microsoft Office Excel® или макросы, внедренные в файл Microsoft Office Word, вложения почтового сообщения).

Дополнительные настройки

При нажатии на кнопку открывается окно **Составные файлы**. В окне вы можете изменить настройки проверки составных файлов.

В блоке **Режим проверки** вы можете выбрать условие, при котором Файловый Антивирус начинает проверять файл.

Интеллектуальный

Режим проверки, при котором Файловый Антивирус проверяет объект на основании анализа операций, выполняемых над объектом (этот режим используется по умолчанию).

Например, при работе с документом Microsoft® Office Kaspersky Anti-Virus проверяет файл при первом открытии и при последнем закрытии. Все промежуточные операции перезаписи файла из проверки исключаются.

При доступе и изменении

Режим проверки, при котором Файловый Антивирус проверяет объекты при попытке их открыть / изменить.

При доступе

Режим проверки, при котором Файловый Антивирус проверяет объекты только при попытке их открыть.

При выполнении

Режим проверки, при котором Файловый Антивирус проверяет объекты только при попытке их запустить.

В блоке **Технологии проверки** вы можете выбрать технологию проверки файлов.

Технология iSwift

Технология, представляющая собой развитие технологии iChecker для компьютеров с файловой системой NTFS.

Технология iSwift имеет ограничение: она привязана к конкретному местоположению файла в файловой системе и применима только к объектам, расположенным в файловой системе NTFS.

Флажок включает / выключает использование технологии iSwift.

Технология iChecker

Технология, позволяющая увеличить скорость проверки за счет исключения из нее некоторых файлов. Файлы исключаются из проверки по специальному алгоритму, учитывающему дату выпуска баз Kaspersky Anti-Virus, дату предыдущей проверки файла, а также изменение настроек проверки.

Технология iChecker имеет ограничение: она не работает с файлами больших размеров, а кроме того, применима только к файлам с известной программе структурой (например, к файлам формата EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP, RAR).

Флажок включает / выключает использование технологии iChecker.

В блоке **Проверка скриптов** вы можете включить проверку скриптов и других объектов с помощью технологии Antimalware Scan Interface (AMSI).

Проверять скрипты с помощью Antimalware Scan Interface (AMSI)

Флажок включает / выключает проверку скриптов и других объектов с помощью технологии Antimalware Scan Interface (AMSI).

Настроить исключения

По ссылке открывается окно **Исключения**. В нем вы можете сформировать список скриптов и других объектов, которые Kaspersky Anti-Virus не будет проверять с помощью технологии Antimalware Scan Interface.

Окно Категории и исключения

Сервисы веб-аналитики

Если флажок установлен, компонент Защита от сбора данных блокирует сервисы веб-аналитики, использующие сбор данных с целью анализа ваших действий в интернете.

По ссылке **Показать список** открывается окно со списком сервисов веб-аналитики, использующих сбор данных с целью анализа ваших действий в интернете.

Рекламные агентства

Если флажок установлен, компонент Защита от сбора данных блокирует сбор данных о ваших действиях в интернете, который выполняют рекламные агентства в рекламных целях.

По ссылке **Показать список** открывается окно со списком рекламных агентств, выполняющих сбор данных о ваших действиях в интернете в рекламных целях.

Веб-маяки

Если флажок установлен, компонент Защита от сбора данных блокирует сбор данных о ваших действиях в интернете, выполняемый веб-маяками. Веб-маяки представляют собой невидимые пользователю объекты, внедренные в веб-страницу.

По ссылке **Показать список** открывается окно со списком веб-маяков.

Социальные сети

Если флажок установлен, компонент Защита от сбора данных блокирует сбор данных при посещении вами социальных сетей, кроме сбора данных, выполняемого самими социальными сетями. Блокирование сбора данных не мешает вам использовать функции "Мне нравится", "+1" и подобные им.

Флажки с названиями социальных сетей позволяют указать социальные сети, на сайтах которых программа должна блокировать сбор данных.

Исключения

По ссылке открывается окно, где вы можете указать сайты, на которых разрешаете сбор данных о ваших действиях.

Окно Несовместимые сайты

В окне представлен список сайтов, о которых специалистам "Лаборатории Касперского" известно, что их работоспособность может быть нарушена в результате запрета на сбор данных.

Список составляют и обновляют специалисты "Лаборатории Касперского". В программе список обновляется автоматически при обновлении баз и программных модулей.

Окно Настройки Защиты от сбора данных

Включить / выключить Защиту от сбора данных

Если переключатель включен, то, когда вы находитесь в интернете, компонент Защита от сбора данных обнаруживает попытки сбора данных сервисами отслеживания. Сервисы отслеживания используют полученную информацию для анализа ваших действий и могут применять результаты анализа, например, для показа вам соответствующей рекламной информации.

Только собирать статистику

При выборе этого варианта компонент Защита от сбора данных работает в *режиме обнаружения*, предоставляя вам возможность просмотреть отчеты об обнаруженных попытках сбора данных.

Запретить сбор данных

При выборе этого варианта компонент Защита от сбора данных работает в *режиме блокировки*, обнаруживая и блокируя попытки сбора данных. Информация о попытках сбора данных записывается в отчет.

Категории и исключения

По ссылке открывается окно, где можно указать категории сервисов отслеживания, которым вы хотите запретить или разрешить сбор данных. Из этого окна можно перейти к формированию списка сайтов, на которых вы хотите разрешить сбор данных.

Отправлять запрет на сбор данных

Если флажок установлен, то в режиме блокировки при обращении к сайту браузер отправляет на сайт HTTP-заголовок Do not track, означающий запрет на сбор данных о ваших действиях.

Разрешить сбор данных на сайтах "Лаборатории Касперского" и ее партнеров

Если флажок установлен, Kaspersky Anti-Virus разрешает сбор данных на сайтах "Лаборатории Касперского" и ее партнеров.

Сайты "Лаборатории Касперского" и ее партнеров

По ссылке открывается окно со списком сайтов "Лаборатории Касперского" и ее партнеров.

Разрешить сбор данных на несовместимых сайтах

Если флажок установлен, Kaspersky Anti-Virus разрешает сбор данных на сайтах, работоспособность которых может быть нарушена в результате запрета на сбор данных.

Несовместимые сайты

По ссылке открывается окно со списком сайтов, работоспособность которых может быть нарушена в результате запрета на сбор данных.

Окно Рекламные агентства

В окне представлен список рекламных агентств, выполняющих сбор данных о ваших действиях в интернете в рекламных целях.

Список составляют и обновляют специалисты "Лаборатории Касперского". В программе список обновляется автоматически при обновлении баз и программных модулей.

Окно Сервисы веб-аналитики

В окне представлен список сервисов веб-аналитики, использующих сбор данных с целью анализа ваших действий в интернете.

Список составляют и обновляют специалисты "Лаборатории Касперского". В программе список обновляется автоматически при обновлении баз и программных модулей.

Настройки Почтового Антивируса

Включить / выключить Почтовый Антивирус

Переключатель включает / выключает Почтовый Антивирус.

Если переключатель включен, Почтовый Антивирус запускается при старте операционной системы, находится в оперативной памяти компьютера и проверяет почтовые сообщения по протоколам POP3, SMTP, IMAP, MAPI и NNTP, а также через защищенные соединения (SSL) по протоколам POP3, SMTP и IMAP.

Если переключатель выключен, использование Почтового Антивируса отключено.

По умолчанию переключатель включен.

В блоке **Уровень безопасности** вы можете выбрать один из предустановленных наборов настроек Почтового Антивируса (уровней безопасности). Решение о том, какой уровень безопасности выбрать, зависит от условий работы и сложившейся ситуации.

Высокий

Уровень безопасности, при котором Почтовый Антивирус максимально контролирует почтовые сообщения. Почтовый Антивирус проверяет входящие и исходящие сообщения, вложенные архивы, а также проводит эвристический анализ с уровнем детализации **Глубокий**.

Высокий уровень безопасности применяется для работы в опасной среде. Примером опасной среды может служить подключение к одному из бесплатных почтовых сервисов из домашней сети, не обеспечивающей централизованную защиту почты.

Рекомендуемый

Уровень безопасности, при котором обеспечивается оптимальный баланс между производительностью операционной системы и безопасностью. При установленном уровне безопасности **Рекомендуемый** Почтовый Антивирус проверяет входящие и исходящие сообщения, вложенные архивы, а также выполняет эвристический анализ с уровнем детализации **Средний**.

Этот уровень безопасности выбран по умолчанию.

Низкий

Уровень безопасности, при котором Почтовый Антивирус проверяет только входящие сообщения, а также проводит эвристический анализ с уровнем детализации **Поверхностный**. Проверка вложенных архивов не производится. При установленном уровне безопасности **Низкий** Почтовый Антивирус проверяет почтовые сообщения максимально быстро и занимает меньше ресурсов операционной системы.

Уровень безопасности **Низкий** применяется для работы в хорошо защищенной среде. Примером такой среды может служить корпоративная сеть с централизованным обеспечением безопасности почты.

Восстановить рекомендуемый уровень безопасности

По ссылке Kaspersky Anti-Virus устанавливает уровень безопасности **Рекомендуемый**. Ссылка отображается, если вы изменили настройки проверки почтовых сообщений в окне **Дополнительные настройки Почтового Антивируса**, кроме настроек в блоке **Встраивание в операционную систему**.

Действие при обнаружении угрозы

В раскрывающемся списке можно выбрать действие, которое Почтовый Антивирус должен выполнять при обнаружении зараженных или возможно зараженных объектов:

- **Запрашивать при обнаружении**. Почтовый Антивирус сообщает вам об обнаружении зараженного или возможно зараженного объекта и запрашивает дальнейшее действие над ним.

  Это значение присутствует в списке и выбрано по умолчанию, если включен интерактивный режим защиты.

- **Выбирать действие автоматически**. При обнаружении зараженных или возможно зараженных объектов Почтовый Антивирус автоматически выполняет действие, рекомендуемое специалистами "Лаборатории Касперского". Для зараженных объектов таким действием будет **Лечить**. Это значение выбрано по умолчанию.

  Перед лечением или удалением зараженного объекта Почтовый Антивирус создает его резервную копию на тот случай, если впоследствии понадобится восстановить объект или появится возможность его вылечить.

  Это значение присутствует в списке и выбрано по умолчанию, если включен автоматический режим защиты.

- **Лечить**. Почтовый Антивирус пытается вылечить все обнаруженные зараженные объекты. Если попытка лечения не удалась, Почтовый Антивирус пропускает почтовое сообщение и добавляет в его заголовок информацию о том, что сообщение содержит зараженный объект. Информация об этом сохраняется в отчете.

- **Лечить, неизлечимую – удалять**. Почтовый Антивирус пытается вылечить все обнаруженные зараженные объекты. Если лечение объектов невозможно, Почтовый Антивирус удаляет их.

- **Блокировать**. Почтовый Антивирус блокирует доступ к зараженному или возможно зараженному объекту. Информация об этом сохраняется в отчете.

- **Удалять**. Почтовый Антивирус удаляет зараженный или возможно зараженный объект. Информация об этом сохраняется в отчете.

Расширенная настройка

По ссылке открывается окно **Дополнительные настройки Почтового Антивируса**. В этом окне вы можете изменить область защиты Почтового Антивируса, установить уровень анализа сообщений эвристическим анализатором, задать настройки проверки составных файлов и настройки встраивания Почтового Антивируса в операционную систему.

Настройки Сетевого экрана

Включить / выключить Сетевой экран

Переключатель включает / выключает Сетевой экран.

Узнать больше

По ссылке открывается окно браузера на странице с более подробной информацией о компоненте.

Уведомлять об уязвимостях при подключении к сети Wi-Fi

Если флажок установлен, Kaspersky Anti-Virus показывает уведомления при обнаружении уязвимостей сети Wi-Fi.

Если флажок снят, уведомления об уязвимостях сети Wi-Fi не отображаются.

Флажок доступен для изменения, если на компьютере не установлена программа Kaspersky Secure Connection.

Выбрать категории

По ссылке открывается окно **Категории**, в котором вы можете указать типы уязвимостей сетей Wi-Fi. Программа будет предупреждать вас о том, что сеть Wi-Fi, к которой вы подключаетесь, имеет указанную уязвимость.

Запрещать передачу пароля в интернете в незащищенном виде и показывать уведомление

Если флажок установлен, при работе в сети Wi-Fi Kaspersky Anti-Virus блокирует передачу паролей в незащищенном виде и выводит уведомление об этом.

Если флажок снят, передача паролей в незащищенном виде при работе в сети Wi-Fi не блокируется.

Восстановить скрытые уведомления

По ссылке можно восстановить значения настроек отображения уведомлений о передаче пароля в незащищенном виде. Уведомления, отображение которых вы отменили ранее, снова будут отображаться.

Разрешать подключения на случайный порт для активного режима FTP

Если флажок установлен, Сетевой экран разрешает подключение к вашему компьютеру на случайный порт, если до этого был обнаружен переход в активный режим FTP на управляющем соединении.

Если флажок снят, Сетевой экран запрещает подключение к вашему компьютеру на случайный порт, если до этого был обнаружен переход в активный режим FTP на управляющем соединении.

Не выключать Сетевой экран до полного завершения работы операционной системы

Флажок включает / выключает функцию, при использовании которой Сетевой экран не прекращает работу до полной остановки операционной системы.

Блокировать сетевые соединения, если нет возможности запросить действие у пользователя

Если флажок установлен, работа Сетевого экрана не останавливается в то время, когда не загружен интерфейс Kaspersky Anti-Virus.

Если флажок снят, при незагруженном интерфейсе Kaspersky Anti-Virus сетевые соединения блокироваться не будут.

Сети

По ссылке открывается окно **Сети**. В этом окне вы можете изменить настройки контроля сетевых соединений, которые Сетевой экран обнаружил на компьютере.

Настроить правила программ

По ссылке открывается окно **Сетевые правила программ**. В этом окне вы можете настроить сетевые правила для программ, установленных на компьютере.

Настроить пакетные правила

По ссылке открывается окно **Пакетные правила**.

В этом окне вы можете настроить пакетные правила. Пакетное правило состоит из набора условий и действий над пакетами и потоками данных, которые Сетевой экран выполняет при соблюдении заданных условий. Пакетные правила имеют более высокий приоритет, чем правила для программ.

Окно Добавление / Изменение пакетного правила

Действие

Раскрывающийся список, в котором вы можете выбрать действие Kaspersky Anti-Virus при обнаружении сетевой активности, для которой создается пакетное правило. Список содержит следующие значения:

- **Разрешить**. Kaspersky Anti-Virus разрешает сетевое соединение.
- **Запретить**. Kaspersky Anti-Virus запрещает сетевое соединение.
- **По правилам программ**. Kaspersky Anti-Virus не обрабатывает поток данных в соответствии с пакетным правилом, а применяет правило для программ.

Название

Название сетевого правила. В качестве названия вы можете использовать имя сетевого сервиса.

Сетевой сервис – это набор настроек, характеризующих сетевую активность, для которой вы создаете правило.

Направление

В раскрывающемся списке вы можете выбрать направление сетевой активности, которое требуется контролировать. Список содержит следующие направления сетевой активности:

- **Входящее**. Kaspersky Anti-Virus применяет правило к сетевому соединению, которое открыл удаленный компьютер.
- **Исходящее**. Kaspersky Anti-Virus применяет правило к сетевому соединению, которое открыл ваш компьютер.
- **Входящее/Исходящее**. Kaspersky Anti-Virus применяет правило как к входящему, так и к исходящему пакету или потоку данных, независимо от того, какой компьютер (ваш или удаленный) инициировал сетевое соединение.
- **Входящее (пакет)**. Kaspersky Anti-Virus применяет правило к пакетам данных, которые принимает ваш компьютер. Не применяется в правилах для программ.
- **Исходящее (пакет)**. Kaspersky Anti-Virus применяет правило к пакетам данных, которые передает ваш компьютер. Не применяется в правилах для программ.

Протокол

В списке вы можете выбрать тип протокола, который контролирует Kaspersky Anti-Virus (доступны протоколы TCP, UDP, ICMP, ICMPv6, IGMP, GRE).

Параметры ICMP

В блоке **Параметры ICMP** можно настроить тип и код проверяемых пакетов данных.

Тип проверяемых ICMP-пакетов вы можете выбрать в раскрывающемся списке слева.

Код проверяемых ICMP-пакетов вы можете выбрать в раскрывающемся списке справа.

Блок настроек доступен, если выбраны протоколы ICMP, ICMPv6.

Удаленные порты

Номера удаленных портов, перечисленные через запятую.

Локальные порты

Номера контролируемых локальных портов, перечисленные через запятую.

Адрес

Позволяет задать диапазон адресов, к которому Kaspersky Anti-Virus применяет правило. Возможные значения:

- **Любой адрес**. Kaspersky Anti-Virus применяет правило к любому IP-адресу.
- **Адреса подсети**. Kaspersky Anti-Virus применяет правило к IP-адресам всех сетей, подключенных в данный момент и имеющих указанный статус. Для этой настройки ниже доступен выбор статуса сети, для которого Kaspersky Anti-Virus применяет правило (доверенные сети, локальные сети, публичные сети).
- **Адреса из списка**. Kaspersky Anti-Virus применяет правило к IP-адресам, входящим в заданный диапазон. Для этой настройки доступны поля **Удаленные адреса** и **Локальные адреса** (список **Локальные адреса** недоступен при создании сетевого правила).

Статус

Статус сетевого правила, который обозначает, используется ли это сетевое правило Сетевым экраном.

Принимает одно из следующих значений:

- **Активно**. Сетевой экран использует сетевое правило для обработки пакетов данных.
- **Неактивно**. Сетевой экран не использует сетевое правило.

Записывать события

Флажок включает / выключает запись подключений, которые производятся с использованием выбранного протокола.

Если флажок установлен, Kaspersky Anti-Virus сохраняет информацию о событиях в отчете.

Шаблон сетевого правила

По ссылке раскрывается список, в котором вы можете выбрать шаблон для создания сетевого правила.

Окно Пакетные правила

Пакетные правила

Содержит пакетные правила. *Пакетное правило* состоит из набора условий и действий над пакетами и потоками данных, которые Сетевой экран выполняет при соблюдении заданных условий. Пакетные правила имеют более высокий приоритет, чем правила для программ.

По умолчанию с помощью пакетных правил программа ограничивает входящую сетевую активность по определенным портам протоколов TCP и UDP и фильтрует ICMP-сообщения.

Название

Графа, в которой указано название сетевого сервиса. *Сетевой сервис* – это набор настроек, характеризующих сетевую активность, для которой вы создаете правило.

Направление

Графа, в которой указана информация о направлении трафика.

В графе могут отображаться следующие значения:

- **Входящее (пакет)**. Kaspersky Anti-Virus применяет правило к пакетам данных, которые принимает ваш компьютер. Не применяется в правилах для программ.
- **Входящее**. Kaspersky Anti-Virus применяет правило к сетевому соединению, которое открыл удаленный компьютер.
- **Входящее/Исходящее**. Kaspersky Anti-Virus применяет правило как к входящему, так и к исходящему пакету или потоку данных, независимо от того, какой компьютер (ваш или удаленный) инициировал сетевое соединение.
- **Исходящее (пакет)**. Kaspersky Anti-Virus применяет правило к пакетам данных, которые передает ваш компьютер. Не применяется в правилах для программ.
- **Исходящее**. Kaspersky Anti-Virus применяет правило к сетевому соединению, которое открыл ваш компьютер.

Протокол

Протокол, по которому выполняется сетевое соединение.

Действие

В графе отображается действие, которое выполняет Сетевой экран, обнаружив сетевую активность, для которой создано пакетное правило. С помощью контекстного меню ячейки в этой графе вы можете перейти к изменению действия:

- **Разрешить**. Kaspersky Anti-Virus разрешает сетевое соединение.
- **Запретить**. Kaspersky Anti-Virus запрещает сетевое соединение.
- **По правилам программ**. Kaspersky Anti-Virus не обрабатывает поток данных в соответствии с пакетным правилом, а применяет правило для программ. Вариант доступен только при создании пакетного правила.

Статус

Поле, в котором отображается статус правила: *Активно* или *Неактивно*.

Если пакетному правилу присвоен статус *Активно*, Сетевой экран применяет правило.

Если пакетному правилу присвоен статус *Неактивно*, Сетевой экран не применяет правило.

Изменить

При нажатии на эту кнопку открывается окно **Изменение пакетного правила**. В этом окне можно изменить пакетное правило, выбранное в списке.

Удалить

При нажатии на эту кнопку Kaspersky Anti-Virus удаляет выбранное правило из списка.

Сетевой экран устанавливает приоритет выполнения для каждого пакетного правила. Приоритет пакетного правила определяется его положением в списке. Первое пакетное правило в списке обладает самым высоким приоритетом. Сетевой экран обрабатывает пакетные правила в порядке их расположения в списке, сверху вниз. Сетевой экран находит первое по списку подходящее для сетевого соединения пакетное правило и выполняет его действие: либо разрешает, либо блокирует сетевую активность. Сетевой экран игнорирует все последующие пакетные правила.

Вверх

При нажатии на эту кнопку правило перемещается на строку выше, тем самым получая более высокий приоритет выполнения.

Вниз

При нажатии на эту кнопку правило перемещается на строку ниже, тем самым получая более низкий приоритет выполнения.

Добавить

При нажатии на эту кнопку открывается окно **Добавление пакетного правила**. В окне можно создать новое пакетное правило.

Окно Свойства сети

Тип подключения

Тип сетевого соединения (например, интернет, проводное Ethernet-соединение, беспроводное соединение).

Состояние

Текущее состояние сетевого соединения: подключено или отключено.

Создано

Дата и время создания соединения.

Название

Обозначение сетевого соединения.

Тип сети

Поле, в котором отображается описание сети.

Для локальных и публичных сетей доступны дополнительные настройки сетевого соединения.

Адреса

Диапазон адресов, входящих в сеть. Отображается с использованием адресации IPv4 и/или IPv6.

В блоке **Дополнительные подсети** вы можете расширить диапазон адресов, входящих в сеть.

Добавить

При нажатии на кнопку открывается окно **IP-адрес**. В окне вы можете добавить адрес в список адресов.

Удалить

При нажатии на кнопку выбранный адрес удаляется из списка.

В блоке добавления нового IP-адреса вы можете указать настройки нового IP-адреса, добавляемого в подсеть. Блок отображается, если была нажата кнопка **Добавить**.

IP-адрес

Адрес или маска адресов, входящих в сеть. Можно указать IP-адрес или DNS-имя (например, IP-адрес `91.103.64.6`, DNS-имя `kaspersky.com`).

Добавить

При нажатии на кнопку указанный IP-адрес появляется в списке IP-адресов подсети.

В блоке **Уведомления** вы можете настроить режим оповещения при изменениях в сети.

Уведомлять при подключении к сети

Флажок включает / выключает уведомление Сетевого экрана о подключении сети.

Уведомлять при появлении нового MAC-адреса

Флажок включает / выключает уведомление Сетевого экрана об изменении MAC-адреса.

Например, если флажок установлен, Сетевой экран уведомляет вас о замене сетевого адаптера.

Уведомлять при изменении соответствия MAC-адреса IP-адресу

Флажок включает / выключает отображение уведомлений от Сетевого экрана об изменениях соответствия MAC-адреса и IP-адреса.

Например, если флажок установлен, Сетевой экран уведомляет вас, когда сервис DHCP назначает другой IP-адрес.

В блоке **Принтер по умолчанию** вы можете изменить настройки подключения к принтеру при установке соединения.

Выбирать принтер при подключении к сети

Флажок включает / выключает использование по умолчанию принтера, выбранного из раскрывающегося списка.

Флажок доступен, если в операционной системе вашего компьютера установлен принтер.

Окно Свойства сети (адаптер)

Название

Название сетевого адаптера.

Тип подключения

Тип сетевого адаптера, например, проводная или беспроводная сеть, модемное соединение.

Состояние

Текущее состояние сетевого соединения: *Подключено* или *Отключено*.

В блоке **Новые подключения** вы можете выбрать действие, которое Сетевой экран должен выполнить при обнаружении нового соединения с помощью этого адаптера.

Запрашивать группу

Если Сетевой экран обнаружит новое сетевое соединение, он уведомит вас об этом и запросит выбрать статус для новой сети.

Автоматически помещать новые сети в группу

Если Сетевой экран обнаружит новое сетевое соединение, он автоматически присвоит сети статус, выбранный в раскрывающемся списке.

В раскрывающемся списке вы можете назначить сети статус, который Сетевой экран автоматически присвоит новой сети.

Окно Сети

Список сетевых соединений

Список сетевых соединений, которые Сетевой экран обнаружил на компьютере.

Для каждого сетевого соединения отображается следующая информация:

- **Сеть**. Уникальное имя сетевого соединения.
- **Тип сети**. Описание сети: Публичная сеть (Интернет), Локальная сеть, Доверенная сеть.
- **Статус**. Текущее состояние сетевого соединения: *Подключена* или *Отключена*.

Изменить

Кнопка, при нажатии на которую открывается окно настройки выбранного сетевого соединения.

Кнопка доступна, если в списке сетевых соединений выбран хотя бы один объект.

Удалить

Кнопка, по которой вы можете удалить выбранное сетевое соединение из списка.

Настройки Файлового Антивируса

Включить / выключить Файловый Антивирус

Переключатель включает / выключает Файловый Антивирус.

Если переключатель включен, Файловый Антивирус запускается при старте операционной системы, находится в оперативной памяти компьютера и проверяет открываемые, сохраняемые и запускаемые файлы. По умолчанию для Файлового Антивируса установлены настройки, рекомендованные специалистами "Лаборатории Касперского".

Если переключатель выключен, использование Файлового Антивируса отключено.

В блоке **Уровень безопасности** вы можете выбрать один из трех предустановленных уровней безопасности файлов и памяти, используемых в процессе работы Файлового Антивируса.

Высокий

Уровень безопасности, при котором Файловый Антивирус максимально контролирует открываемые, сохраняемые и запускаемые файлы. Файловый Антивирус проверяет все типы файлов на всех жестких, сменных и сетевых дисках компьютера, а также архивы, установочные пакеты и вложенные OLE-объекты.

Рекомендуемый

Уровень безопасности, при котором обеспечивается оптимальный баланс между производительностью операционной системы и безопасностью. Он подходит для большинства случаев. Файловый Антивирус проверяет только файлы определенных форматов на всех жестких, сменных и сетевых дисках компьютера, а также выполняет поверхностный эвристический анализ. Проверяются OLE-объекты. Проверка установочных пакетов и архивов не производится.

Низкий

Уровень безопасности, при котором Файловый Антивирус проверяет только файлы с определенными расширениями на всех жестких, сменных и сетевых дисках компьютера, а также проводит поверхностный эвристический анализ. Проверка составных файлов не производится.

При включенном уровне безопасности **Низкий** достигается максимальная скорость проверки.

Восстановить рекомендуемый уровень безопасности

По ссылке Kaspersky Anti-Virus устанавливает уровень безопасности **Рекомендуемый**. Ссылка отображается, если вы изменили настройки в окне **Дополнительные настройки Файлового Антивируса**.

Действие при обнаружении угрозы

В раскрывающемся списке можно выбрать действие, которое Файловый Антивирус должен выполнять при обнаружении зараженных или возможно зараженных объектов:

- **Запрашивать при обнаружении**. Файловый Антивирус информирует вас об обнаружении зараженного или возможно зараженного объекта и запрашивает дальнейшее действие над ним.

  В интерактивном режиме защиты этот вариант выбран по умолчанию. В автоматическом режиме защиты этот вариант недоступен.

- **Выбирать действие автоматически**. При обнаружении зараженного или возможно зараженного объекта Файловый Антивирус автоматически выполняет над объектом действие, рекомендуемое специалистами "Лаборатории Касперского". Для зараженных объектов таким действием будет **Лечить**. Это значение выбрано по умолчанию.

  Перед лечением или удалением зараженного объекта Файловый Антивирус создает его резервную копию на тот случай, если впоследствии понадобится восстановить объект или появится возможность его вылечить.

  В автоматическом режиме защиты этот вариант выбран по умолчанию. В интерактивном режиме защиты этот вариант недоступен.

- **Лечить**. Файловый Антивирус пытается вылечить все обнаруженные зараженные объекты. Если лечение невозможно, то Файловый Антивирус блокирует доступ к этим объектам.

- **Лечить, неизлечимую – удалять**. Файловый Антивирус пытается вылечить все обнаруженные зараженные объекты. Если лечение невозможно, то Файловый Антивирус удаляет их.

- **Блокировать**. Файловый Антивирус блокирует доступ к объекту. Информация об этом сохраняется в отчете.

- **Удалять**. Файловый Антивирус удаляет зараженный или возможно зараженный объект. Информация об этом сохраняется в отчете.

Расширенная настройка

По ссылке открывается окно **Дополнительные настройки Файлового Антивируса**. В этом окне вы можете изменить область защиты Файлового Антивируса, установить уровень анализа файлов эвристическим анализатором, задать настройки проверки различных типов файлов, выбрать режимы и технологии проверки.

Окно Область защиты Файлового Антивируса

Список проверяемых объектов

Содержит объекты, которые проверяет Файловый Антивирус.

По умолчанию Файловый Антивирус проверяет файлы, запускаемые со всех жестких, съемных и сетевых дисков. Объекты, добавленные в список по умолчанию, невозможно изменить или удалить.

Если флажок установлен, Файловый Антивирус проверяет объект.

Если флажок снят, Файловый Антивирус исключает объект из проверки.

Добавить

При нажатии на кнопку открывается окно **Выбор файла или папки для проверки**. В окне вы можете выбрать папку или файл, которые нужно включить в область защиты Файлового Антивируса.

Кнопка

При нажатии на кнопку выбранный объект удаляется из списка.

Кнопка отображается справа от объектов, которые были добавлены вручную. Удалить объекты проверки, присутствующие в списке по умолчанию, невозможно.

Окно Составные файлы

В блоке **Фоновая проверка** вы можете настроить фоновый режим проверки, при использовании которого составные файлы большого размера быстрее становятся доступными для работы.

Распаковывать составные файлы в фоновом режиме

Флажок включает / выключает функцию, благодаря которой Файловый Антивирус сокращает время задержки при открытии составных файлов большого размера.

Если флажок установлен, то Файловый Антивирус не распаковывает файлы, размер которых превышает заданное ограничение. Файлы, размеры которых больше или равны заданному, доступны для работы во время их проверки. Файлы, размеры которых меньше заданного, доступны для работы только после того, как Файловый Антивирус их распакует и проверит содержимое.

Если флажок снят, Файловый Антивирус распаковывает все составные файлы.

Вне зависимости от того, проверяется ли сам составной файл, Файловый Антивирус проверяет файлы, извлеченные из него.

Минимальный размер файла

Файлы, размеры которых превышают заданное ограничение, будут доступны для работы во время их проверки. Значение задается в мегабайтах.

В блоке **Ограничение по размеру** вы можете ограничить проверку составных файлов большого размера.

Не распаковывать составные файлы большого размера

Если флажок установлен, то Файловый Антивирус исключает из проверки составные файлы, размеры которых больше заданного.

Если флажок снят, проверяются составные файлы любого размера.

Вне зависимости от того, проверяется ли сам составной файл, Файловый Антивирус проверяет файлы, извлеченные из него.

Максимальный размер файла

Kaspersky Anti-Virus проверяет только те файлы, размер которых не превышает указанного. Размер файлов задается в мегабайтах.

Окно Добавление / изменение персональных данных

Типы персональных данных

По ссылкам в поле **Название поля** подставляется соответствующий тип персональных данных.

Название поля

Описание, которое отображается в списке записей персональных данных (например, *Домашний телефон*, *Рабочий телефон*, *Почтовый индекс*).

Можно подставить описание персональных данных автоматически по нужной ссылке с типом персональных данных.

Значение

Персональные данные, пересылка которых запрещается или разрешается.

Отчет о пересылке персональных данных

В верхней части окна отображается имя учетной записи пользователя, отчет о действиях которого приводится в этом окне.

Контроль включен / выключен  /

Переключатель позволяет включать / выключать контроль действий пользователя с помощью Родительского контроля.

В зависимости от того контролирует ли действия пользователя Родительский контроль, переключатель имеет следующий вид:

 – Родительский контроль контролирует действия пользователя.

 – Родительский контроль не контролирует действия пользователя.

Контроль действий пользователя выполняется в соответствии с заданными для него настройками Родительского контроля.

В окне можно просмотреть информацию об употреблении выбранным пользователем ключевых слов и попытках пересылки персональных данных.

Сегодня

При нажатии на кнопку отображается отчет о действиях пользователя, совершенных за сегодняшний день.

Кнопки 

При нажатии на кнопки отображаются отчеты за предыдущий и следующий период.

День / Неделя / Месяц

Период, за который формируется отчет. Можно сформировать отчет за следующие периоды: день, неделя, месяц.

Кнопка 

При нажатии на кнопку открывается окно настройки Родительского контроля на разделе **Контроль содержимого**. В этом разделе можно указать ограничения пересылки персональных данных.

Список заблокированных персональных данных

Содержит перечень персональных данных в отправленных и полученных выбранным пользователем сообщениях за отчетный период.

Данные

Графа содержит персональные данные, которые содержались в отправленных или полученных сообщениях.

Для заблокированных персональных данных также указывается тип информации, запрещенной к пересылке.

Ресурс

В графе отображается сайт, через который пользователь пытался отправить или получить сообщение с персональными данными, запрещенными к пересылке.

Статус

Если пересылка сообщения была заблокирована Родительским контролем, в графе отображается значение *Заблокировано*.

Дата

Графа содержит дату отправки или получения сообщения, содержащего персональные данные, запрещенные к пересылке.

Выбор профиля пользователя

Сбор статистики

При нажатии на кнопку к учетной записи выбранного пользователя применяется профиль с предустановленными по умолчанию настройками. Этот профиль предусматривает только сбор статистики о действиях выбранного пользователя. Ограничения на использование программ и интернета не установлены.

Выборочные ограничения

К учетной записи выбранного пользователя применяются ограничения, настроенные вручную.

Ребенок (4+)

При нажатии на кнопку к учетной записи выбранного пользователя применяется профиль, предусмотренный для детей в возрасте от четырех до двенадцати лет. Этот профиль предусматривает следующие правила использования программ и интернета:

- разрешено использование интернета;
- разрешено посещение только сайтов, относящихся к категориям "Общение в сети", "Компьютерные игры";
- запрещена загрузка файлов всех типов;
- включен контроль использования компьютера, ограничения использования не установлены;
- включен контроль использования программ, ограничения использования не установлены;
- включен контроль использования игр, ограничения установлены в соответствии с рейтинговой системой.

Подросток (12+)

При нажатии на кнопку к учетной записи выбранного пользователя применяется профиль, предусмотренный для детей старше двенадцати лет. Этот профиль предусматривает следующие правила использования программ и интернета:

- разрешено использование интернета;
- разрешено посещение только сайтов, относящихся к категориям "Общение в сети", "Интернет-магазины, банки и платежные системы", "Компьютерные игры";
- включен контроль использования компьютера, ограничения использования не установлены;
- включен контроль использования программ, ограничения использования не установлены;
- включен контроль использования игр, ограничения установлены в соответствии с рейтинговой системой.

Настройки по умолчанию

При нажатии на кнопку к учетной записи выбранного пользователя применяется профиль с настройками по умолчанию. Этот профиль предусматривает следующие правила использования программ и интернета:

- разрешено использование интернета;
- разрешено посещение только сайтов, относящихся к категориям "Общение в сети", "Интернет-магазины, банки и платежные системы", "Компьютерные игры";
- включен безопасный поиск;
- включен контроль использования компьютера, ограничения использования не установлены;
- включен контроль использования программ, ограничения использования не установлены;
- включен контроль запуска игр, ограничения запуска не установлены;
- включен контроль защищенных SSL-соединений в браузерах.

Импорт

По ссылке открывается окно для выбора файла, содержащего настройки Родительского контроля. После выбора файла эти настройки применяются к учетной записи выбранного пользователя.

Экспорт

По ссылке открывается окно для сохранения текущих настроек Родительского контроля в файл.

Окно Добавить / Изменить маску веб-адреса

Маска веб-адреса

Адрес или маска адреса сайта, доступ к которому требуется разрешить ли запретить.

Действие

Позволяет разрешить или запретить доступ пользователя к сайту.

Можно выбрать один из следующих вариантов:

- **Разрешить**. При выборе этого варианта Родительский контроль разрешает пользователю доступ к сайту, даже если он относится к запрещенной категории или включено блокирование всех сайтов.
- **Запретить**. При выборе этого варианта Родительский контроль запрещает пользователю доступ к сайту, даже если он относится к разрешенной категории.

Тип

Позволяет указать область, на которую распространяется разрешение или запрет доступа к сайту.

Можно выбрать один из следующих вариантов:

- **Маска сайта**. При выборе этого варианта Родительский контроль разрешает или запрещает пользователю доступ ко всем веб-страницам указанного сайта.

  Например, если в поле **Маска веб-адреса** указан адрес example.com, то Родительский контроль будет разрешать или запрещать доступ ко всем веб-страницам сайта example.com: news.example.com, market.example.com, mail.example.com.

- **Указанный веб-адрес**. При выборе этого варианта Родительский контроль разрешает или запрещает пользователю доступ только к конкретной странице сайта, указанной в поле **Маска веб-адреса**.

  Например, если в поле **Маска веб-адреса** указан адрес mail.example.com/login, то Родительский контроль будет разрешать или запрещать доступ только к указанной странице авторизации для входа в почтовый ящик интернет-почты. На другие страницы сайта это правило распространяться не будет.

Применить шаблон

Позволяет применить к исключению один из существующих шаблонов с заданным набором настроек.

Вы можете выбрать один из следующих вариантов:

- **Весь сайт** – при выборе этого варианта Родительский контроль разрешает или запрещает доступ к домену, указанному в поле **Маска веб-адреса**. Например, если в поле **Маска веб-адреса** указан адрес example.com, Родительский контроль будет разрешать или запрещать доступ ко всем веб-страницам домена example.com: news.example.com, market.example.com, mail.example.com.

- **Указанная веб-страница** – при выборе этого варианта Родительский контроль разрешает или запрещает доступ к конкретной странице, указанной в поле **Маска веб-адреса**, и ко всем веб-адресам, содержащим эту страницу. Например, если в поле **Маска веб-адреса** указан адрес example.com/hl, Родительский контроль будет разрешать или запрещать доступ как к этой странице, так и к содержащим ее веб-адресам, например, example.com/hl/example1.html.

- **Указанный веб-адрес** – при выборе этого варианта Родительский контроль разрешает или запрещает доступ к конкретному веб-адресу, указанному в поле **Маска веб-адреса**. Например, если в поле **Маска веб-адреса** указан адрес mail.example.com/login, Родительский контроль будет разрешать или запрещать доступ только к указанной странице авторизации для входа в почтовый ящик интернет-почты. На другие страницы сайта это правило распространяться не будет.

Окно Исключения

В этом окне вы можете сформировать список исключений из заданных настроек Родительского контроля. Настройки доступа к сайтам, добавленным в список исключений, действуют как при блокировке сайтов по категориям (кнопка выбора **Блокировать доступ к сайтам из выбранных категорий**), так и при блокировке всех сайтов (кнопка выбора **Блокировать доступ ко всем сайтам**).

Например, можно разрешить доступ к сайтам из категории "Средства интернет-коммуникации", но добавить в список исключений сайт example.com с запретом доступа. В этом случае Родительский контроль разрешает доступ ко всем социальным сетям, кроме сайта example.com. Также можно установить блокирование всех сайтов и добавить в список исключений сайт интернет-почты, доступ к которому разрешен. В этом случае Родительский контроль предоставляет пользователю доступ только к сайту интернет-почты.

Список исключений

Список содержит перечень веб-адресов, доступ к которым разрешен или запрещен вне зависимости от установленных настроек Родительского контроля.

С помощью контекстного меню веб-адреса в списке можно изменить веб-адрес или удалить его из списка, а также разрешить или запретить доступ к сайту.

Маска веб-адреса

Адрес или маска адреса сайта, доступ к которому разрешен или запрещен.

Тип

В графе указана область применения запрета или разрешения доступа к сайту.

Если в графе установлено значение *Маска сайта*, разрешение или запрет доступа применяется ко всем страницам сайта.

Если в графе установлено значение *Указанный веб-адрес*, разрешение или запрет доступа применяется только к указанной странице сайта.

Действие

В графе указано, разрешен или запрещен доступ к сайту.

Если в графе установлено значение *Разрешено*, Родительский контроль разрешает доступ к сайту.

Если в графе установлено значение *Запрещено*, Родительский контроль запрещает доступ к сайту.

Изменить

При нажатии на кнопку открывается окно **Изменить**, где вы можете изменить маску веб-адреса или адрес веб-сайта, выбранного в списке исключений, и настройки доступа к нему.

Кнопка доступна, если в списке исключений выбрана маска веб-адреса.

Удалить

При нажатии на кнопку программа удаляет выбранную маску веб-адреса из списка исключений.

Кнопка доступна, если в списке исключений выбрана маска веб-адреса.

Добавить

При нажатии на кнопку открывается окно добавления маски веб-адреса, в котором можно добавить адрес или маску адреса веб-сайта в список исключений.

Окно Ограничения использования программы

В этом окне можно настроить ограничения времени использования выбранной программы.

В блоке **Рабочие дни** вы можете указать ограничения времени использования программы по рабочим дням.

Разрешить доступ не более <N> часов в день

Флажок включает / выключает ограничение времени использования программы в рабочие дни.

Если флажок установлен, Родительский контроль ограничивает суммарное время использования программы для выбранного пользователя. Ограничение времени использования программы (в часах) указывается в раскрывающемся списке рядом с флажком.

Если флажок снят, Родительский контроль не ограничивает использование программы по рабочим дням.

В блоке **Выходные дни** вы можете указать ограничения времени использования программы по выходным дням.

Разрешить доступ не более <N> часов в день

Флажок включает / выключает ограничение времени использования программы в выходные дни.

Если флажок установлен, Родительский контроль ограничивает суммарное время использования программы для выбранного пользователя. Ограничение времени использования программы (в часах) указывается в раскрывающемся списке рядом с флажком.

Если флажок снят, Родительский контроль не ограничивает использование программы по выходным дням.

В блоке **Перерывы в работе** вы можете настроить периодическое блокирование доступа к программе в течение суток.

Делать перерыв каждые <N> часов в течение <N минут>

Флажок включает / выключает периодическое блокирование работы программы с указанной длительностью, чтобы обеспечить отдых пользователя.

Если флажок установлен, Родительский контроль блокирует работу программы с периодичностью, указанной в раскрывающемся списке **<ЧЧ:ММ>**. Доступ блокируется на промежуток времени, указанный в раскрывающемся списке **<N минут>**.

В блоке **Точное время использования** отображается таблица времени использования программы. С помощью таблицы вы можете составить почасовое расписание использования программы пользователем в течение недели.

Таблица времени использования программы

С помощью таблицы можно указать дни недели и часы, когда пользователю разрешено пользоваться программой. Строки таблицы соответствуют дням недели, графы – интервалам в один час на временной шкале. В зависимости от установленных в операционной системе региональных настроек временная шкала может иметь 24- и 12-часовое представление. Цвета ячеек таблицы отражают установленные ограничения: красный цвет означает, что использование программы запрещено, серый – использование программы разрешено. При нажатии на ячейку таблицы цвет ячейки изменяется. При наведении на ячейку курсора мыши под таблицей отображается временной интервал, которому соответствует ячейка.

Окно Список персональных данных

Список персональных данных

Список содержит персональные данные пользователя, пересылку которых необходимо контролировать.

Название поля

В графе отображается тип персональных данных (например, *Номер банковской карты*, *Домашний телефон*).

Значение

В графе отображаются персональные данные (например, номер банковской карты, телефон), упоминание которых необходимо отслеживать в переписке.

Изменить

При нажатии на кнопку открывается окно, в котором вы можете изменить запись с персональными данными.

Удалить

Кнопка позволяет удалить выбранную запись из списка.

Добавить

При нажатии на кнопку открывается окно, в котором вы можете добавить в список персональных данных новую запись.

Отчет о заблокированных сайтах и загрузках

Сегодня

При нажатии на кнопку отображается отчет о действиях пользователя, совершенных за сегодняшний день.

Кнопки 

При нажатии на кнопки отображаются отчеты за предыдущий и следующий период.

День / Неделя / Месяц

Период, за который формируется отчет. Можно сформировать отчет за следующие периоды: день, неделя, месяц.

Кнопка 

При нажатии на кнопку открывается окно настройки Родительского контроля на разделе **Интернет**. В этом разделе можно ограничить выбранному пользователю время использования интернета и доступ к сайтам и ограничить скачивание файлов.

Заблокированные сайты и файлы

Список содержит перечень сайтов, открытие которых было запрещено Родительским контролем, а также перечень файлов, скачивание которых было заблокировано.

Список содержит следующую информацию:

- название заблокированного сайта или файла;
- причина, по которой пользователю заблокирована попытка доступа (например, *Сайт из запрещенной категории*);
- дата открытия сайта или скачивания файла.

Отчет о запускавшихся программах

В верхней части окна отображается имя учетной записи пользователя, отчет о действиях которого приводится в этом окне.

Контроль включен / выключен  /

Переключатель позволяет включать / выключать контроль действий пользователя с помощью Родительского контроля.

В зависимости от того контролирует ли действия пользователя Родительский контроль, переключатель имеет следующий вид:

 – Родительский контроль контролирует действия пользователя.

 – Родительский контроль не контролирует действия пользователя.

Контроль действий пользователя выполняется в соответствии с заданными для него настройками Родительского контроля.

В окне **Отчет о запускавшихся программах** вы можете получить информацию о запуске программ за отчетный период для выбранной учетной записи.

Сегодня

При нажатии на кнопку отображается отчет о действиях пользователя, совершенных за сегодняшний день.

Кнопки 

При нажатии на кнопки отображаются отчеты за предыдущий и следующий период.

День / Неделя / Месяц

Период, за который формируется отчет. Можно сформировать отчет за следующие периоды: день, неделя, месяц.

Кнопка 

При нажатии на кнопку открывается окно настройки Родительского контроля на разделе **Программы**. В этом разделе можно указать ограничения запуска и использования программ.

Самые используемые программы

Содержит перечень программ, которые запускались пользователем наиболее часто в течение отчетного периода. Также в списке отображается информация о длительности использования программ.

Заблокированные программы

Содержит перечень программ, запуск которых был заблокирован Родительским контролем. Программы отображаются в порядке их запуска, начиная с последних.

По ссылке **Еще <N>** можно перейти к просмотру других программ, запуск которых был заблокирован.

Все используемые программы

Содержит перечень всех программ, которые пользователь запускал в течение отчетного периода. Также в списке отображается информация о длительности использования программ.

Программы сгруппированы по категориям (например, "Игры" или "IM-клиенты").

При нажатии на кнопку ⌄ можно просмотреть список программ в категории.

При нажатии на кнопку › список программ в категории сворачивается в одну строку.

Раздел Интернет

В блоке **Ограничение доступа в интернет** можно настроить ограничения времени доступа в интернет в рабочие и выходные дни.

Ограничивать доступ в рабочие дни до <N> часов в день

Флажок включает / выключает ограничение времени использования интернета в рабочие дни.

Если флажок установлен, Родительский контроль ограничивает суммарное время использования интернета для выбранного пользователя. Ограничение времени использования интернета (в часах) указывается в раскрывающемся списке рядом с флажком.

Если флажок снят, Родительский контроль не ограничивает использование интернета по рабочим дням.

Ограничивать доступ в выходные дни до <N> часов в день

Флажок включает / выключает ограничение времени использования интернета в выходные дни.

Если флажок установлен, Родительский контроль ограничивает суммарное время использования интернета для выбранного пользователя. Ограничение времени использования интернета (в часах) указывается в раскрывающемся списке рядом с флажком.

Если флажок снят, Родительский контроль не ограничивает использование интернета по выходным дням.

В блоке **Контроль посещения сайтов** вы можете ограничивать доступ пользователей к сайтам в зависимости от их содержимого.

Включить безопасный поиск

Флажок включает / выключает *режим безопасного поиска*, который применяется во время работы пользователя с сайтами:

- Bing®.
- Google™.
- Mail.ru.
- Yandex.
- Yahoo! (при поиске информации на английском языке).
- YouTube™ (при поиске информации на английском языке).
- ВКонтакте.

Контролировать доступ к сайтам

Флажок включает / выключает блокирование доступа к сайтам.

Если флажок установлен, Родительский контроль блокирует доступ ко всем сайтам или к сайтам из указанных категорий.

Если флажок снят, Родительский контроль разрешает доступ ко всем сайтам.

Блокировать доступ к сайтам из выбранных категорий

При выборе этого варианта Родительский контроль блокирует доступ к сайтам указанных категорий. Категории сайтов, которые нужно блокировать, можно указать по ссылке **Выбрать категории сайтов**.

Выбрать категории сайтов

По ссылке открывается окно **Блокировать доступ к категориям сайтов**. В окне можно указать категории сайтов, доступ к которым будет заблокирован.

Блокировать доступ ко всем сайтам

При выборе этого варианта Родительский контроль блокирует доступ ко всем сайтам, кроме сайтов, добавленных в список исключений.

По ссылке **Настроить исключения** можно перейти к созданию списка сайтов, к которым применяются индивидуальные настройки доступа.

Настроить исключения

По ссылке открывается окно **Исключения**. В этом окне можно сформировать список сайтов, к которым будут применяться индивидуальные настройки доступа.

В блоке **Запрет загрузки файлов** вы можете указать типы файлов, скачивание которых нужно блокировать.

Программа блокирует скачивание файлов только в том случае, если скачивание выполняется непосредственно браузером, без использования плагинов, предназначенных для скачивания.

Программы

Флажок включает / выключает запрет скачивания программ из интернета.

Если флажок установлен, Родительский контроль запрещает скачивать программы из интернета.

Если флажок снят, скачивание программ разрешено.

Аудио

Если флажок установлен, Родительский контроль запрещает скачивать аудиофайлы из интернета.

Если флажок снят, скачивание аудиофайлов разрешено.

Архивы

Флажок включает / выключает запрет скачивания архивов из интернета.

Если флажок установлен, Родительский контроль запрещает скачивать архивы из интернета.

Если флажок снят, скачивание архивов разрешено.

Видео

Флажок включает / выключает запрет скачивания видеофайлов из интернета.

Если флажок установлен, Родительский контроль запрещает скачивать видеофайлы из интернета.

Если флажок снят, скачивание видеофайлов разрешено.

Раздел Компьютер

В этом окне вы можете указать, когда доступ пользователя к компьютеру необходимо ограничивать.

Кнопка переключения вида окна  /

При нажатии на кнопку выполняется переключение вида окна.

Кнопка может находится в одном из следующих состояний:

-  Отображаются блоки **Рабочие дни** и **Выходные дни**.

Это состояние выбрано по умолчанию.

-  Отображается блок **Точное время использования**.

В блоке **Рабочие дни** вы можете указать ограничения времени использования компьютера по рабочим дням. Блок отображается, если кнопка переключения вида окна находится в состоянии  .

Блокировать доступ с <ЧЧ:ММ> до <ЧЧ:ММ>

Флажок включает / выключает блокирование компьютера в течение указанного времени сна. Ограничение действует по рабочим дням недели.

Если флажок установлен, Родительский контроль блокирует пользователю доступ к компьютеру в течение времени, указанного в полях рядом с флажком.

По умолчанию флажок снят.

Разрешить доступ не более <N> часов в день

Флажок включает / выключает дневной лимит общего времени использования компьютера по рабочим дням. Общее время использования компьютера в течение рабочего дня указывается в раскрывающемся списке рядом с флажком.

Если флажок установлен, Родительский контроль блокирует пользователю доступ к компьютеру после истечения времени, указанного в раскрывающемся списке рядом с флажком.

Если флажок снят, время использования компьютера в течение рабочего дня не ограничено.

По умолчанию флажок снят.

В блоке **Выходные дни** вы можете указать ограничения времени использования компьютера по выходным дням. Блок отображается, если кнопка переключения вида окна находится в состоянии  .

Блокировать доступ с <ЧЧ:ММ> до <ЧЧ:ММ>

Флажок включает / выключает блокирование компьютера в течение указанного времени сна. Ограничение действует по выходным дням.

Если флажок установлен, Родительский контроль блокирует пользователю доступ к компьютеру в течение времени, указанного в полях ввода рядом с флажком.

По умолчанию флажок снят.

Разрешить доступ не более <N> часов в день

Флажок включает / выключает дневной лимит общего времени использования компьютера по выходным дням. Время использования компьютера в течение выходного дня указывается в раскрывающемся списке рядом с флажком.

Если флажок установлен, Родительский контроль блокирует пользователю доступ к компьютеру после истечения времени, указанного в раскрывающемся списке рядом с флажком.

Если флажок снят, время использования компьютера в течение выходного дня не ограничено.

По умолчанию флажок снят.

В блоке **Точное время использования** отображается таблица времени использования компьютера. С помощью таблицы вы можете составить почасовое расписание использования компьютера пользователем в течение недели. Блок отображается, если кнопка переключения вида окна находится в состоянии  .

Таблица времени использования компьютера

С помощью таблицы можно указать дни недели и часы, когда пользователю разрешено пользоваться компьютером. Строки таблицы соответствуют дням недели, графы – интервалам в один час на временной шкале. В зависимости от установленных в операционной системе региональных настроек временная шкала может иметь 24- и 12-часовое представление. Цвета ячеек таблицы отражают установленные ограничения: красный цвет означает, что использование компьютера запрещено, зеленый – использование компьютера разрешено. При нажатии на ячейку таблицы цвет ячейки изменяется. При наведении на ячейку курсора мыши под таблицей отображается временной интервал, которому соответствует ячейка.

В блоке **Перерывы в работе** вы можете настроить периодическое блокирование компьютера в течение суток.

Делать перерыв каждые <N> часов в течение <N минут>

Флажок включает / выключает периодическое блокирование компьютера с указанной длительностью, чтобы обеспечить отдых пользователя.

Если флажок установлен, Родительский контроль блокирует доступ к компьютеру с периодичностью, указанной в раскрывающемся списке <ЧЧ:ММ>. Доступ блокируется на промежуток времени, указанный в раскрывающемся списке <N минут>.

По умолчанию флажок снят.

Раздел Контроль содержимого

В блоке **Контроль передачи персональных данных** можно настроить ограничения пересылки пользователем персональных данных через социальные сети и сайты.

Запретить передачу персональных данных третьим лицам

Флажок включает / выключает блокирование пересылки персональных данных через социальные сети и сайты.

Если флажок установлен, Родительский контроль блокирует пересылку персональных данных. Типы персональных данных, пересылку которых необходимо контролировать, можно сформировать в окне **Список персональных данных**. Окно открывается по ссылке **Изменить список персональных данных**.

Если список персональных данных, которые необходимо контролировать, пуст, Родительский контроль не отслеживает их пересылку.

Если флажок снят, Родительский контроль разрешает пересылку персональных данных и не сохраняет сведения о пересылке в отчет.

Изменить список персональных данных

По ссылке открывается окно **Список персональных данных**. В этом окне можно сформировать список персональных данных, которые будет отслеживать Родительский контроль.

Раздел Программы

В блоке **Блокировать игры по содержимому** можно настроить контроль запускаемых игр по возрастным ограничениям и по содержимому.

Ограничить запуск игр для возраста младше

Флажок включает / выключает блокирование запуска игр с рейтингом выше указанного. Максимальный разрешенный рейтинг игр можно указать в раскрывающемся списке рядом с флажком.

Рейтинги игр в списке соответствуют рейтинговой системе PEGI или ESRB, в зависимости от вашего местоположения.

Если флажок установлен, Родительский контроль блокирует запуск игр с рейтингом выше указанного в раскрывающемся списке. По умолчанию выбран рейтинг, соответствующий возрасту пользователя.

Если флажок снят, Родительский контроль разрешает запуск игр, если они относятся к разрешенным категориям.

Блокировать игры из категорий для взрослых

Флажок включает / выключает ограничение запуска игр по содержимому.

Если флажок установлен, Родительский контроль разрешает запуск игры, если ее содержимое не относится ни к одной из запрещенных категорий. По ссылке **Выбрать категории игр** можно указать запрещенные и разрешенные категории содержимого игр.

Если флажок снят, Родительский контроль разрешает запуск игры (при соответствии игры установленным возрастным ограничениям).

Выбрать категории игр

По ссылке открывается окно **Блокировать игры по категориям**. В этом окне можно разрешить или запретить запуск игр, которые относятся к определенной категории.

Для блокирования игр использовать рейтинговую систему

В раскрывающемся списке можно выбрать тип рейтингов и категоризации содержимого игр (PEGI или ESRB), который будет использоваться при настройке разрешений запуска программ в Родительском контроле:

- **Определять автоматически**. При выборе этого варианта Kaspersky Anti-Virus выбирает тип рейтингов игр в зависимости от вашего местоположения: европейскую рейтинговую систему (PEGI) или ESRB (для США и Канады).
- **PEGI**. При настройке разрешений запуска игр используется европейская рейтинговая система (PEGI).
- **ESRB**. При настройке разрешений запуска игр используется тип рейтингов и категоризации ESRB.

Настроить

По ссылке открывается окно, в котором вы можете настроить ограничения в использовании программ.

Блокировать игры по категориям

В этом окне можно разрешить или запретить запуск игр в зависимости от их содержимого. Тип категоризации содержимого игр (набор флажков) соответствует рейтингам PEGI или ESRB. Тип категоризации игр выбирается автоматически в зависимости от вашего местоположения. При необходимости можно установить тип категоризации игр вручную в настройках компонента Родительский контроль.

Если флажок напротив категории установлен, Родительский контроль блокирует запуск игр, относящихся к этой категории.

Если флажок напротив категории снят, Родительский контроль разрешает запуск игр, относящихся к этой категории.

Запуск игры разрешен, если ее содержимое относится к категориям, каждая из которых разрешена.

Блокировать доступ к категориям сайтов

В этом окне можно указать категории сайтов, доступ к которым будет блокировать Родительский контроль.

Если флажок с наименованием категории установлен, Родительский контроль блокирует доступ к сайту, входящему в эту категорию.

Если флажок с наименованием категории снят, доступ к сайту, входящему в эту категорию, разрешен.

Окно Область действия пароля

Флажок включает / выключает запрос пароля при попытке пользователя открыть окно **Резервное копирование**.

Настройка программы

Флажок включает / выключает запрос пароля при попытке пользователя сохранить изменения настроек программы.

Завершение работы программы

Флажок включает / выключает запрос пароля при попытке пользователя завершить работу программы.

Удаление программы

Флажок включает / выключает запрос пароля при попытке пользователя удалить программу.

Создать пароль

Кнопка, при нажатии на которую доступ к указанным функциям программы ограничивается паролем.

Общая статистика

В верхней части окна отображается имя учетной записи пользователя, отчет о действиях которого приводится в этом окне.

Контроль включен / выключен  / 

Переключатель позволяет включать / выключать контроль действий пользователя с помощью Родительского контроля.

В зависимости от того контролирует ли действия пользователя Родительский контроль, переключатель имеет следующий вид:

 – Родительский контроль контролирует действия пользователя.

 – Родительский контроль не контролирует действия пользователя.

Контроль действий пользователя выполняется в соответствии с заданными для него настройками Родительского контроля.

Профиль: <настройки профиля>

По ссылке можно изменить настройки Родительского контроля, которые требуется применить к текущей учетной записи.

В блоке **Компьютер** можно просмотреть информацию о времени использования компьютера выбранным пользователем, а также перейти к просмотру отчета об использовании компьютера и настройке Родительского контроля. Статистика использования компьютера отображается за период времени, указанный в отчете о времени работы за компьютером. По умолчанию отображается статистика за текущие сутки.

Подробнее

По ссылке открывается окно **Отчет об использовании компьютера**. В окне можно получить информацию об использовании компьютера выбранным пользователем.

Настройка

По ссылке открывается окно. В этом окне вы можете указать время, в течение которого выбранному пользователю можно находиться за компьютером.

В блоке **Программы** отображается информация о программах, которые выбранный пользователь использовал в последнее время. Статистика использования программ отображается за период времени, указанный в отчете о запускаемых программах. По умолчанию отображается статистика за текущие сутки.

Подробнее

По ссылке открывается окно **Отчет о запускавшихся программах**. В окне вы можете получить информацию о программах, которые запускал выбранный пользователь, и времени их использования.

Настройка

По ссылке открывается окно. В этом окне вы можете указать программы, с которыми выбранный пользователь может работать.

Блок **Интернет** содержит статистику посещений сайтов и отчет о времени, которое провел пользователь на этих сайтах. Также вы можете посмотреть общее количество заблокированных попыток посещения запрещенных сайтов.

Статистика посещения веб-ресурсов отображается за период времени, указанный в отчете о времени работы в интернете. По умолчанию отображается статистика за текущие сутки.

Подробнее

По ссылке открывается окно **Отчет об использовании интернета**. В окне можно получить информацию о веб-ресурсах, которые посещал выбранный пользователь.

Настройка

По ссылке открывается окно. В этом окне вы можете указать время, в течение которого выбранному пользователю можно пользоваться интернетом.

В блоке **Контроль содержимого** отображается информация об количестве заблокированных попыток передачи персональных данных.

Статистика отображается за период времени, указанный в отчете о контроле содержимого. По умолчанию отображается статистика за одну неделю.

Подробнее

По ссылке открывается окно. В окне можно получить информацию о том, какие персональные данные пытался передать выбранный пользователь, общаясь в социальных сетях.

Настройка

По ссылке открывается окно. В этом окне вы можете указать персональные данные, использование которых в переписке выбранного пользователя вы хотите контролировать.

Отчет об использовании интернета

В верхней части окна отображается имя учетной записи пользователя, отчет о действиях которого приводится в этом окне.

Контроль включен / выключен  / 

Переключатель позволяет включать / выключать контроль действий пользователя с помощью Родительского контроля.

В зависимости от того контролирует ли действия пользователя Родительский контроль, переключатель имеет следующий вид:

 – Родительский контроль контролирует действия пользователя.

 – Родительский контроль не контролирует действия пользователя.

Контроль действий пользователя выполняется в соответствии с заданными для него настройками Родительского контроля.

В окне **Отчет об использовании интернета** вы можете получить информацию о сайтах, которые посещал выбранный пользователь за отчетный период.

Сегодня

При нажатии на кнопку отображается отчет о действиях пользователя, совершенных за сегодняшний день.

Кнопки 

При нажатии на кнопки отображаются отчеты за предыдущий и следующий период.

День / Неделя / Месяц

Период, за который формируется отчет. Можно сформировать отчет за следующие периоды: день, неделя, месяц.

Кнопка 

При нажатии на кнопку открывается окно настройки Родительского контроля на разделе **Интернет**. В этом разделе можно ограничить выбранному пользователю время использования интернета и доступ к сайтам и ограничить скачивание файлов.

Самые посещаемые сайты

Отчет показывает список сайтов, которые пользователь часто посещал в течение отчетного периода, и количество посещений.

Потрачено

Общее время, проведенное выбранным пользователем в интернете за отчетный период.

Заблокировано веб-ресурсов

Перечень сайтов, открытие которых было запрещено Родительским контролем, а также перечень файлов, скачивание которых было заблокировано.

Показать все

По ссылке открывается окно с информацией о количестве заблокированных загрузок файлов и переходов на сайты.

Категории сайтов

Содержит перечень категорий сайтов. Для каждой категории сайтов указано количество посещений, заблокированных или разрешенных Родительским контролем:

- красным цветом отображается количество переходов на сайты, заблокированных Родительским контролем;
- серым цветом отображается количество переходов на сайты, разрешенных Родительским контролем.

Отчет об использовании компьютера

В верхней части окна отображается имя учетной записи пользователя, отчет о действиях которого приводится в этом окне.

Контроль включен / выключен  / 

Переключатель позволяет включать / выключать контроль действий пользователя с помощью Родительского контроля.

В зависимости от того контролирует ли действия пользователя Родительский контроль, переключатель имеет следующий вид:

 – Родительский контроль контролирует действия пользователя.

 – Родительский контроль не контролирует действия пользователя.

Контроль действий пользователя выполняется в соответствии с заданными для него настройками Родительского контроля.

В окне **Отчет об использовании компьютера** вы можете получить информацию о времени использования компьютера за отчетный период для выбранной учетной записи.

Сегодня

При нажатии на кнопку отображается отчет о действиях пользователя, совершенных за сегодняшний день.

Кнопки 

При нажатии на кнопки отображаются отчеты за предыдущий и следующий период.

День / Неделя / Месяц

Период, за который формируется отчет. Можно сформировать отчет за следующие периоды: день, неделя, месяц.

Кнопка 

При нажатии на кнопку открывается окно настройки Родительского контроля на разделе **Компьютер**. В этом разделе можно указать ограничения использования компьютера по времени.

Отчет об использовании компьютера

Содержит информацию о периодах и длительности использования компьютера за отчетный период.

Розовым цветом отображаются промежутки времени, в которые компьютер использовался выбранной учетной записью.

Зеленым цветом отображается текущий период времени (сутки, неделя или месяц).

Красной линией отображается текущее время сегодняшнего дня (если выбран период *День* или *Неделя*).

Окно Сетевые правила программ

Вид

По ссылке раскрывается меню, с помощью которого можно выбрать способ отображения программ в списке:

- При выборе пункта **Развернуть все** в списке отображаются все программы, установленные на компьютере.
- При выборе пункта **Свернуть все** в списке отображаются группы доверия. Для просмотра входящих в группу программ необходимо развернуть группу, нажав на значок .
- При выборе пункта **Показывать только сетевые программы** в списке отображаются только сетевые программы. Сетевые программы – это программы, предназначенные для организации совместной работы группы пользователей на разных компьютерах.
- При выборе пункта **Скрывать системные программы** в списке не отображаются программы, которые входят в состав операционной системы.
- При выборе пункта **Скрывать Kaspersky Anti-Virus** в списке не отображается Kaspersky Anti-Virus.

Список программ

В списке содержится информация о программах, установленных на вашем компьютере:

- название программы;
- значок с всплывающей подсказкой о том, разрешена ли программе сетевая активность;
- популярность программы среди пользователей Kaspersky Security Network;
- объем сетевого трафика программы.

По правой клавише мыши на строке программы открывается контекстное меню. В контекстном меню можно выбрать следующие действия:

- открыть окно **Правила программы**, в котором можно настроить разрешения для действий программы;
- разрешить или запретить сетевую активность программы;
- переместить программу в другую группу доверия;
- восстановить разрешения действий программы, установленные Kaspersky Anti-Virus;
- удалить программу из списка;
- открыть папку, содержащую исполняемый файл программы.

Окно Добавление / Изменение сетевого правила

Действие

Раскрывающийся список, в котором вы можете выбрать действие Kaspersky Anti-Virus при обнаружении сетевого соединения. Возможные значения:

- **Разрешить**. Kaspersky Anti-Virus разрешает сетевое соединение.
- **Запросить действие**. Kaspersky Anti-Virus запрашивает пользователя о разрешении или запрете сетевого соединения.
- **Запретить**. Kaspersky Anti-Virus запрещает сетевое соединение.

Название

Название сетевого правила. В качестве названия вы можете использовать имя сетевого сервиса.

Сетевой сервис – это набор настроек, характеризующих сетевую активность, для которой вы создаете правило.

Направление

В раскрывающемся списке вы можете выбрать направление сетевой активности, которое требуется контролировать. Список содержит следующие направления сетевой активности:

- **Входящее**. Kaspersky Anti-Virus применяет правило к сетевому соединению, которое открыл удаленный компьютер.
- **Исходящее**. Kaspersky Anti-Virus применяет правило к сетевому соединению, которое открыл ваш компьютер.
- **Входящее/Исходящее**. Kaspersky Anti-Virus применяет правило как к входящему, так и к исходящему пакету или потоку данных, независимо от того, какой компьютер (ваш или удаленный) инициировал сетевое соединение.

Протокол

В списке можно выбрать протокол, для которого создается правило.

При выборе протоколов ICMP и ICMPv6 становятся доступными раскрывающиеся списки **Параметры ICMP** и **Код**, в которых можно указать тип сообщения и код сообщения соответственно.

При выборе протоколов TCP и UDP становятся доступными поля **Удаленные порты** и **Локальные порты**.

Параметры ICMP

В списке можно выбрать тип сообщения, передаваемого по ICMP или ICMPv6.

Код

В списке можно выбрать код сообщения, передаваемого по ICMP или ICMPv6.

Удаленные порты

Номера удаленных портов, перечисленные через запятую.

Локальные порты

Номера контролируемых локальных портов, перечисленные через запятую.

Адрес

Позволяет задать диапазон адресов, к которому Kaspersky Anti-Virus применяет правило. Возможные значения:

- **Любой адрес**. Kaspersky Anti-Virus применяет правило к любому IP-адресу.
- **Адреса подсети**. Kaspersky Anti-Virus применяет правило к IP-адресам всех сетей, подключенных в данный момент и имеющих указанный статус. Для этой настройки ниже доступен выбор статуса сети, для которого Kaspersky Anti-Virus применяет правило (доверенные сети, локальные сети, публичные сети).
- **Адреса из списка**. Kaspersky Anti-Virus применяет правило к IP-адресам, входящим в заданный диапазон. Для этой настройки доступны поля **Удаленные адреса** и **Локальные адреса** (список **Локальные адреса** недоступен при создании сетевого правила).

Удаленные адреса

В поле можно указывать адреса, которые контролирует Kaspersky Anti-Virus. Вы можете задавать, изменять и удалять адреса или маски адресов из списка.

Адрес, заданный в виде доменного имени, Kaspersky Anti-Virus пытается преобразовать в IP-адрес. Если такое преобразование невозможно, на экран выводится соответствующее уведомление.

Список доступен, если в раскрывающемся списке **Адрес** выбран элемент **Адреса из списка**.

Записывать события

Флажок включает / выключает запись информации о попытке соединения и о реакции программы на него в отчет Kaspersky Anti-Virus.

Шаблон сетевого правила

По ссылке раскрывается список, в котором вы можете выбрать шаблон для создания сетевого правила.

Закладка Исключения

Не проверять открываемые файлы

Флажок включает / выключает исключение из проверки всех файлов, которые открываются этой программой.

Если флажок установлен, Kaspersky Anti-Virus исключает из проверки файлы, которые открываются выбранной программой.

Если флажок снят, Kaspersky Anti-Virus проверяет файлы, которые открываются выбранной программой.

Не контролировать активность программы

Флажок включает / выключает исключение из проверки любой активности программы в рамках работы Проактивной защиты.

Если флажок установлен, любая активность программы исключается из проверки компонентами Проактивная защита.

Если флажок снят, Kaspersky Anti-Virus будет проверять любую активность программы.

Не наследовать ограничения родительского процесса (программы)

Если флажок установлен, активность программы контролируется по заданным вами правилам или по правилам группы доверия, в которую входит эта программа.

Если флажок снят, программа наследует правила от родительской программы, которая ее запустила.

Не контролировать активность дочерних программ

Флажок включает / выключает исключение из проверки любой активности любой дочерней программы.

Разрешить взаимодействие с интерфейсом Kaspersky Anti-Virus

Если флажок установлен, программе разрешено управлять программой Kaspersky Anti-Virus, используя ее графический интерфейс. Необходимость разрешить программе управлять интерфейсом Kaspersky Anti-Virus может возникнуть при использовании программы для удаленного доступа к рабочему столу или программы, обеспечивающей работу устройства ввода данных. К таким устройствам относятся, например, сенсорные панели (тачпады), графические планшеты.

Не проверять весь трафик / Не проверять зашифрованный трафик

Флажок включает / выключает исключение сетевого трафика программы из проверки на спам, вирусы и другие программы, представляющие угрозу.

Если выбран пункт **Не проверять весь трафик**, Kaspersky Anti-Virus не проверяет весь трафик программы.

Если выбран пункт **Не проверять зашифрованный трафик**, Kaspersky Anti-Virus не проверяет зашифрованный трафик программы.

Только для указанных IP-адресов

Флажок включает / выключает функцию исключения из проверки сетевого трафика программы для указанных IP-адресов.

IP-адреса, которые нужно исключать из проверки, можно указать в поле ввода, расположенном под флажком.

Если флажок установлен, Kaspersky Anti-Virus исключает из проверки сетевой трафик только для указанных IP-адресов.

Если флажок снят, Kaspersky Anti-Virus исключает из проверки все IP-адреса.

Только для указанных портов

Флажок включает / выключает функцию исключения из проверки сетевого трафика только для указанных портов.

Порты, которые нужно исключать из проверки, можно указать в поле ввода, расположенном под флажком.

Если флажок установлен, Kaspersky Anti-Virus исключает из проверки сетевой трафик только для указанных портов.

Если флажок снят, Kaspersky Anti-Virus исключает из проверки все порты.

Закладка История

Группа доверия

В графе отображается группа доверия, в которую Kaspersky Anti-Virus поместил программу. По правилам групп доверия Kaspersky Anti-Virus регулирует активность программ.

Событие

Графа, в которой отображается информация о действиях программы.

Путь

Содержит путь к файлу.

Время

Графа, в которой указаны дата и время события.

Закладка Права

Права

Содержит права доступа программы или группы программ к ресурсам системы.

В графе **Действие** отображается реакция Kaspersky Anti-Virus на действия программы над контролируемыми ресурсами. С помощью контекстного меню ячейки вы можете изменить реакцию Kaspersky Anti-Virus на действия программы

В таблице ниже описаны реакции Kaspersky Anti-Virus на действия программы.

Описание действий Kaspersky Anti-Virus

Реакция	Описание
Наследовать	Программа или группа наследует реакцию из вышестоящей группы.
Разрешить	Kaspersky Anti-Virus разрешает программам в выбранном статусе действие над ресурсом.
Запретить	Kaspersky Anti-Virus запрещает программам в выбранном статусе действие над ресурсом.
Запросить действие	Kaspersky Anti-Virus запрашивает пользователя о предоставлении программе или группе доступа к ресурсу.
Записывать в отчет	Помимо заданной реакции, Kaspersky Anti-Virus записывает в отчет информацию о попытке доступа программы к ресурсу.

Закладка Файл

Путь

Путь к исполняемому файлу программы.

Производитель

Производитель программы.

Программа

Название программы.

Версия

Номер установленной версии.

Размер

Размер исполняемого файла.

Создан

Дата и время создания файла.

Изменен

Дата и время изменения файла.

Группа доверия

Группа доверия, в которую Kaspersky Anti-Virus помещает программу.

Причина помещения в группу

Причина, по которой программа помещена в указанную группу доверия.

Цифровая подпись

Наличие цифровой подписи и ее владелец.

Статус сертификата

Информация о сертификате, с помощью которого подписана программа.

Дата подписи

Дата создания цифровой подписи.

Число пользователей

Количество пользователей, которые используют программу (на основе данных Kaspersky Security Network).

Впервые появилась

Дата появления этой программы у первого из участников Kaspersky Security Network.

Распространение

Список стран, в которых проживает наибольшее число пользователей программы.

Рядом с названием каждой страны Kaspersky Anti-Virus отображает, какой процент среди всех участников Kaspersky Security Network приходится на пользователей из этой страны.

Закладка Файлы и системный реестр

Файлы и системный реестр

Содержит правила доступа программы или группы программ к ресурсам, объединенным в категорию **Файлы и системный реестр**.

В графе **Ресурс** файлы объединены в категории **Операционная система** и **Персональные данные**.

В графах **Чтение**, **Запись**, **Удаление**, **Создание** отображается реакция Kaspersky Anti-Virus на действия программы над контролируемыми ресурсами. С помощью контекстного меню ячейки вы можете изменить реакцию Kaspersky Anti-Virus.

В таблице ниже приведено описание действий Kaspersky Anti-Virus над контролируемыми ресурсами.

Описание действий Kaspersky Anti-Virus

Действие	Описание
Наследовать	Программа или группа наследует реакцию из вышестоящей группы.
Разрешить	Kaspersky Anti-Virus разрешает программам, входящим в выбранную группу, действие над ресурсом.
Запретить	Kaspersky Anti-Virus запрещает программам, входящим в выбранную группу, действие над ресурсом.
Запросить действие	Kaspersky Anti-Virus запрашивает пользователя о предоставлении программе или группе доступа к ресурсу.
Записывать в отчет	Помимо заданной реакции, Kaspersky Anti-Virus записывает в отчет информацию о попытке доступа программы к ресурсу.

Окно Удаленные порты

Удаленные порты

Номера портов, перечисленные через запятую (например `25,80,110`). Kaspersky Anti-Virus исключает их при проверке сетевого трафика программы.

Закладка Сетевые правила

Сетевые правила

Содержит правила, в соответствии с которыми Kaspersky Anti-Virus регулирует сетевую активность программ.

Название

Графа, в которой указано название сетевого правила.

Сетевой сервис – это набор настроек, характеризующих сетевую активность, для которой вы создаете правило.

При формировании условий правил вы можете указывать сетевой сервис и сетевой адрес. В качестве сетевого адреса можно использовать IP-адрес или указывать статус сети. В последнем случае адреса берутся из всех сетей, подключенных в данный момент и имеющих указанный статус.

Адрес

В графе отображается статус сетей, для которых применяется данное правило.

Действие

Графа, в которой отображается реакция Kaspersky Anti-Virus на сетевую активность программы. С помощью контекстного меню ячейки в этой графе вы можете изменить реакцию Kaspersky Anti-Virus. В таблице ниже описаны действия Kaspersky Anti-Virus при возникновении сетевой активности программы.

Описания действий Kaspersky Anti-Virus

Пункт	Значение
Наследовать	Программа или группа наследует реакцию из вышестоящей группы.
Разрешить	Kaspersky Anti-Virus разрешает программам выбранной группы действие над ресурсом.
Запретить	Kaspersky Anti-Virus запрещает программам выбранной группы действие над ресурсом.
Запросить действие	Kaspersky Anti-Virus запрашивает пользователя о предоставлении программе или группе доступа к ресурсу.
Записывать в отчет	Помимо заданной реакции, Kaspersky Anti-Virus записывает в отчет информацию о попытке доступа программы к ресурсу.

Добавить

При нажатии на кнопку открывается окно **Добавление сетевого правила**. В окне можно создать новое сетевое правило.

Изменить

При нажатии на эту кнопку открывается окно **Изменение сетевого правила**. В этом окне можно изменить сетевое правило, выбранное в списке.

Удалить

При нажатии на эту кнопку Kaspersky Anti-Virus удаляет выбранное правило из списка.

Вверх

При нажатии на эту кнопку правило перемещается на строку выше, тем самым получая более высокий приоритет выполнения.

Вниз

При нажатии на эту кнопку правило перемещается на строку ниже, тем самым получая более низкий приоритет выполнения.

В блоке **Описание правила**, расположенном в нижней части окна, вы можете посмотреть свойства выбранного правила.

Окно Управление программами

Запуск / Ограничения

По ссылкам изменяется способ отображения программ в списке:

- По ссылке **Запуск** список программ в списке распределяются по двум группам: **Запретить запуск** и **Разрешить запуск**.
- По ссылке **Ограничения** программы в списке распределяются по группам доверия. Например, доверенные программы будут располагаться в группе **Доверенные**.

Очистка

По ссылке Kaspersky Anti-Virus удаляет из списка несуществующие программы.

Вид

В раскрывающемся списке можно выбрать вид отображения программ и процессов.

- **Развернуть все**. При выборе этого варианта в списке отображаются все программы, установленные на компьютере.
- **Свернуть все**. При выборе этого варианта в списке отображаются группы доверия.

В раскрывающемся списке можно выбрать способ отображения программ и процессов:

- **Показывать как список**. При выборе этого варианта программы / процессы отображаются в виде списка.
- **Показывать как дерево**. При выборе этого варианта программы / процессы отображаются в виде иерархической структуры в соответствии с последовательностью вызова процессов.

В раскрывающемся списке также можно выключить отображение системных программ, программ "Лаборатории Касперского" и несетевых программ:

- **Скрывать системные программы**. При выборе этого элемента в общем списке программ и процессов не отображаются программы, необходимые для работы операционной системы. По умолчанию системные программы скрыты.
- **Скрывать Kaspersky Anti-Virus**. При выборе этого элемента в общем списке программ и процессов не отображаются программы "Лаборатории Касперского". По умолчанию программы "Лаборатории Касперского" скрыты.
- **Показывать только сетевые программы**. При выборе этого элемента в общем списке программ и процессов отображаются только сетевые программы. Сетевые программы – это программы, предназначенные для организации совместной работы группы пользователей на разных компьютерах.

Список программ

В списке содержатся программы, установленные на вашем компьютере. Для каждой программы в списке отображается информация о статусе, цифровой подписи, группе доверия, популярности программы среди пользователей KSN и времени последнего запуска.

По двойному щелчку мышью на строке программы или процесса открывается окно **Правила программы**. В окне можно настроить правила для контроля действий программы.

По правой клавише мыши на строке программы открывается контекстное меню. В контекстном меню можно выполнить следующие действия:

- открыть окно **Правила программы**, в котором можно настроить разрешения для действий программы;
- разрешить или запретить запуск программы;
- переместить программу в другую группу доверия;
- установить для программы настройки контроля активности, предусмотренные по умолчанию (сбросить настройки программы);
- удалить программу из списка;
- открыть папку, содержащую исполняемый файл программы.

Программы в списке объединены в группы и подгруппы. По правой клавише мыши на строке группы открывается контекстное меню. В контекстном меню можно выполнить следующие действия:

- открыть окно **Правила группы**, в котором можно настроить разрешения для действий программ из этой группы, используемые по умолчанию;
- создать подгруппу внутри группы; по умолчанию к подгруппе применяются правила, указанные для группы, в которую она входит;
- добавить программу в группу; по умолчанию к программе применяются правила, указанные для группы, в которую она входит;
- установить для группы и всех входящих в нее подгрупп и программ настройки контроля активности, предусмотренные по умолчанию (сбросить настройки группы);
- установить для подгрупп и программ, входящих в группу, настройки контроля активности, предусмотренные по умолчанию, оставив настройки группы без изменений (сбросить настройки подгрупп и программ);
- удалить входящие в группу подгруппы и программы.

Программа

В графе отображается название программы.

Ограничения

В графе отображается группа доверия, в которую помещена программа. Группа доверия определяет правила использования программы на компьютере: запрет или разрешение запуска, доступ программы к файлам и системному реестру, ограничения сетевой активности программы.

Популярность

В графе отображается уровень популярности программы среди участников Kaspersky Security Network (KSN). Уровень популярности соответствует числу участников KSN, использующих программу.

Сеть

В этой графе можно выбрать действие при попытке программы получить доступ к сети.

В таблице ниже приведено описание действий Kaspersky Anti-Virus, если программа или группа программ пытается получить доступ к сети.

Описание действий Kaspersky Anti-Virus

Действие	Описание
Наследовать	Программа или группа наследует реакцию из вышестоящей группы.
Разрешить	Kaspersky Anti-Virus разрешает программам, входящим в выбранную группу, доступ к сети.
Запретить	Kaspersky Anti-Virus запрещает программам, входящим в выбранную группу, доступ к сети.
Запросить действие	Kaspersky Anti-Virus запрашивает пользователя о предоставлении программе или группе доступа к сети.
Записывать в отчет	Помимо заданной реакции, Kaspersky Anti-Virus записывает в отчет информацию о попытке доступа программы к сети.

Запуск

В графе с помощью переключателя можно разрешить или запретить запуск выбранной программы. По умолчанию запуск программы разрешен или запрещен в зависимости от ограничений группы, в которую входит программа.

Поиск следов активности / Поиск изменений

В этом окне отображается процесс поиска следов активности на вашем компьютере или анализ изменений, выполненных мастером устранения следов активности ранее.

Процесс может занять некоторое время. Процесс можно прервать, нажав на кнопку **Отмена**.

Завершение работы

Перезагрузить компьютер

Если флажок установлен, компьютер перезагружается после завершения работы мастера.

Готово

Кнопка, при нажатии на которую мастер устранения следов активности завершает работу.

Начало работы мастера

Выполнить поиск следов активности пользователя

Kaspersky Anti-Virus запускает поиск следов вашей активности на компьютере.

Отменить внесенные ранее изменения

Kaspersky Anti-Virus отменяет изменения, которые были сделаны в результате предыдущей работы мастера устранения следов активности.

Этот вариант действия доступен, если в результате предыдущей работы мастера следы активности были устранены.

Поиск следов активности завершен / Поиск изменений завершен

Список действий

Список содержит три группы действий для устранения следов вашей активности в операционной системе:

- *Настоятельно рекомендуемые действия* помогут избавиться от следов активности, представляющих серьезную проблему.
- *Рекомендуемые действия* направлены на устранение следов активности, которые представляют потенциальную опасность.
- *Дополнительные действия* предназначены для устранения неопасных следов активности.

Если флажок в строке действия установлен, Kaspersky Anti-Virus выполнит это действие.

Если флажок в строке действия снят, Kaspersky Anti-Virus не выполнит это действие.

Если на первом шаге был выбран вариант **Отменить внесенные ранее изменения**, в списке содержатся выполненные ранее действия, которые вы можете отменить.

Устранение следов активности / Отмена изменений

В этом окне отображается процесс устранения следов вашей активности в операционной системе. Устранение может занять некоторое время. Для устранения некоторых следов активности может потребоваться перезагрузка компьютера.

Если на первом шаге был выбран вариант **Отменить внесенные ранее изменения**, мастер устранения следов активности выполняет откат действий, выбранных на предыдущем шаге.

Центр уведомлений

В разделе **Лицензирование** отображаются уведомления о лицензии и о проблемах, связанных с лицензией.

Подробнее

При нажатии на кнопку открывается окно **Лицензирование** с подробной информацией о лицензии.

В разделе **Защита** отображаются уведомления о состоянии защиты вашего компьютера, о выключенных компонентах защиты, об обнаруженных объектах и о проблемах с обновлениями баз и программных модулей.

Подробнее

При нажатии на кнопку открывается окно с детальной информацией о проблеме.

Устранить

При нажатии на кнопку Kaspersky Anti-Virus запускает обработку обнаруженного объекта.

Кнопка отображается при наличии обнаруженного объекта.

При нажатии на кнопку раскрывается меню, в котором можно выбрать дополнительное действие:

- **Добавить в исключения** – создать исключение, в соответствии с которым объект не должен считаться вредоносным.
- **Игнорировать** – перенести уведомление в раздел **Игнорируемые уведомления**.
- **Перейти к файлу** – открыть папку исходного размещения файла.
- **Посмотреть отчет** – открыть окно **Подробные отчеты** с детальной информацией об обнаруженных объектах и действиях программы в отношении этих объектов.
- **Узнать больше** – открыть веб-страницу с описанием обнаруженного объекта.

Устранить все

При нажатии на кнопку Kaspersky Anti-Virus запускает обработку всех обнаруженных объектов.

Кнопка отображается, если обнаружено более 10 объектов.

При нажатии на кнопку раскрывается меню, в котором можно выбрать дополнительное действие:

- **Игнорировать все** – перенести все уведомления этой группы в раздел **Игнорируемые уведомления**.
- **Показать все** – открыть окно со списком всех обнаруженных объектов.

Обновить

При нажатии на кнопку Kaspersky Anti-Virus запускает обновление баз и программных модулей.

При нажатии на кнопку раскрывается меню, в котором можно выбрать дополнительные действия:

- **Настроить обновление** – открыть окно настройки программы на разделе **Настройки обновления**. В этом разделе можно настроить режим скачивания и установки пакетов обновлений, а также выбрать источник обновлений.
- **Посмотреть отчет** – открыть отчет об обновлениях баз и программных модулей.

Остановить

При нажатии на кнопку Kaspersky Anti-Virus прекращает обновление баз и программных модулей. Это действие доступно, если выполняется обновление баз и программных модулей.

Включить

При нажатии на кнопку программа запускает компонент Kaspersky Anti-Virus, который ранее был приостановлен.

Разблокировать

При нажатии на кнопку выключается блокирование сетевого трафика.

Возобновить

При нажатии на кнопку Kaspersky Anti-Virus возобновляет защиту вашего компьютера.

Кнопка отображается, если защита компьютера приостановлена.

Перезапустить

При нажатии на кнопку программа перезапускается. Это может понадобиться, например, для завершения обновления баз и программных модулей.

Перезагрузить

При нажатии на кнопку запускается процесс перезагрузки компьютера. Это может понадобиться, например, для окончания лечения обнаруженного объекта.

В разделе **Рекомендации** отображаются уведомления о действиях, которые рекомендуется выполнить для оптимизации работы программы и более эффективного ее использования.

Включить

При нажатии на кнопку становится возможным автоматическое обновление баз и программных модулей.

При нажатии на кнопку раскрывается меню, в котором можно выбрать действие **Настроить обновление**. При выборе этого действия открывается окно настройки программы на разделе **Настройки обновления**. В этом разделе можно настроить режим скачивания и установки пакета обновлений, а также выбрать источник обновлений.

Включить KSN

При нажатии на кнопку открывается окно **Настройки дополнительных средств защиты**. В этом окне можно включить использование Kaspersky Security Network.

Обновить версию

При нажатии на кнопку Kaspersky Anti-Virus запускает обновление программы до новой версии.

Перезагрузить

При нажатии на кнопку запускается процесс перезагрузки компьютера. Это может понадобиться, если необходимо завершить обновление версии программы.

Установить

При нажатии на кнопку Kaspersky Anti-Virus устанавливает расширение Kaspersky Protection в браузер Internet Explorer.

Кнопка отображается, если при работе в операционной системе Windows 10 в браузере Internet Explorer не установлено расширение Kaspersky Protection.

В разделе **Новости** отображаются уведомления о новостях от "Лаборатории Касперского".

Прочитать

При нажатии на кнопку открывается окно со списком новостей от "Лаборатории Касперского".

В разделе **Игнорируемые уведомления** отображаются уведомления, к которым было применено действие **Игнорировать**. Уведомления в этом разделе не влияют на цвет индикатора защиты в главном окне программы.

Включить

При нажатии на кнопку программа запускает компонент Kaspersky Anti-Virus, который ранее был приостановлен.

Не игнорировать

При нажатии на кнопку уведомление из раздела **Игнорируемые уведомления** переносится в раздел **Защита**.

Выберите zip-файл или папку

Применение альтернативных тем оформления доступно не во всех регионах.

При выборе темы оформления учитывайте следующие ограничения:

- Kaspersky Anti-Virus не сможет использовать выбранную тему оформления в следующих случаях:
  - Если внутри архива файлы отличаются наименованием или имеют иное расположение в структуре папок, чем в стандартной теме.
  - Если внутри архива повреждены файлы, отвечающие за тексты на окнах программы.
- Темы оформления предназначены для определенной версии Kaspersky Anti-Virus и не применимы к другим версиям и другим программам. При обновлении программы до новой версии или установки поверх нее другой программы тема оформления меняется на стандартную.

Если в результате выбора альтернативной темы оформления вы столкнулись с проблемами и не можете установить стандартную тему оформления предусмотренным для этого способом (например, не можете снять флажок **Использовать альтернативную тему оформления** в окне **Настройки отображения Kaspersky Anti-Virus** из-за того, что шрифт сливается с фоном и нужные элементы управления неразличимы), рекомендуется переустановить Kaspersky Anti-Virus.

Более подробную информацию вы можете найти в статье о применении альтернативных тем оформления.