kaspersky

Kaspersky Endpoint Security

Подготовительные процедуры и руководство по эксплуатации

Версия программы: 11.6.0.394

kaspersky

Уважаемый пользователь!

Спасибо, что доверяете нам. Мы надеемся, что этот документ поможет вам в работе и ответит на большинство возникающих вопросов.

Дата редакции документа: 29.01.2021

Обозначение документа: 643.46856491.00100-04 90 01

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

О "Лаборатории Касперского": https://www.kaspersky.ru/about/company

kaspersky

Оглавление

kaspersky

Об этом документе

Настоящий документ представляет собой подготовительные процедуры и руководство по эксплуатации программного обеспечения "Kaspersky Endpoint Security для Windows" (далее также "Kaspersky Endpoint Security", "программа").

Подготовительные процедуры изложены в разделах "Подготовка к установке программы", "Установка программы", "Подготовка программы к работе" и "Процедура приемки" и содержат процедуры безопасной установки и первоначальной настройки программы, которые необходимы для получения безопасной (сертифицированной) конфигурации. В разделе "Требования" приведены минимально необходимые системные требования для безопасной установки программы.

Остальные разделы этого документа представляют собой руководство по эксплуатации. Руководство по эксплуатации содержит сведения о том, как осуществлять безопасное администрирование программы, а также инструкции и указания по безопасному использованию программы.

В документе также содержатся разделы с дополнительной информацией о программе.

Документ адресован техническим специалистам, в обязанности которых входит установка, эксплуатация и администрирование Kaspersky Endpoint Security, а также поддержка организаций, использующих Kaspersky Endpoint Security.

kaspersky

Источники информации о программе

Указанные источники информации о программе (в частности, электронная справка) созданы для удобства пользователя и не являются полноценным эквивалентом этого документа.

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

- страница Kaspersky Endpoint Security на веб-сайте "Лаборатории Касперского";
- страница Kaspersky Endpoint Security в Базе знаний;
- электронная справка.

Страница Kaspersky Endpoint Security на веб-сайте "Лаборатории Касперского"

На странице Kaspersky Endpoint Security (http://www.kaspersky.ru/business-security/endpoint-windows) вы можете получить общую информацию о программе, ее возможностях и особенностях работы.

Страница Kaspersky Endpoint Security в Базе знаний

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

На странице Kaspersky Endpoint Security в Базе знаний (https://support.kaspersky.ru/kes11) 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 Endpoint Security, но и к другим программам "Лаборатории Касперского". Статьи Базы знаний также могут содержать новости Службы технической поддержки.

Электронная справка

Электронная справка входит в состав программы Kaspersky Endpoint Security. Вы можете открыть справку по кнопке  или по клавише **F1**. В электронной справке вы можете найти описание параметров Kaspersky Endpoint Security.

kaspersky

О программе

Программное изделие "Kaspersky Endpoint Security для Windows" представляет собой САВЗ типов "Б", "В", "Г" второго класса защиты, с функциями аутентификации администратора безопасности и ограничения программной среды.

Объект оценки представляет собой программное средство, реализующее функции обнаружения компьютерных программ либо иной компьютерной информации, предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирования на обнаружение этих программ и информации, предназначенное для применения на серверах или АРМ информационных систем, а также на автономных АРМ.

Основными угрозами, для противостояния которым используется Kaspersky Endpoint Security, являются:

- угрозы, связанные с внедрением в информационные системы из информационно-телекоммуникационных сетей, в том числе сетей международного информационного обмена (сетей связи общего пользования) и / или съемных машинных носителей информации, вредоносных компьютерных программ (вирусов) (КВ);
- угрозы, связанные с установкой на узлы информационной системы внутренними и внешними нарушителями незарегистрированного (неучтенного) потенциально вредоносного программного обеспечения.

В программе реализованы следующие функции безопасности:

- разграничение доступа к управлению ОО;
- управление работой ОО;
- управление параметрами ОО;
- управление установкой обновлений (актуализации) БД ПКВ ОО;
- аудит безопасности ОО;
- выполнение проверок объектов воздействия;
- обработка объектов воздействия;
- сигнализация ОО;
- идентификация и аутентификация администратора безопасности;
- ограничение программной среды (управление запуском компонентов ПО, контроль доступа к веб-ресурсам).

kaspersky

Требования

Этот раздел содержит аппаратные и программные требования для установки и работы программы, а также указания по эксплуатации и требования к среде.

В этом разделе

Аппаратные и программные требования

Для функционирования Kaspersky Endpoint Security компьютер должен удовлетворять следующим требованиям.

Минимальные общие требования:

- 2 ГБ свободного места на жестком диске;
- процессор:
  - рабочая станция – 1 ГГц;
  - сервер – 1.4 ГГц;
  - поддержка инструкций SSE2.
- оперативная память:
  - рабочая станция (x86) – 1 ГБ;
  - рабочая станция (x64) – 2 ГБ;
  - сервер – 2 ГБ.
- Microsoft .NET Framework 4.0 или выше.

Поддерживаемые операционные системы для рабочих станций:

- Windows 7 Home / Professional / Ultimate / Enterprise Service Pack 1 и выше;
- Windows 8 Professional / Enterprise;
- Windows 8.1 Professional / Enterprise;
- Windows 10 Home / Pro / Education / Enterprise.

Алгоритм подписи модулей SHA-1 больше не поддерживается Microsoft. Для успешной установки Kaspersky Endpoint Security на компьютер под управлением операционной системы Microsoft Windows 7 необходимо установить на компьютер обновление KB4474419. Подробнее об этом обновлении см. на сайте Службы технической поддержки Microsoft https://support.microsoft.com/ru-ru/help/4474419/sha-2-code-signing-support-update.
Особенности поддержки операционной системы Microsoft Windows 10 вы можете узнать в базе знаний Службы технической поддержки https://support.kaspersky.ru/kes11/13036.

Поддерживаемые операционные системы для серверов:

- Windows Small Business Server 2011 Essentials / Standard (64-разрядная);

  Microsoft Small Business Server 2011 Standard (64-разрядная) поддерживается только с установленным Service Pack 1 для Microsoft Windows Server 2008 R2.

- Windows MultiPoint Server 2011 (64-разрядная);
- Windows Server 2008 R2 Foundation / Standard / Enterprise / Datacenter Service Pack 1 и выше;
- Windows Server 2012 Foundation / Essentials / Standard / Datacenter;
- Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter;
- Windows Server 2016 Essentials / Standard / Datacenter;
- Windows Server 2019 Essentials / Standard / Datacenter.

Алгоритм подписи модулей SHA-1 больше не поддерживается Microsoft. Для успешной установки Kaspersky Endpoint Security на компьютер под управлением операционной системы Microsoft Windows Server 2008 R2 необходимо установить на компьютер обновление KB4474419. Подробнее об этом обновлении см. на сайте Службы технической поддержки Microsoft https://support.microsoft.com/ru-ru/help/4474419/sha-2-code-signing-support-update.
Особенности поддержки операционной системы Microsoft Windows Server 2016 и Microsoft Windows Server 2019 вы можете узнать в базе знаний Службы технической поддержки https://support.kaspersky.ru/kes11/13036.

Указания по эксплуатации и требования к среде

1. Установка, конфигурирование и управление программой должны осуществляться в соответствии с эксплуатационной документацией.
2. Программа должна эксплуатироваться на компьютерах, отвечающих минимальным требованиям, приведенным в разделе "Аппаратные и программные требования".
3. Перед установкой и началом эксплуатации программы необходимо установить все доступные обновления для используемых версий ПО среды функционирования.
4. Должен быть обеспечен доступ программы ко всем объектам информационной системы, которые необходимы программе для реализации своих функциональных возможностей (к контролируемым объектам информационной системы).
5. Должна быть обеспечена совместимость программы с контролируемыми ресурсами информационной системы.
6. Должна быть обеспечена возможность корректной совместной работы программы со средствами антивирусной защиты других производителей в случае их совместного использования в информационной системе.
7. Должна быть обеспечена физическая защита элементов информационной системы, на которых установлена программа.
8. Должна быть обеспечена синхронизация по времени между компонентами программы, а также между программой и средой ее функционирования.

9. Персонал, ответственный за функционирование программы, должен обеспечивать надлежащее функционирование программы, руководствуясь эксплуатационной документацией.
10. Должна быть обеспечена доверенная связь между программой и уполномоченными субъектами информационной системы (администраторами безопасности).
11. Функционирование программы должно осуществляться в среде функционирования, предоставляющей механизмы аутентификации и идентификации администраторов безопасности программы.
12. Должен быть обеспечен доверенный канал получения обновлений БД ПКВ.
13. Должна быть обеспечена защищенная область для выполнения функций безопасности программы.
14. Управление атрибутами безопасности, связанными с доступом к функциям и данным программы, должно предоставляться только уполномоченным ролям (администраторам программы и информационной системы).
15. Администратор должен установить в среде ИТ максимальное число попыток неуспешных попыток аутентификации с момента последней успешной попытки аутентификации пользователя с последующей блокировкой попыток аутентификации при превышении установленного значения.
16. Администратор должен задать метрику качества паролей, включающую требования к длине паролей, требования по запрещению использования определенных комбинаций символов, а также требования к категории используемых символов.

kaspersky

Установка программы с помощью мастера

Интерфейс мастера установки программы состоит из последовательности окон, соответствующих шагам установки программы.

► *Чтобы установить программу или обновить предыдущую версию программы с помощью мастера установки программы,*

скопируйте файл setup_kes.exe, входящий в комплект поставки, на компьютер пользователя и запустите его.

Запустится мастер установки программы.

Подготовка к установке

Перед установкой Kaspersky Endpoint Security на компьютер или обновлением предыдущей версии программы проверяются следующие условия:

- наличие несовместимого программного обеспечения (список несовместимого ПО приведен в файле incompatible.txt в комплекте поставки);
- выполнение аппаратных и программных требований;
- наличие прав на установку программного обеспечения.

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

Если компьютер соответствует предъявляемым требованиям, мастер установки программы выполняет поиск программ "Лаборатории Касперского", одновременная работа которых может привести к возникновению конфликтов. Если такие программы найдены, вам предлагается удалить их вручную.

Если в числе обнаруженных программ есть предыдущие версии Kaspersky Endpoint Security, то все данные, которые могут быть мигрированы (например, информация об активации, параметры программы), сохраняются и используются при установке Kaspersky Endpoint Security 11.6.0 для Windows, а предыдущая версия программы автоматически удаляется. Это относится к следующим версиям программы:

- Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 4 для Windows (сборка 10.2.6.3733).
- Kaspersky Endpoint Security 10 Service Pack 2 для Windows (сборка 10.3.0.6294).
- Kaspersky Endpoint Security 10 Service Pack 2 Maintenance Release 1 для Windows (сборка 10.3.0.6294).
- Kaspersky Endpoint Security 10 Service Pack 2 Maintenance Release 2 для Windows (сборка 10.3.0.6294).
- Kaspersky Endpoint Security 10 Service Pack 2 Maintenance Release 3 для Windows (сборка 10.3.3.275).
- Kaspersky Endpoint Security 10 Service Pack 2 Maintenance Release 4 для Windows (сборка 10.3.3.275).
- Kaspersky Endpoint Security для Windows 11.0.0 (сборка 11.0.0.6499).

- Kaspersky Endpoint Security для Windows 11.0.1 (сборка 11.0.1.90).
- Kaspersky Endpoint Security для Windows 11.0.1 SF1 (сборка 11.0.1.90).
- Kaspersky Endpoint Security для Windows 11.1.0 (сборка 11.1.0.15919).
- Kaspersky Endpoint Security для Windows 11.1.1 (сборка 11.1.1.126).
- Kaspersky Endpoint Security для Windows 11.2.0 (сборка 11.2.0.2254).
- Kaspersky Endpoint Security для Windows 11.2.0 CF1 (сборка 11.2.0.2254).
- Kaspersky Endpoint Security для Windows 11.3.0 (сборка 11.3.0.773).
- Kaspersky Endpoint Security для Windows 11.4.0 (сборка 11.4.0.233).
- Kaspersky Endpoint Security для Windows 11.5.0 (сборка 11.5.0.590).

Компоненты Kaspersky Endpoint Security

В процессе установки вы можете выбрать компоненты Kaspersky Endpoint Security, которые вы хотите установить.

Для установки сертифицированной конфигурации программы Kaspersky Endpoint Security необходимо исключить установку компонентов Сетевой экран и Контроль устройств (см. рис. ниже).

Выберите следующие компоненты для установки:

- Ядро программы, включая задачи проверки;
- Продвинутая защита:
  - Анализ поведения;
  - Защита от эксплойтов;
  - Отказ вредоносных действий;
  - Предотвращение вторжений (только для рабочей станции).
- Базовая защита:
  - Защита от файловых угроз;
  - Защита от почтовых угроз;
  - Защита от веб-угроз (только для рабочей станции);
  - Защита от сетевых угроз (только для рабочей станции);
  - Защита от атак BadUSB;
  - AMSI-защита.
- Контроль безопасности:
  - Веб-Контроль (только для рабочей станции);
  - Контроль программ;
  - Адаптивный контроль аномалий (только для рабочей станции).
- Endpoint Agent.

- Коннектор к Агенту администрирования.

Вы можете изменить состав компонентов после установки программы. Для этого вам нужно запустить мастер установки повторно и выбрать операцию изменения состава компонентов.

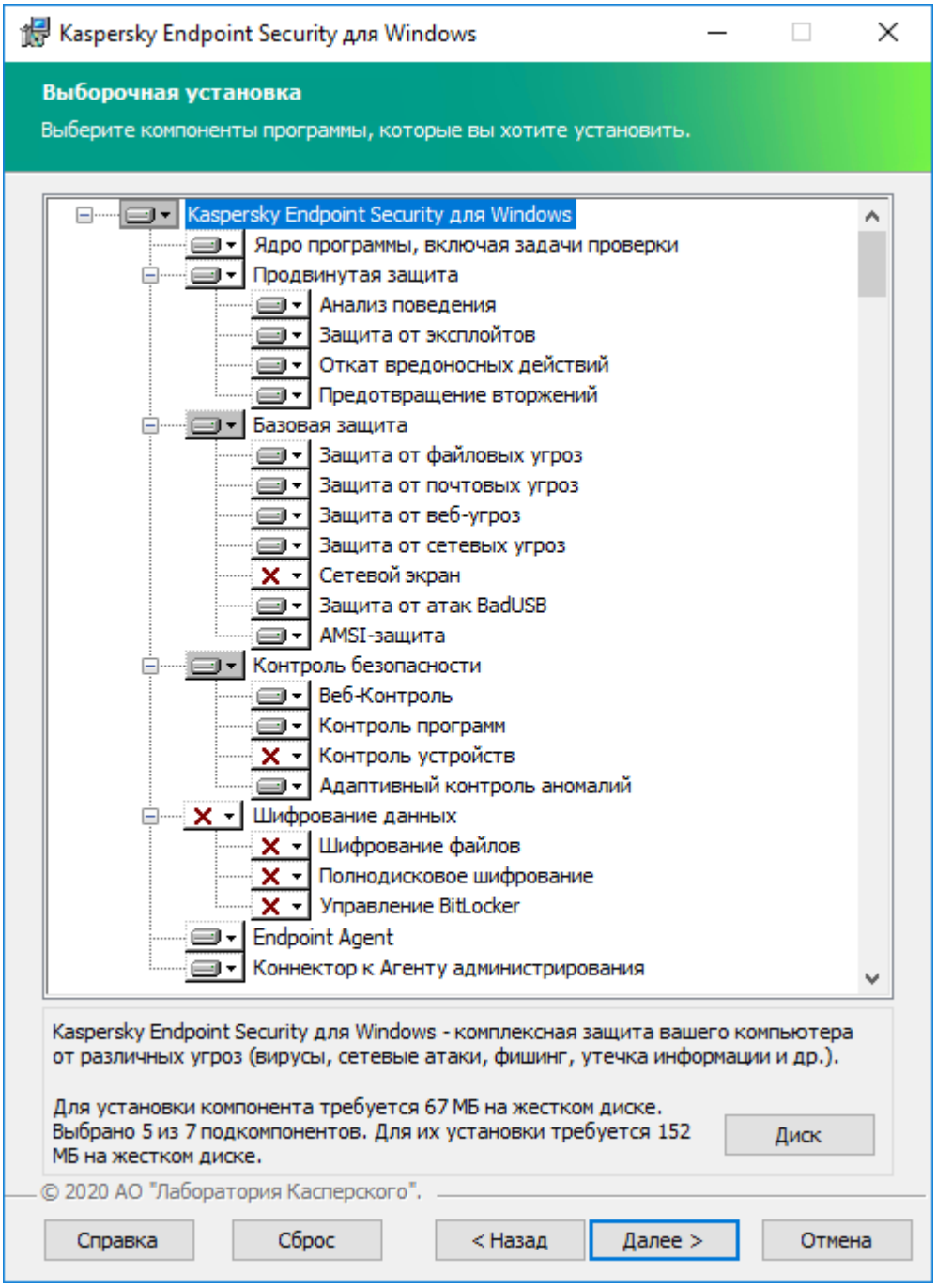


Рисунок 1. Сертификационная конфигурация программы для рабочей станции

Дополнительные параметры

Защитить процесс установки программы. Защита установки включает в себя защиту от подмены дистрибутива вредоносными программами, блокирование доступа к папке установки Kaspersky Endpoint Security и блокирование доступа к разделу системного реестра с ключами программы. Выключать защиту процесса установки рекомендуется в том случае, когда иначе невозможно выполнить установку программы (например, такая ситуация может возникнуть при удаленной установке через Windows Remote Desktop).

Обеспечить совместимость с Citrix PVS. Вы можете включить поддержку Citrix Provisioning Services для установки Kaspersky Endpoint Security на виртуальную машину.

Добавить путь к программе в переменную окружения %PATH%. Вы можете добавить путь установки в переменную %PATH% для удобства использования интерфейса командной строки.

kaspersky

Активация программы с помощью мастера активации программы

Активация программы должна быть выполнена на компьютере с актуальными системными датой и временем. При изменении системных даты и времени после активации программы ключ становится неработоспособным. Программа переходит к режиму работы без обновлений, и Kaspersky Security Network недоступен. Восстановить работоспособность ключа можно только переустановкой операционной системы.

► *Чтобы активировать Kaspersky Endpoint Security с помощью мастера активации программы, выполните следующие действия:*

1. Нажмите на кнопку **Лицензия**, расположенную в нижней части главного окна программы.
2. В открывшемся окне нажмите на кнопку **Активировать программу по новой лицензии**.

   Запустится мастер активации программы. Следуйте указаниям мастера активации программы.

   В сертифицированной версии программы Kaspersky Endpoint Security допускается только активация файлом ключа. Иные способы активации ведут к выходу из безопасного состояния программы.

3. В блоке **Активировать с помощью файла ключа** нажмите на кнопку **Выбрать файл ключа**.

   Файл ключа – это файл с расширением key, который вам предоставляет "Лаборатория Касперского". Файл ключа предназначен для добавления лицензионного ключа, активирующего программу. Чтобы активировать программу с помощью файла ключа, не требуется подключение к серверам активации "Лаборатории Касперского".

4. В открывшемся окне выберите файл ключа.

   Kaspersky Endpoint Security покажет информацию о лицензии: тип лицензии, срок действия лицензии и другая информация.

5. Нажмите на кнопку **Активировать**.

В результате на компьютер будет добавлен лицензионный ключ (см. рис. ниже).

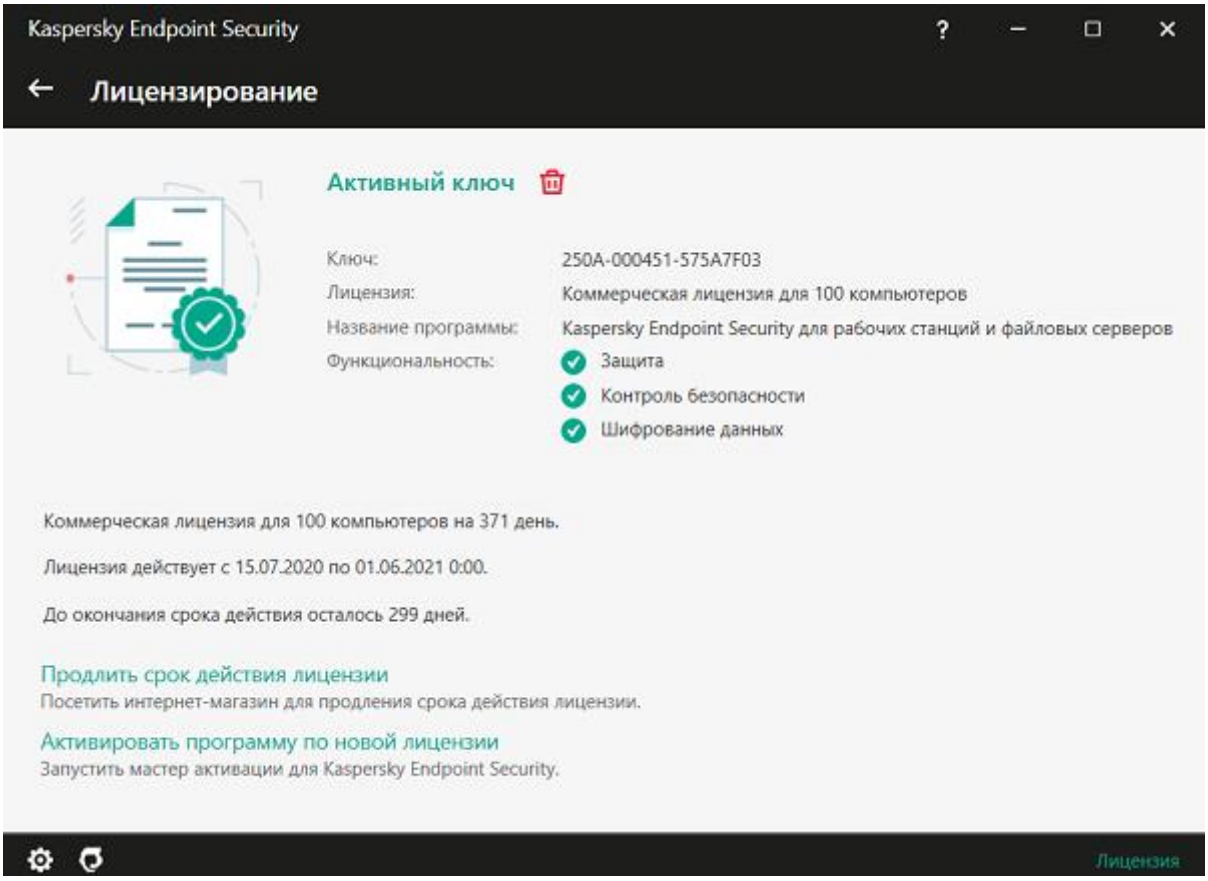


Рисунок 2. Информация о лицензионной ключе

kaspersky

Удаление программы

► *Чтобы удалить Kaspersky Endpoint Security с помощью мастера установки программы, выполните следующие действия:*

1. Откройте окно **Панель управления** одним из следующих способов:
   - Если вы используете Windows 7, то в меню **Пуск** выберите пункт **Панель управления**.
   - Если вы используете Windows 8 или Windows 8.1, то нажмите сочетание клавиш **WIN+I** и выберите пункт **Панель управления**.
   - Если вы используете Windows 10, то нажмите сочетание клавиш **WIN+X** и выберите пункт **Панель управления**.
2. В окне **Панель управления** выберите пункт **Программы и компоненты**.
3. В списке установленных программ выберите элемент **Kaspersky Endpoint Security для Windows**.
4. Нажмите на кнопку **Удалить/Изменить**.

   Запустится мастер установки программы.
5. В окне мастера установки программы **Изменение, восстановление или удаление программы** нажмите на кнопку **Удаление**.
6. Следуйте указаниям мастера установки программы.

kaspersky

Процедура приемки

Перед вводом программы в эксплуатацию проводится процедура приемки, включающая проверку правильной установки, работоспособности и соответствия безопасной (сертифицированной) конфигурации.

В этом разделе

Безопасное состояние

Программа находится в безопасном состоянии (сертифицированной конфигурации), если параметры программы находятся в рамках допустимых значений, приведенных в приложении к этому документу.

Проверка работоспособности. Тестовый файл EICAR

Чтобы проверить работоспособность программы, вы можете использовать тестовый файл EICAR.

Тестовый файл EICAR предназначен для проверки работы антивирусных программ. Он разработан организацией The European Institute for Computer Antivirus Research (EICAR).

Тестовый файл EICAR не является вирусом и не содержит программного кода, который может нанести вред вашему компьютеру, но антивирусные программы большинства производителей идентифицируют в нем угрозу.

Вы можете загрузить тестовый файл EICAR со страницы веб-сайта организации EICAR.

Проверка работоспособности Защиты от веб-угроз

Проверку работоспособности Защиты от веб-угроз не рекомендуется выполнять в браузере Edge. У браузера Edge есть встроенная система безопасности. Браузер Edge блокирует тестовый вредоносный веб-сайт раньше Kaspersky Endpoint Security. Для проверки работоспособности Защиты от веб-угроз используйте браузер Explorer.

► *Чтобы проверить работоспособность Защиты от веб-угроз, выполните следующие действия:*

1. Включите защиту виртуальной машины от веб-угроз.
   a. В главном окне программы нажмите на кнопку ⚙.
   b. В окне параметров программы выберите раздел **Защита** → **Базовая защита** → **Защита от веб-угроз**.
   c. В правой части окна настройки программы убедитесь, что переключатель **Защита от веб-угроз** включен.
   d. Сохраните внесенные изменения.
2. В окне браузера перейдите по ссылке на тестовый вредоносный веб-сайт.

   Kaspersky Endpoint Security сообщает о запрете доступа, отобразив уведомление в окне браузера (см. рис. ниже).
3. Проверьте информацию в отчете об обнаруженных вирусах:
   a. В главном окне программы нажмите на кнопку **Больше функций** → **Отчеты**.
   b. В открывшемся окне перейдите в раздел **Защита от веб-угроз**.
   c. Убедитесь, что в отчете присутствует сообщение об обнаружении вируса и информация об этом событии верна.

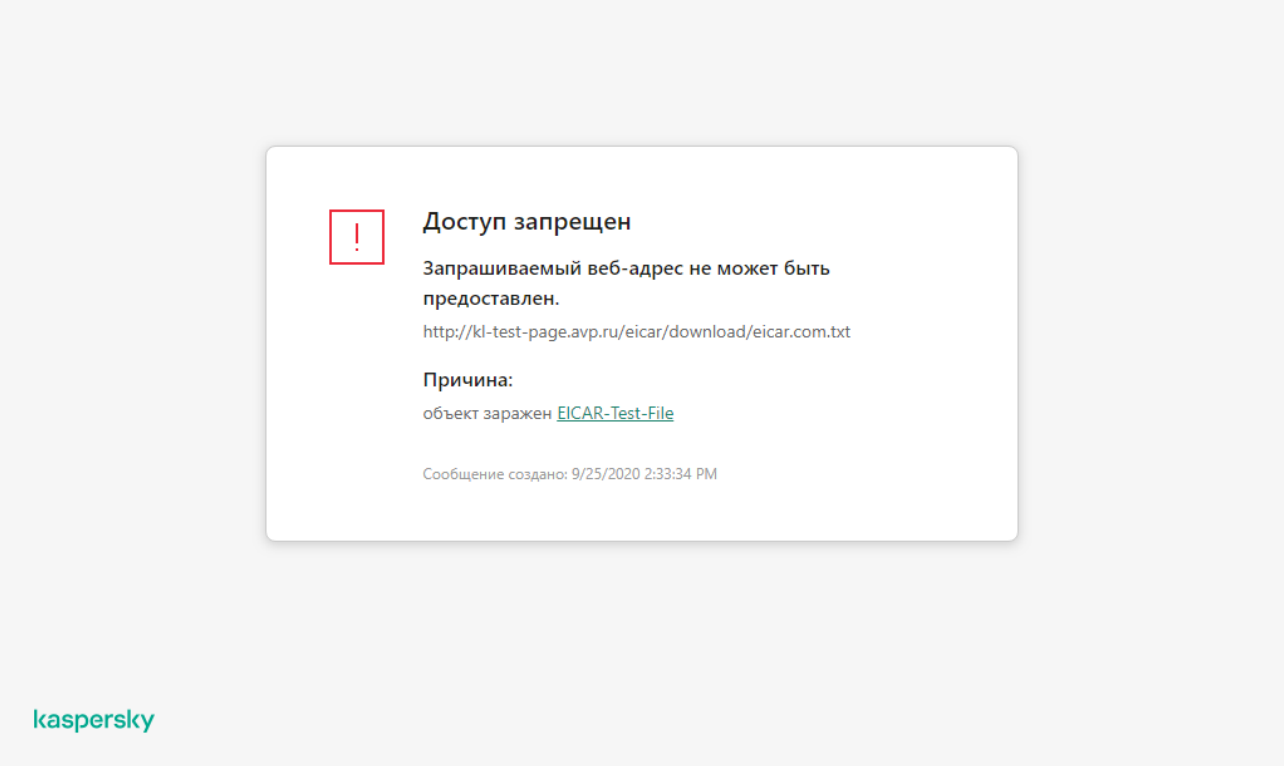


Рисунок 3. Сообщение о запрете доступа к веб-сайту

Проверка работоспособности Защиты от файловых угроз

► *Чтобы проверить работоспособность Защиты от файловых угроз, выполните следующие действия:*

1. Отключите защиту виртуальной машины от веб-угроз:

   > Этот шаг необходим для успешного размещения на виртуальной машине тестового файла, иначе он будет мгновенно удален программой.

   a. В главном окне программы нажмите на кнопку ⚙.

   b. В окне параметров программы выберите раздел **Защита** → **Базовая защита** → **Защита от веб-угроз**.

   c. В правой части окна настройки программы выключите переключатель **Защита от веб-угроз**.

   d. Сохраните внесенные изменения.

2. Загрузите тестовый файл EICAR и разместите его в новую папку на системном диске виртуальной машины.

3. Перейдите в папку с тестовым файлом, загруженным на шаге, и запустите его.

   Kaspersky Endpoint Security удаляет тестовый файл с виртуальной машины.

4. Проверьте информацию в отчете об обнаруженных вирусах:

   a. В главном окне программы нажмите на кнопку **Больше функций** → **Отчеты**.

   b. В открывшемся окне перейдите в раздел **Защита от файловых угроз**.

   c. Убедитесь, что в отчете отображается верная информация об обнаружении зараженного файла (время события, путь к файлу).

Проверка работоспособности антивирусной проверки

► *Что проверить работоспособность функции антивирусной проверки, выполните следующие действия:*

1. Отключите защиту виртуальной машины:

   > Этот шаг необходим для успешного размещения на виртуальной машине тестового файла, иначе он будет мгновенно удален программой.

   a. В главном окне программы нажмите на кнопку ⚙.

   b. В окне параметров программы выберите раздел **Защита** → **Базовая защита** → **Защита от веб-угроз**.

   c. В правой части окна настройки программы выключите переключатель **Защита от веб-угроз**.

   d. Сохраните внесенные изменения.

2. Загрузите тестовый файл EICAR и разместите его в новую папку на системном диске виртуальной машины.

3. Добавьте в область проверки папку с тестовым файлом EICAR:
   a. В главном окне программы нажмите на кнопку **Задачи**.
   b. В открывшемся окне выберите виджет задачи **Выборочная проверка**.
   c. Нажмите на кнопку **Выбрать** и добавьте в область проверки папку с тестовым файлом EICAR.

      В виджете задачи будет добавлена информация о количестве выбранных объектов для проверки.
4. В виджете задачи выборочной проверки нажмите на кнопку **Запустить проверку**.
5. По окончании выполнения задачи проверки проверьте информацию в отчете об обнаруженных вирусах:
   a. В главном окне программы нажмите на кнопку **Больше функций** → **Отчеты**.
   b. В открывшемся окне перейдите в раздел **Проверка**.
   c. Убедитесь, что в отчете отображается верная информация об обнаружении зараженного файла (время события, путь к файлу).

Проверка работоспособности функции контроля запуска программ

Перед проверкой работоспособности функции контроля запуска программ установите программу для тестирования, например, Notepad++. Контроль программ по умолчанию разрешает запуск программ для правила *Операционная система и ее компоненты*. Это правило включает в себя программы, такие как Блокнот, Explorer, WordPad и другие. Специалисты "Лаборатории Касперского" не рекомендует выключать правило *Операционная система и ее компоненты*, так как возможна некорректная работа операционной системы и пользовательских программ.

► *Чтобы проверить работоспособность функции контроля запуска программ, выполните следующие действия:*

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Защита** → **Контроль безопасности** → **Контроль программ**.
3. Включите переключатель **Контроль программ**.
4. В блоке **Действие при запуске запрещенных программ** выберите **Блокировать запуск программ, запрещенных правилами**.
5. В блоке **Режим контроля запуска программ** выберите значение **Список запрещенных**.

   Если выбран этот вариант, Контроль программ разрешает всем пользователям запуск любых программ, кроме случаев, удовлетворяющих условиям запрещающих правил Контроля программ.
6. Нажмите на кнопку **Запрещенные программы**.

   Откроется список правил Контроля программ.
7. Нажмите на кнопку **Добавить**.

   Откроется окно для добавления условий контроля программы.

8. На закладке **Общие настройки** задайте основные параметры правила:
   a. В поле **Название правила** укажите произвольное имя.
   b. В поле **Описание** введите описание правила.
   c. Убедитесь, что в таблице **Субъекты и их права** для пользователей из группы **Все** установлено значение **Запрещено**.
9. На закладке **Условия** добавьте условие срабатывания правила.
   a. Нажмите на кнопку **Добавить**.

      Запустится мастер добавления условия для работы правила.
   b. Выберите вариант **Условие вручную** и перейдите на следующий шаг.
   c. Выберите вариант **Метаданные**, установите флажок **Название файла,** в поле ввода введите `Notepad++.exe`.
   d. Сохраните внесенные изменения.
10. Запустите программу Notepad++.
11. Убедитесь, что запуск программы запрещен (см. рис. ниже).

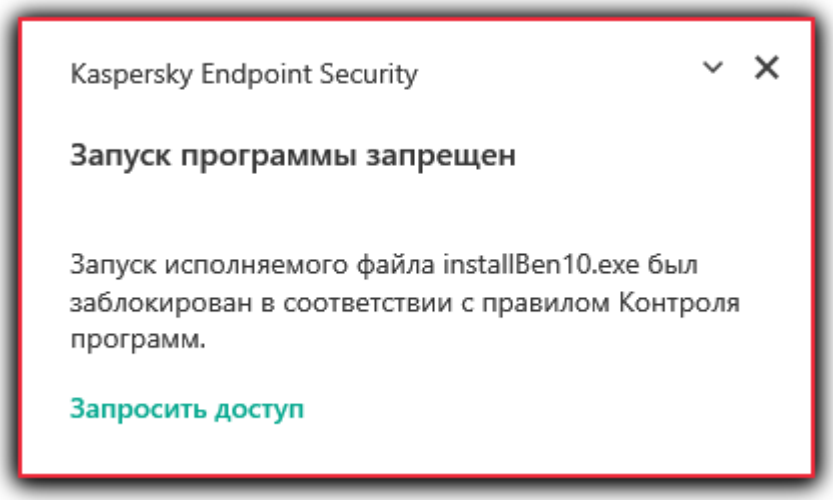


Рисунок 4. Уведомление Контроля программ

12. Проверьте информацию в отчете:
   a. В главном окне программы нажмите на кнопку **Больше функций** → **Отчеты**.
   b. В открывшемся окне перейдите в раздел **Контроль программ**.
   c. Убедитесь, что в отчете присутствует сообщение о запрете запуска программы Notepad++ и информация об этом событии верна.

kaspersky

Разделение доступа к функциям программы по пользовательским ролям

По умолчанию пользователи с ролью "Администратор Kaspersky Endpoint Security" в системе администрирования Kaspersky Security Center, имеют доступ ко всем функциям Kaspersky Endpoint Security.

Пользователи, которые имеют право **Изменение** в Kaspersky Endpoint Security, могут предоставлять доступ к функциям Kaspersky Endpoint Security другим пользователям, добавленным в Kaspersky Security Center или входящим в домен.

Вы можете выбрать для пользователя или группы пользователей Kaspersky Endpoint Security один из следующих предустановленных уровней доступа к функциям Kaspersky Endpoint Security:

- **Чтение** – возможность просматривать общие параметры работы Kaspersky Endpoint Security, параметры работы компонентов Kaspersky Endpoint Security, статистику работы Kaspersky Endpoint Security и права пользователей Kaspersky Endpoint Security.
- **Изменение** – доступ ко всем функциям программы, кроме изменения прав пользователей: возможность просматривать и изменять общие параметры работы Kaspersky Endpoint Security, параметры работы компонентов Kaspersky Endpoint Security, а также просматривать статистику работы Kaspersky Endpoint Security и права пользователей Kaspersky Endpoint Security.
- **Выполнение** – возможность запускать и останавливать задачи Kaspersky Endpoint Security.
- **Выполнение операций с выборкой устройств** – возможность запускать и останавливать задачи Kaspersky Endpoint Security для выборки устройств.

Также вы можете выполнять расширенную настройку прав доступа: разрешать или запрещать доступ к отдельным функциям Kaspersky Endpoint Security.

Таблица 1. Права доступа к функциям Kaspersky Endpoint Security

Функциональная область	Компонент Kaspersky Endpoint Security
Адаптивный контроль аномалий	Адаптивный контроль аномалий.
Компоненты защиты	Защита от файловых угроз Защита от веб-угроз Защита от почтовых угроз Защита от сетевых угроз Сетевой экран AMSI-защита Защита от эксплойтов Анализ поведения Откат вредоносных действий
Контроль программ	Контроль программ.

Функциональная область	Компонент Kaspersky Endpoint Security
Базовая функциональность	Проверка Обновление баз / Откат обновления баз Проверка целостности Удаление данных Добавление ключа Установка Изменение состава компонентов Управление учетными записями Агента аутентификации
Контроль устройств	Контроль устройств
Шифрование	Шифрование диска Kaspersky Управление BitLocker Шифрование файлов Шифрование съемных дисков
Предотвращение вторжений	Предотвращение вторжений
Исключения	Угрозы и исключения
Веб-Контроль	Веб-Контроль

kaspersky

Управление программой через Консоль администрирования Kaspersky Security Center

Kaspersky Security Center позволяет удаленно устанавливать и удалять, запускать и останавливать Kaspersky Endpoint Security, настраивать параметры работы программы, изменять состав компонентов программы, добавлять ключи, запускать и останавливать задачи обновления и проверки.

Управление программой через Kaspersky Security Center осуществляется с помощью плагина управления Kaspersky Endpoint Security.

Подробнее об управлении программой через Kaspersky Security Center *см. в справке Kaspersky Security Center* https://help.kaspersky.com/KSC/12/ru-RU/.

В этом разделе

О плагине управления Kaspersky Endpoint Security для Windows

Плагин управления Kaspersky Endpoint Security для Windows обеспечивает взаимодействие Kaspersky Endpoint Security с Kaspersky Security Center. Плагин управления позволяет управлять Kaspersky Endpoint Security с помощью следующих инструментов: политики (см. раздел "Управление политиками" на стр. 37), задачи (см. раздел "Управление задачами" на стр. 33), а также локальные параметры программы (см. раздел "Настройка локальных параметров программы" на стр. 32). Для взаимодействия с Kaspersky Security Center 12 Web Console предназначен веб-плагин.

Версия плагина управления может отличаться от версии программы Kaspersky Endpoint Security, установленной на клиентском компьютере. Если в установленной версии плагина управления предусмотрено меньше функций, чем в установленной версии Kaspersky Endpoint Security, то параметры недостающих функций не регулируются плагином управления. Такие параметры могут быть изменены пользователем в локальном интерфейсе Kaspersky Endpoint Security.

Веб-плагин по умолчанию не установлен в Kaspersky Security Center 12 Web Console. В отличие от плагина управления для Консоли администрирования Kaspersky Security Center, который устанавливается на рабочее место администратора, веб-плагин требуется установить на компьютер с установленной программой Kaspersky Security Center 12 Web Console. При этом функции веб-плагина доступны всем

администраторам, у которых есть доступ к Web Console в браузере. Вы можете просмотреть список установленных веб-плагинов в интерфейсе Web Console (**Параметры Консоли** → **Плагины**). Подробнее о совместимости версий веб-плагинов и Web Console см. в *справке Kaspersky Security Center* https://help.kaspersky.com/KSC/12/ru-RU/.

Установка веб-плагина

Вы можете установить веб-плагин следующими способами:

- Установить веб-плагин с помощью мастера первоначальной настройки Kaspersky Security Center 12 Web Console.

  Web Console автоматически предлагает запустить мастер первоначальной настройки при первом подключении Web Console к Серверу администрирования. Также вы можете запустить мастер первоначальной настройки в интерфейсе Web Console (**Обнаружение устройств и развертывание** → **Развертывание и назначение** → **Мастер первоначальной настройки**). Мастер первоначальной настройки также может проверить актуальность установленных веб-плагинов и загрузит необходимые обновления для них. Подробнее о мастере первоначальной настройки Kaspersky Security Center 12 Web Console см. в *справке Kaspersky Security Center* https://help.kaspersky.com/KSC/12/ru-RU/.

- Установить веб-плагин из списка доступных дистрибутивов в Web Console.

  Для установки веб-плагина требуется выбрать дистрибутив веб-плагина Kaspersky Endpoint Security в интерфейсе Web Console (**Параметры Консоли** → **Плагины**). Список доступных дистрибутивов обновляется автоматически после выпуска новых версий программ "Лаборатории Касперского".

- Загрузить дистрибутив в Web Console из стороннего источника.

  Для установки веб-плагина требуется добавить ZIP-архив дистрибутива веб-плагина Kaspersky Endpoint Security в интерфейсе Web Console (**Параметры Консоли** → **Плагины**). Дистрибутив веб-плагина вы можете загрузить, например, на веб-сайте "Лаборатории Касперского".

Особенности использования защищенных протоколов для взаимодействия с внешними службами

Kaspersky Endpoint Security и Kaspersky Security Center используют защищенный канал связи с TLS (Transport Layer Security) для работы с внешними службами "Лаборатории Касперского". Kaspersky Endpoint Security использует внешние службы для работы следующих функций:

- обновление баз и модулей программы;
- активация программы с помощью кода активации (тип активации 2.0);
- использование Kaspersky Security Network.

Использование TLS обеспечивает безопасность работы программы за счет следующих свойств:

- Шифрование. Содержание сообщений конфиденциально и не раскрывается посторонним пользователям.
- Целостность. Получатель сообщения уверен в неизменности содержания с момента отсылки отправителем.
- Аутентификация. Получатель уверен, что связь устанавливается только с доверенным сервером "Лаборатории Касперского".

Для аутентификации серверов Kaspersky Endpoint Security использует сертификаты открытых ключей. Для работы с сертификатами требуется инфраструктура открытых ключей (англ. Public Key Infrastructure – PKI). Удостоверяющий центр является частью PKI. Так как службы "Лаборатории Касперского" не являются публичными и носят технический характер, "Лаборатория Касперского" использует собственный Удостоверяющий центр. В этом случае при отзыве корневых сертификатов Thawte, VeriSign, GlobalTrust и других, работоспособность PKI "Лаборатории Касперского" не будет нарушена.

Окружения, имеющие MITM (программные и аппаратные средства, поддерживающие разбор протокола HTTPS), Kaspersky Endpoint Security считает небезопасными. При работе со службами "Лаборатории Касперского" могут возникать ошибки, например, ошибки об использовании самозаверяющих сертификатов (англ. Self-Signed Certificate). Эти ошибки могут возникать из-за того, что средство HTTPS Inspection из вашего окружения не распознает PKI "Лаборатории Касперского". Для устранения проблем необходимо настроить исключения для взаимодействия с внешними службами (см. раздел "Приложение 5. Сетевые параметры для взаимодействия с внешними службами" на стр. 286).

Настройка локальных параметров программы

В Kaspersky Security Center вы можете настроить параметры Kaspersky Endpoint Security на конкретном компьютере – *локальные параметры программы*. Некоторые параметры могут быть недоступны для изменения. Эти параметры заблокированы атрибутом в свойствах политики (см. раздел "Управление политиками" на стр. 37).

Как настроить локальные параметры программы в Консоли администрирования (MMC):

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева Консоли администрирования откройте папку с названием группы администрирования, в состав которой входит нужный вам клиентский компьютер.
3. В рабочей области выберите закладку **Устройства**.
4. Выберите компьютер, для которого вы хотите настроить параметры Kaspersky Endpoint Security.
5. В контекстном меню клиентского компьютера выберите пункт **Свойства**.

   Откроется окно свойств клиентского компьютера.
6. В окне свойств клиентского компьютера выберите раздел **Программы**.

   Справа в окне свойств клиентского компьютера отобразится список программ "Лаборатории Касперского", установленных на клиентском компьютере.
7. Выберите программу Kaspersky Endpoint Security.
8. Нажмите на кнопку **Свойства** под списком программ "Лаборатории Касперского".

   Откроется окно **Параметры программы "Kaspersky Endpoint Security для Windows"**.
9. В разделе **Общие параметры** настройте параметры работы Kaspersky Endpoint Security, а также параметры отчетов и хранилищ.

   Остальные разделы окна **Параметры программы "Kaspersky Endpoint Security для Windows"** стандартны для программы Kaspersky Security Center. Описание этих разделов вы можете прочитать в справке для Kaspersky Security Center.

Если для программы создана политика, в которой запрещено изменение некоторых параметров, то во время настройки параметров программы в разделе **Общие параметры** их изменение недоступно.

10. В окне **Параметры программы "Kaspersky Endpoint Security для Windows"** нажмите на кнопку **OK**, чтобы сохранить внесенные изменения.

Как настроить локальные параметры программы в Web Console и Cloud Console:

1. В главном окне Web Console выберите **Устройства** → **Управляемые устройства**.
2. Нажмите на имя компьютера, на котором вы хотите настроить локальные параметры программы.

   Откроются свойства компьютера.
3. Выберите закладку **Программы**.
4. Нажмите на **Kaspersky Endpoint Security для Windows**.

   Откроются локальные параметры программы
5. Выберите закладку **Параметры программы**.
6. Настройте локальные параметры программы.
7. Локальные параметры программы повторяют параметры политики, кроме параметров шифрования.

Управление задачами

Для работы с Kaspersky Endpoint Security через Kaspersky Security Center вы можете создавать следующие типы задач:

- локальные задачи, определенные для отдельного клиентского компьютера;
- групповые задачи, определенные для клиентских компьютеров, входящих в группы администрирования;
- задачи для выборки компьютеров.

Вы можете создавать любое количество групповых задач, задач для выборки компьютеров и локальных задач. Подробнее о работе с группами администрирования и выборками компьютеров *см. в справке Kaspersky Security Center* https://help.kaspersky.com/KSC/12/ru-RU/.

Kaspersky Endpoint Security поддерживает выполнение следующих задач:

- **Антивирусная проверка** (см. раздел "**Проверка компьютера**" на стр. 52). Kaspersky Endpoint Security проверяет на вирусы и другие программы, представляющие угрозу, области компьютера, указанные в параметрах задачи. Задача *Антивирусная проверка* является обязательной для работы Kaspersky Endpoint Security и создается во время работы мастера первоначальной настройки. Рекомендуется настроить расписание выполнения задачи минимум раз в неделю.
- **Добавление ключа**. Kaspersky Endpoint Security добавляет ключ для активации программ, в том числе дополнительный. Перед выполнением задачи убедитесь, что количество компьютеров, на которых будет выполняться задача, не превышает количество компьютеров, на которые рассчитана лицензия.

- **Изменение состава компонентов программы**. Kaspersky Endpoint Security устанавливает или удаляет на клиентских компьютерах компоненты согласно списку компонентов, указанному в параметрах задачи. Компонент Защита от файловых угроз удалить невозможно. Оптимальный состав компонентов Kaspersky Endpoint Security позволяет экономить ресурсы компьютера.
- **Инвентаризация**. Kaspersky Endpoint Security получает информацию обо всех исполняемых файлах программ, хранящихся на компьютерах. Задачу *Инвентаризация* выполняет компонент Контроль программ. Если компонент Контроль программ не установлен, задача завершит работу с ошибкой.
- **Обновление**. Kaspersky Endpoint Security обновляет базы и модули программы. Задача *Обновление* является обязательной для работы Kaspersky Endpoint Security и создается во время работы мастера первоначальной настройки. Рекомендуется настроить расписание выполнения задачи минимум раз в день.
- **Удаление данных**. Kaspersky Endpoint Security удаляет файлы и папки с компьютеров пользователей немедленно или при длительном отсутствии связи с Kaspersky Security Center.
- **Откат обновления** (см. раздел "**Откат последнего обновления**" на стр. 76). Kaspersky Endpoint Security откатывает последнее обновление баз и модулей программы. Это может понадобиться, например, если новые базы содержат некорректные данные, из-за которых Kaspersky Endpoint Security может блокировать безопасную программу.
- **Проверка целостности** (см. раздел "**Проверка целостности программы**" на стр. 62). Kaspersky Endpoint Security анализирует файлы программы, проверяет файлы на наличие повреждений или изменений и проверяет цифровые подписи файлов программы.
- **Управление учетными записями Агента аутентификации**. Kaspersky Endpoint Security настраивает параметры учетных записей Агента аутентификации. Агент аутентификации нужен для работы с зашифрованными дисками. Перед загрузкой операционной системы пользователю нужно пройти аутентификацию с помощью агента.

Запуск задач на компьютере выполняется только в том случае, если запущена программа Kaspersky Endpoint Security (см. раздел "Запуск и остановка Kaspersky Endpoint Security" на стр. 47).

Создание задачи

Как создать задачу в Консоли администрирования (MMC):

1. Откройте Консоль администрирования Kaspersky Security Center.
2. Выберите папку **Задачи** дерева Консоли администрирования.
3. Нажмите на кнопку **Новая задача**.

   Запустится мастер создания задачи.
4. Следуйте указаниям мастера создания задачи.

Как создать задачу в Web Console и Cloud Console:

1. В главном окне Web Console выберите **Устройства** → **Задачи**.

   Откроется список задач.
2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи.

3. Настройте параметры задачи:
   a. В раскрывающемся списке **Программа** выберите **Kaspersky Endpoint Security для Windows (11.6.0)**.
   b. В раскрывающемся списке **Тип задачи** выберите задачу, которую вы хотите запустить на компьютерах пользователей.
   c. В поле **Название задачи** введите короткое описание, например, `Обновление программы для бухгалтерии`.
   d. В блоке **Выбор устройств, которым будет назначена задача** выберите область действия задачи.
4. Выберите устройства в соответствии с выбранным вариантом области действия задачи. Нажмите на кнопку **Далее**.
5. Завершите работу мастера по кнопке **Готово**.

В списке задач отобразится новая задача. Задача будет иметь параметры по умолчанию. Для настройки параметров задачи вам нужно перейти в свойства задачи. Для выполнения задачи вам нужно установить флажок напротив задачи и нажать на кнопку **Запустить**. После запуска задачи вы можете остановить задачу и возобновить выполнение задачи позже.

В списке задач вы можете контролировать результат выполнения задачи: статус задачи и статистику выполнения задачи на компьютерах. Также вы можете создать выборку событий для контроля за выполнением задач (**Мониторинг и отчеты** → **Выборки событий**). Подробнее о выборке событий *см. в справке Kaspersky Security Center* https://help.kaspersky.com/KSC/12/ru-RU/. Также результаты выполнения задач сохраняются локально на компьютере в журнале событий Windows и в отчетах Kaspersky Endpoint Security (см. раздел "Работа с отчетами" на стр. 210).

Управление доступом к задачам

Права на доступ к задачам Kaspersky Endpoint Security (чтение, изменение, выполнение) задаются для каждого пользователя, имеющего доступ к Серверу администрирования Kaspersky Security Center, через параметры доступа к функциональным областям Kaspersky Endpoint Security. Для настройки доступа к функциональным областям Kaspersky Endpoint Security перейдите в раздел **Безопасность** окна свойств Сервера администрирования Kaspersky Security Center. Подробнее о концепции управления задачами через Kaspersky Security Center *см. в справке Kaspersky Security Center* https://help.kaspersky.com/KSC/12/ru-RU/.

Вы можете настроить права доступа к задачам для пользователей компьютеров с помощью политики (*режим работы с задачами*). Например, вы можете скрыть групповые задачи в интерфейсе Kaspersky Endpoint Security.

Как настроить режим работы с задачами в интерфейсе Kaspersky Endpoint Security через Консоль администрирования (MMC):

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева Консоли администрирования откройте папку с названием группы администрирования, в состав которой входят нужные клиентские компьютеры.
3. В рабочей области выберите закладку **Политики**.
4. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
5. В окне политики выберите **Локальные задачи** → **Управление задачами**.

6. Настройте режим работы с задачами (см. таблицу ниже).
7. Сохраните внесенные изменения.

Как настроить режим работы с задачами в интерфейсе Kaspersky Endpoint Security через Web Console:

1. В главном окне Web Console выберите закладку **Устройства** → **Политики и профили политик**.
2. Нажмите на название политики Kaspersky Endpoint Security для компьютеров, на которых вы хотите включить поддержку портативного режима.

   Откроется окно свойств политики.
3. Выберите закладку **Параметры программы**.
4. Перейдите в раздел **Локальные задачи** → **Управление задачами**.
5. Настройте режим работы с задачами (см. таблицу ниже).
6. Нажмите на кнопку **ОК**.
7. Подтвердите изменения по кнопке **Сохранить**.

Таблица 2. Параметры управления задачами

Параметр	Описание
Разрешить использование локальных задач	Если флажок установлен, то локальные задачи отображаются в локальном интерфейсе Kaspersky Endpoint Security. Пользователь, при отсутствии дополнительных ограничений политики, может настраивать и запускать задачи. При этом параметры расписания запуска задачи остаются недоступными для пользователя. Пользователь может запускать задачи только вручную. Если флажок снят, то использование локальных задач прекращается. В этом режиме локальные задачи не запускаются по расписанию. Задачи недоступны для запуска и настройки в локальном интерфейсе Kaspersky Endpoint Security, а также при работе с командной строкой. Пользователь по-прежнему может запустить антивирусную проверку файла или папки, выбрав пункт **Проверить на вирусы** в контекстном меню файла или папки. При этом задача проверки запустится со значениями параметров, установленными по умолчанию для задачи выборочной проверки.
Разрешить отображение групповых задач	Если флажок установлен, то локальные задачи отображаются в локальном интерфейсе Kaspersky Endpoint Security. Пользователь может просмотреть полный список задач в интерфейсе программы. Если флажок снят, Kaspersky Endpoint Security показывает пустой список задач.
Разрешить управление групповыми задачами	Если флажок установлен, пользователь может запускать и останавливать заданные в Kaspersky Security Center групповые задачи. Пользователь может запускать и останавливать задачи в интерфейсе программы или в упрощенном интерфейсе программы. Если флажок снят, Kaspersky Endpoint Security запускает задачи автоматически по расписанию, или администратор запускает задачи вручную в Kaspersky Security Center.

kaspersky

Управление политиками

Политика – это набор параметров работы программы, определенный для группы администрирования. Для одной программы можно настроить несколько политик с различными значениями. Для разных групп администрирования параметры работы программы могут быть различными. В каждой группе администрирования может быть создана собственная политика для программы.

Параметры политики передаются на клиентские компьютеры с помощью Агента администрирования при *синхронизации*. По умолчанию Сервер администрирования выполняет синхронизацию сразу после изменения параметров политики. Синхронизация выполняется через UDP-порт 15000 на клиентском компьютере. Сервер администрирования по умолчанию выполняет синхронизацию каждые 15 минут. Если синхронизация после изменения параметров политики не удалась, следующая попытка синхронизации будет выполнена по настроенному расписанию.

Активная и неактивная политика

Политика предназначена для группы управляемых компьютеров и может быть активной или неактивной. Параметры активной политики во время синхронизации сохраняются на клиентских компьютерах. К одному компьютеру нельзя одновременно применить несколько политик, поэтому в каждой группе активной может быть только одна политика.

Вы можете создать неограниченное количество неактивных политик. Неактивная политика не влияет на параметры программы на компьютерах в сети. Неактивные политики предназначены для подготовки к нештатным ситуациям, например, в случае вирусной атаки. В случае атаки через флеш-накопители, вы можете активировать политику, блокирующую доступ к флеш-накопителям. При этом активная политика автоматически становится неактивной.

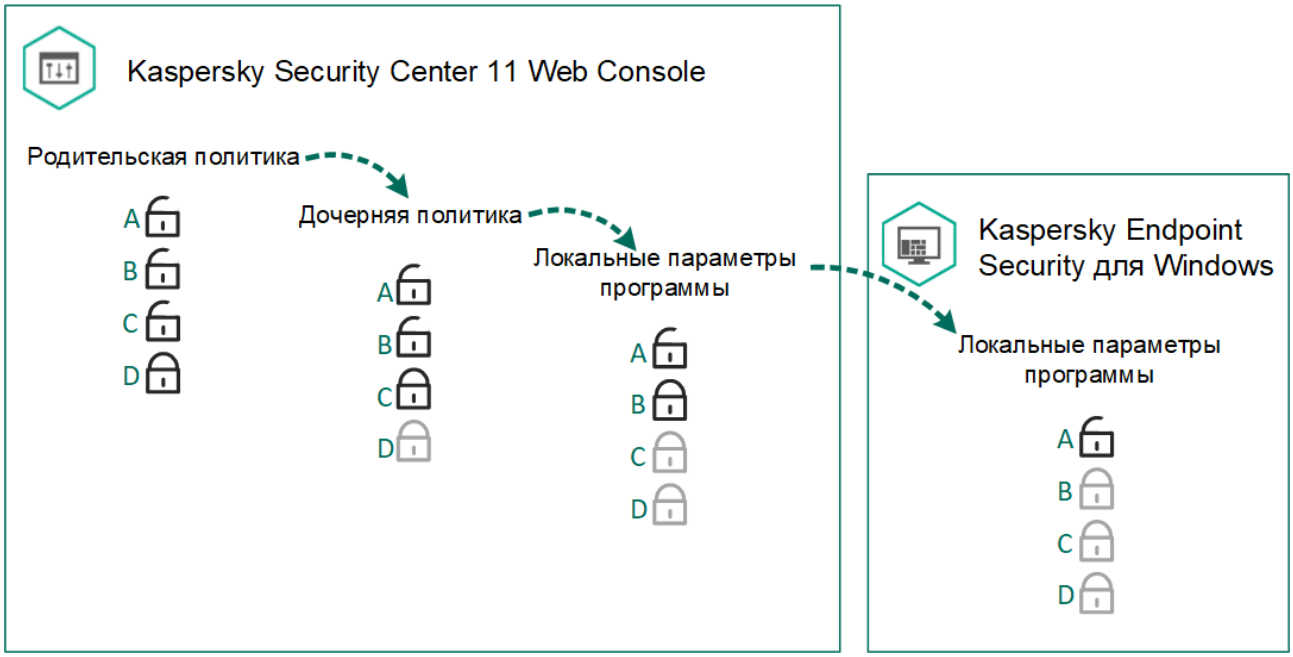
Политика для автономных пользователей

Политика для автономных пользователей активируется, когда компьютер покидает периметр сети организации.

Наследование параметров

Политики, как и группы администрирования, имеют иерархию. По умолчанию дочерняя политика наследует параметры родительской политики. *Дочерняя политика* – политика вложенного уровня иерархии, т.е. политика для вложенных групп администрирования и подчиненных Серверов администрирования. Вы можете выключить наследование параметров из родительской политики.

Каждый параметр, представленный в политике, имеет атрибут , который показывает, наложен ли запрет на изменение параметров в дочерних политиках и локальных параметрах программы (см. раздел "Настройка локальных параметров программы" на стр. 32). Атрибут работает только, если в дочерней политике включено наследование параметров из родительской политики. Политики для автономных пользователей не действуют по иерархии групп администрирования на другие политики.



Права на доступ к параметрам политики (чтение, изменение, выполнение) задаются для каждого пользователя, имеющего доступ к Серверу администрирования Kaspersky Security Center, и отдельно для каждой функциональной области Kaspersky Endpoint Security. Для настройки прав доступа к параметрам политики перейдите в раздел **Безопасность** окна свойств Сервера администрирования Kaspersky Security Center.

Создание политики

Как создать политику в Консоли администрирования (MMC):

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева Консоли администрирования выберите папку с названием группы администрирования, в состав которой входят интересующие вас клиентские компьютеры.
3. В рабочей области выберите закладку **Политики**.
4. Нажмите на кнопку **Новая политика**.

   Запустится мастер создания политики.
5. Следуйте указаниям мастера создания политики.

Как создать политику в Web Console и Cloud Console:

1. В главном окне Web Console выберите **Устройства** → **Политики и профили политик**.
2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания политики.
3. Выберите программу Kaspersky Endpoint Security и нажмите **Далее**.

4. Прочитайте и примите условия Положения о Kaspersky Security Network (KSN) и нажмите **Далее**.
5. На закладке **Общие** вы можете выполнить следующие действия:
   - Изменить имя политики.
   - Выбрать состояние политики:
     - **Активна**. После следующей синхронизации политика будет использоваться на компьютере в качестве действующей.
     - **Неактивна**. Резервная политика. При необходимости неактивную политику можно сделать активной.
     - **Для автономных пользователей**. Политика начинает действовать, когда компьютер покидает периметр сети организации.
   - Настроить наследование параметров:
     - **Наследовать параметры родительской политики**. Если переключатель включен, значения параметров политики наследуются из политики верхнего уровня иерархии. Параметры политики недоступны для изменения, если в родительской политике установлен .
     - **Обеспечить принудительное наследование параметров для дочерних политик**. Если переключатель включен, значения параметров политики будут распространены на дочерние политики. В свойствах дочерней политики будет автоматически включен и недоступен для выключения переключатель **Наследовать параметры родительской политики**. Параметры дочерней политики наследуются из родительской политики, кроме параметров с . Параметры дочерних политик недоступны для изменения, если в родительской политике установлен .
6. На закладке **Параметры программ** вы можете настроить параметры политики Kaspersky Endpoint Security.
7. Нажмите на кнопку **Сохранить**.

В результате параметры Kaspersky Endpoint Security будут настроены на клиентских компьютерах при следующей синхронизации. Вы можете просмотреть информацию о политике, которая применена к компьютеру, в интерфейсе Kaspersky Endpoint Security по кнопке **Поддержка** на главном экране (например, имя политики). Для этого в параметрах политики Агента администрирования нужно включить получение расширенных данных политики. Подробнее о политике Агента администрирования см. в *справке Kaspersky Security Center* https://help.kaspersky.com/KSC/12/ru-RU/.

Индикатор уровня защиты

В верхней части окна **Свойства: <Название политики>** отображается индикатор уровня защиты. Индикатор может принимать одно из следующих значений:

- **Уровень защиты высокий**. Индикатор принимает это значение и цвет индикатора изменяется на зеленый, если включены все компоненты, относящиеся к следующим категориям:
  - **Критические**. Категория включает следующие компоненты:
    - Защита от файловых угроз.
    - Анализ поведения.
    - Защита от эксплойтов.
    - Откат вредоносных действий.

  - **Важные**. Категория включает следующие компоненты:
    - Kaspersky Security Network.
    - Защита от веб-угроз.
    - Защита от почтовых угроз.
    - Предотвращение вторжений.
- **Уровень защиты средний**. Индикатор принимает это значение и цвет индикатора изменяется на желтый, если отключен один важный компонент.
- **Уровень защиты низкий**. Индикатор принимает это значение и цвет индикатора изменяется на красный в одном из следующих случаев:
  - отключены один или несколько критических компонентов;
  - отключены два или более важных компонента.

Если отображается индикатор со значением **Уровень защиты средний** или **Уровень защиты низкий**, то справа от индикатора доступна ссылка, по которой открывается окно **Рекомендованные компоненты защиты**. В этом окне вы можете включить любой из рекомендованных компонентов защиты.

Интерфейс программы

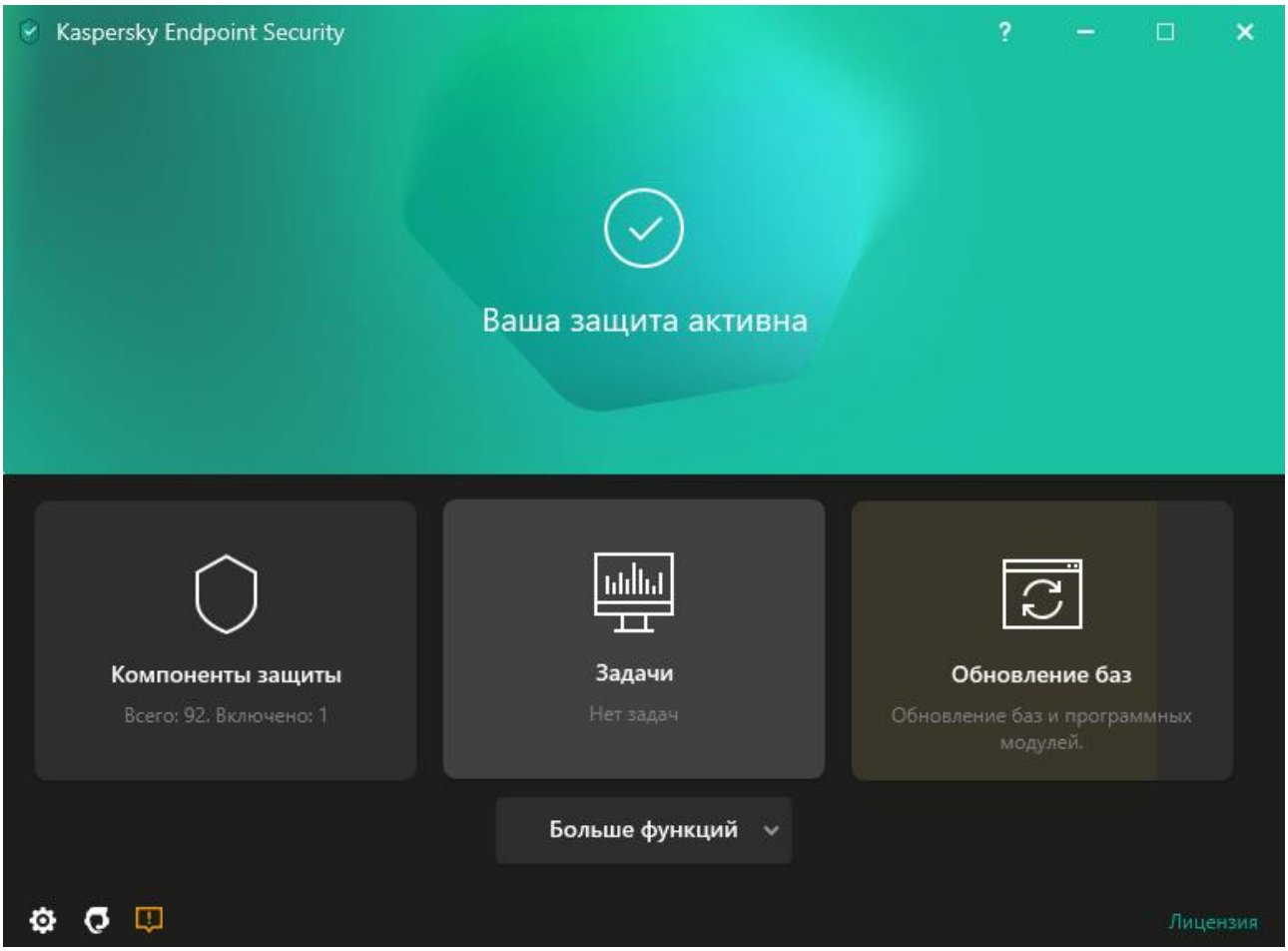


Рисунок 5. Главное окно программы

Компоненты защиты Статус работы установленных компонентов. Также вы можете перейти к настройке любого из установленных компонентов, кроме компонентов шифрования.

Задачи Управление задачами проверки Kaspersky Endpoint Security. Вы можете выполнять антивирусную проверку (см. раздел "Проверка компьютера" на стр. 52) и проверку целостности программы (см. раздел "Проверка целостности программы" на стр. 62). Администратор может скрыть задачи от пользователя (см. раздел "Управление задачами" на стр. 33) или ограничить управление задачами (см. раздел "Управление задачами" на стр. 33).

Обновление баз Управление задачами обновления Kaspersky Endpoint Security. Вы можете выполнять обновление антивирусных баз и модулей программы и откат последнего обновления (на стр. 76). Администратор может скрыть задачи от пользователя (см. раздел "Управление задачами" на стр. 33) или ограничить управление задачами (см. раздел "Управление задачами" на стр. 33).

Больше функций

Переход к другим функциям программы:

- **Отчеты**. Просмотр событий, произошедших во время работы программы, отдельных компонентов и задач.
- **Хранилище**. Просмотр списка копий зараженных файлов, которые были удалены в ходе работы программы.
- **Технологии обнаружения угроз**. Просмотр информации о технологиях обнаружения угроз и количестве угроз, обнаруженных с помощью этих технологий.
- **Kaspersky Security Network**. Статус подключения Kaspersky Endpoint Security к Kaspersky Security Network и глобальная статистика KSN. *Kaspersky Security Network (KSN)* – это инфраструктура облачных служб, предоставляющая доступ к оперативной базе знаний "Лаборатории Касперского" о репутации файлов, интернет-ресурсов и программного обеспечения. Использование данных Kaspersky Security Network обеспечивает более высокую скорость реакции Kaspersky Endpoint Security на неизвестные угрозы, повышает эффективность работы некоторых компонентов защиты, а также снижает вероятность ложных срабатываний. Если вы участвуете в Kaspersky Security Network, программа Kaspersky Endpoint Security получает от служб KSN сведения о категории и репутации проверяемых файлов, а также сведения о репутации проверяемых веб-адресов.
- **Мониторинг активности**. Просмотр информации о работе установленных программ. Мониторинг активности отслеживает файловые, реестровые и системные события в операционной системе, связанные с программой.
- **Мониторинг сети**. Просмотр информации о сетевой активности компьютера в режиме реального времени.
- **Мониторинг шифрования**. Контроль процесса шифрования или расшифровки дисков в режиме реального времени. Мониторинг шифрования доступен, если установлены компоненты Шифрование диска Kaspersky или Шифрование диска BitLocker.

Настройка параметров программы. Администратор может запретить изменение параметров в Kaspersky Security Center (см. раздел "Управление политиками" на стр. 37).

Информация о программе: текущая версия Kaspersky Endpoint Security, дата выпуска баз, ключ и другая информация. Также вы можете перейти на информационные ресурсы "Лаборатории Касперского", чтобы получить полезную информацию, рекомендации и ответы на часто задаваемые вопросы о приобретении, установке и использовании программы.

Сообщения с информацией о доступных обновлениях, а также запросы доступа к зашифрованным файлам и устройствам.

Лицензия

Лицензирование программы. Вы можете приобрести лицензию, активировать программу или продлить подписку. Так же вы можете просмотреть информацию о действующей лицензии.

kaspersky

В этом разделе

Значок программы в области уведомлений

Сразу после установки Kaspersky Endpoint Security значок программы появляется в области уведомлений панели задач Microsoft Windows.

Значок программы выполняет следующие функции:

- служит индикатором работы программы;
- обеспечивает доступ к контекстному меню значка программы и главному окну программы.

Для отображения информации о работе программы предназначены следующие статусы значка программы:

- Значок  означает, что работа критически важных компонентов защиты программы включена. Kaspersky Endpoint Security покажет предупреждение  , если от пользователя требуется выполнить действие, например, перезагрузить компьютер после обновления программы.
- Значок  означает, что работа критически важных компонентов защиты программы выключена или нарушена. Работа компонентов защиты может быть нарушена, например, если срок действия лицензии истек или произошел сбой в работе программы. Kaspersky Endpoint Security покажет предупреждение  с описанием проблемы в защите компьютера.

Контекстное меню значка программы содержит следующие пункты:

- **Kaspersky Endpoint Security для Windows**. Открывает главное окно программы. В этом окне вы можете регулировать работу компонентов и задач программы, просматривать статистику об обработанных файлах и обнаруженных угрозах.
- **Приостановить защиту / Возобновить защиту**. Приостановка работы всех компонентов защиты и контроля, не отмеченных в политике замком (). Перед выполнением этой операции рекомендуется выключить политику Kaspersky Security Center.

  Перед приостановкой работы компонентов защиты и контроля программа запрашивает пароль доступа к Kaspersky Endpoint Security (см. раздел "Защита паролем" на стр. 189) (пароль учетной записи или временный пароль). Далее вы можете выбрать период приостановки: на указанное время, до перезагрузки или по требованию пользователя.

  Этот пункт контекстного меню доступен, если включена Защита паролем (см. раздел "Включение Защиты паролем" на стр. 192). Для возобновления работы компонентов защиты и контроля выберите пункт **Возобновление защиты** в контекстном меню программы.

  Приостановка работы компонентов защиты и контроля не влияет на выполнение задач обновления и проверки. Также программа продолжает использование Kaspersky Security Network.

- **Выключить политику** / **Включить политику**. Выключает политику Kaspersky Security Center на компьютере. Все параметры Kaspersky Endpoint Security доступны для настройки, в том числе параметры, отмеченные в политике закрытым замком ( ). При выключении политики программа запрашивает пароль доступа к Kaspersky Endpoint Security (см. раздел "Защита паролем" на стр. 189) (пароль учетной записи или временный пароль). Этот пункт контекстного меню доступен, если включена Защита паролем (см. раздел "Включение Защиты паролем" на стр. 192). Для включения политики выберите пункт **Включить политику** в контекстном меню программы.
- Настройка. Открывает окно настройки параметров программы.
- **Поддержка**. Вызов окна **Поддержка**, содержащего информацию, необходимую для обращения в Службу технической поддержки "Лаборатории Касперского".
- **О программе**. Открывает информационное окно со сведениями о программе.
- **Выход**. Завершает работу Kaspersky Endpoint Security. Если вы выбрали этот пункт контекстного меню, программа выгружается из оперативной памяти компьютера.

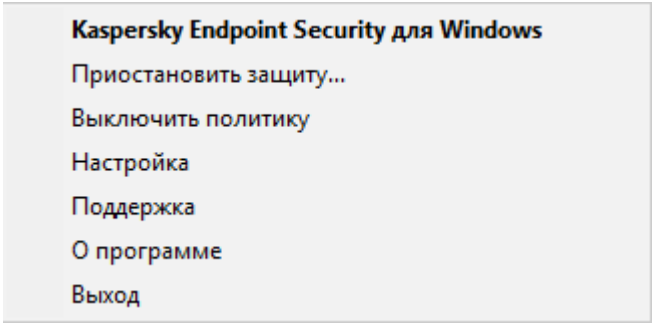


Рисунок 6. Контекстное меню значка программы

Упрощенный интерфейс программы

Если к клиентскому компьютеру, на котором установлена программа Kaspersky Endpoint Security, применена политика Kaspersky Security Center, в которой настроено отображение упрощенного интерфейса программы (см. раздел "Настройка отображения интерфейса программы" на стр. 45), то на этом клиентском компьютере недоступно главное окно программы. По правой клавише мыши пользователь может открыть контекстное меню значка Kaspersky Endpoint Security (см. рис. ниже), содержащее следующие пункты:

- **Выключить политику** / **Включить политику**. Выключает политику Kaspersky Security Center на компьютере. Все параметры Kaspersky Endpoint Security доступны для настройки, в том числе параметры, отмеченные в политике закрытым замком ( ). При выключении политики программа запрашивает пароль доступа к Kaspersky Endpoint Security (см. раздел "Защита паролем" на стр. 189) (пароль учетной записи или временный пароль). Этот пункт контекстного меню доступен, если включена Защита паролем (см. раздел "Включение Защиты паролем" на стр. 192). Для включения политики выберите пункт **Включить политику** в контекстном меню программы.
- **Задачи**. Раскрывающийся список, содержащий следующие элементы:
  - **Проверка целостности**.
  - **Откат последнего обновления**.
  - **Полная проверка**.
  - **Выборочная проверка**.
  - **Проверка важных областей**.
  - **Обновление**.

- **Поддержка**. Вызов окна **Поддержка**, содержащего информацию, необходимую для обращения в Службу технической поддержки "Лаборатории Касперского".
- **Выход**. Завершает работу Kaspersky Endpoint Security. Если вы выбрали этот пункт контекстного меню, программа выгружается из оперативной памяти компьютера.

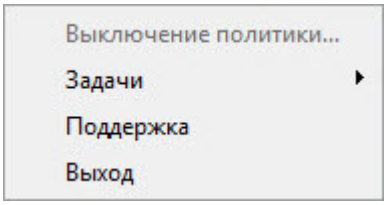


Рисунок 7. Контекстное меню значка программы при отображении упрощенного интерфейса программы

Настройка отображения интерфейса программы

Вы можете настроить отображение интерфейса программы для пользователя компьютера. Пользователь может взаимодействовать с программой следующими способами:

- **С упрощенным интерфейсом**. На клиентском компьютере недоступно главное окно программы, а доступен только значок в области уведомлений Windows (см. раздел "Значок программы в области уведомлений" на стр. 43). В контекстном меню значка пользователь может выполнять ограниченный список операций с Kaspersky Endpoint Security (см. раздел "Упрощенный интерфейс программы" на стр. 44). Также Kaspersky Endpoint Security показывает уведомления над значком программы.
- **С полным интерфейсом**. На клиентском компьютере доступно главное окно Kaspersky Endpoint Security и значок в области уведомлений Windows (см. раздел "Значок программы в области уведомлений" на стр. 43). В контекстном меню значка пользователь может выполнять операции с Kaspersky Endpoint Security. Также Kaspersky Endpoint Security показывает уведомления над значком программы.
- **Без интерфейса**. На клиентском компьютере не отображается никаких признаков работы Kaspersky Endpoint Security. Также недоступны значок в области уведомлений Windows (см. раздел "Значок программы в области уведомлений" на стр. 43) и уведомления.

Как настроить отображение интерфейса программы в Консоли администрирования (MMC):

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева Консоли администрирования откройте папку с названием группы администрирования, в состав которой входят нужные клиентские компьютеры.
3. В рабочей области выберите закладку **Политики**.
4. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
5. В окне политики выберите **Общие настройки** → **Интерфейс**.
6. В блоке **Взаимодействие с пользователем** выполните одно из следующих действий:
   - Установите флажок **Отображать интерфейс программы**, если вы хотите, чтобы на клиентском компьютере отображались следующие элементы интерфейса:
     - папка с названием программы в меню **Пуск**;
     - значок Kaspersky Endpoint Security (см. раздел "Значок программы в области уведомлений" на стр. 43) в области уведомлений панели задач Microsoft Windows;
     - всплывающие уведомления.

Если установлен этот флажок, пользователь может просматривать и, при наличии прав, изменять параметры программы из интерфейса программы.

- Снимите флажок **Отображать интерфейс программы**, если вы хотите скрыть все признаки работы Kaspersky Endpoint Security на клиентском компьютере.

7. В блоке **Взаимодействие с пользователем** установите флажок **Упрощенный интерфейс программы**, если вы хотите, чтобы на клиентском компьютере с установленной программой Kaspersky Endpoint Security отображался упрощенный интерфейс программы (на стр. 44).

Как настроить отображение интерфейса программы в Web Console и Cloud Console:

1. В главном окне Web Console выберите **Устройства** → **Политики и профили политик**.
2. Нажмите на название политики Kaspersky Endpoint Security для компьютеров, на которых вы хотите включить поддержку портативного режима.

   Откроется окно свойств политики.
3. Выберите закладку **Параметры программы**.
4. Перейдите в раздел **Общие настройки** → **Интерфейс**.
5. В блоке **Взаимодействие с пользователем** настройте отображение интерфейса программы:

   - **С упрощенным интерфейсом**. На клиентском компьютере недоступно главное окно программы, а доступен только значок в области уведомлений Windows (см. раздел "Значок программы в области уведомлений" на стр. 43). В контекстном меню значка пользователь может выполнять ограниченный список операций с Kaspersky Endpoint Security (см. раздел "Упрощенный интерфейс программы" на стр. 44). Также Kaspersky Endpoint Security показывает уведомления над значком программы.
   - **С полным интерфейсом**. На клиентском компьютере доступно главное окно Kaspersky Endpoint Security и значок в области уведомлений Windows (см. раздел "Значок программы в области уведомлений" на стр. 43). В контекстном меню значка пользователь может выполнять операции с Kaspersky Endpoint Security. Также Kaspersky Endpoint Security показывает уведомления над значком программы.
   - **Без интерфейса**. На клиентском компьютере не отображается никаких признаков работы Kaspersky Endpoint Security. Также недоступны значок в области уведомлений Windows (см. раздел "Значок программы в области уведомлений" на стр. 43) и уведомления.
6. Нажмите на кнопку **ОК**.

kaspersky

Запуск и остановка Kaspersky Endpoint Security

После установки Kaspersky Endpoint Security на компьютер пользователя запуск программы выполняется автоматически. Далее по умолчанию запуск Kaspersky Endpoint Security выполняется сразу после операционной системы. Настроить автоматический запуск программы в параметрах операционной системы невозможно.

Загрузка антивирусных баз Kaspersky Endpoint Security после загрузки операционной системы занимает до двух минут, в зависимости от производительности (технических возможностей) компьютера. В течение этого времени уровень защиты компьютера снижен. Загрузка антивирусных баз при запуске программы Kaspersky Endpoint Security в уже запущенной операционной системе не вызывает снижения уровня защиты компьютера.

Как настроить запуск Kaspersky Endpoint Security в Консоли администрирования (MMC):

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева Консоли администрирования откройте папку с названием группы администрирования, в состав которой входят нужные клиентские компьютеры.
3. В рабочей области выберите закладку **Политики**.
4. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
5. В окне политики выберите **Общие настройки** → **Настройки программы**.
6. С помощью флажка **Запускать Kaspersky Endpoint Security для Windows при включении компьютера** настройте запуск программы.
7. Сохраните внесенные изменения.

Как настроить запуск Kaspersky Endpoint Security в Web Console:

1. В главном окне Web Console выберите **Устройства** → **Политики и профили политик**.
2. Нажмите на название политики Kaspersky Endpoint Security для компьютеров, на которых вы хотите настроить запуск программы.

   Откроется окно свойств политики.
3. Выберите закладку **Параметры программы**.
4. Выберите раздел **Общие настройки**.
5. Перейдите по ссылке **Настройки программы**.
6. С помощью флажка **Запускать Kaspersky Endpoint Security для Windows при включении компьютера** настройте запуск программы.
7. Нажмите на кнопку **ОК**.
8. Подтвердите изменения по кнопке **Сохранить**.

Как настроить запуск Kaspersky Endpoint Security в интерфейсе программы:

1. В нижней части главного окна программы нажмите на кнопку .
2. В окне параметров программы выберите раздел **Общие**.
3. С помощью флажка **Запускать при включении компьютера** настройте запуск программы.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Специалисты "Лаборатории Касперского" рекомендуют не завершать работу Kaspersky Endpoint Security, поскольку в этом случае защита компьютера и ваших данных окажется под угрозой. Если требуется, вы можете приостановить защиту компьютера (см. раздел "Приостановка и возобновление защиты и контроля компьютера" на стр. 50) на необходимый срок, не завершая работу программы.

Вы можете контролировать статус работы программы с помощью виджета **Состояние защиты**.

Как запустить или остановить Kaspersky Endpoint Security в Консоли администрирования (MMC):

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева Консоли администрирования откройте папку с названием группы администрирования, в состав которой входит нужный вам клиентский компьютер.
3. В рабочей области выберите закладку **Устройства**.
4. Выберите компьютер, на котором вы хотите запустить или остановить программу.
5. По правой клавише мыши откройте контекстное меню клиентского компьютера и выберите пункт **Свойства**.
6. В окне свойств клиентского компьютера выберите раздел **Программы**.

   Справа в окне свойств клиентского компьютера отобразится список программ "Лаборатории Касперского", установленных на клиентском компьютере.
7. Выберите программу Kaspersky Endpoint Security.
8. Выполните следующие действия:
   - Если вы хотите запустить программу, справа от списка программ "Лаборатории Касперского" нажмите на кнопку .
   - Если вы хотите остановить работу программы, справа от списка программ "Лаборатории Касперского" нажмите на кнопку .

Как запустить или остановить Kaspersky Endpoint Security в Web Console:

1. В главном окне Web Console выберите **Устройства** → **Управляемые устройства**.
2. Нажмите на имя компьютера, на котором вы хотите запустить или остановить Kaspersky Endpoint Security.

   Откроется окно свойств компьютера.
3. Выберите закладку **Программы**.
4. Установите флажок напротив программы **Kaspersky Endpoint Security для Windows**.
5. Нажмите на кнопку **Запустить** или **Остановить**.

Для завершения работы программы из командной строки необходимо выключить внешнее управление системными службами (см. раздел "Включение и выключение защиты от внешнего управления" на стр. 216).

Для запуска или завершения работы программы из командной строки используется файл klpsm.exe, входящий в комплект поставки Kaspersky Endpoint Security.

1. Запустите интерпретатор командной строки cmd от имени администратора.
2. Перейдите в папку, в которой расположен исполняемый файл Kaspersky Endpoint Security.
3. Для запуска программы в командной строке введите `klpsm.exe start_avp_service`.
4. Для остановки программы в командной строке введите `klpsm.exe stop_avp_service`.

kaspersky

Приостановка и возобновление защиты и контроля компьютера

Приостановка защиты и контроля компьютера означает выключение на некоторое время всех компонентов защиты и всех компонентов контроля Kaspersky Endpoint Security.

Состояние программы отображается с помощью значка программы в области уведомлений панели задач (см. раздел «Значок программы в области уведомлений» на стр. 43):

- значок свидетельствует о приостановке защиты и контроля компьютера;
- значок свидетельствует о том, что защита и контроль компьютера включены.

Приостановка и возобновление защиты и контроля компьютера не оказывает влияния на выполнение задач проверки и задачи обновления.

Если в момент приостановки и возобновления защиты и контроля компьютера были установлены сетевые соединения, на экран выводится уведомление о разрыве этих сетевых соединений.

► *Чтобы приостановить защиту и контроль компьютера, выполните следующие действия:*

1. По правой клавише мыши откройте контекстное меню значка программы, который расположен в области уведомлений панели задач.
2. В контекстном меню выберите пункт **Приостановить защиту** (см. рисунок ниже).

   Этот пункт контекстного меню доступен, если включена Защита паролем (см. раздел "Включение Защиты паролем" на стр. 192).
3. Выберите один из следующих вариантов:
   - **Приостановить на <период времени>** – защита и контроль компьютера включатся через интервал времени, указанный в раскрывающемся списке ниже.
   - **Приостановить до перезагрузки программы** – защита и контроль компьютера включатся после перезапуска программы или перезагрузки операционной системы. Для использования этой возможности должен быть включен автоматический запуск программы.
   - **Приостановить** – защита и контроль компьютера включатся тогда, когда вы решите возобновить их.
4. Нажмите на кнопку **Приостановить защиту**.

Kaspersky Endpoint Security приостановит работу всех компонентов защиты и контроля, не отмеченных в политике замком ( ). Перед выполнением этой операции рекомендуется выключить политику Kaspersky Security Center.

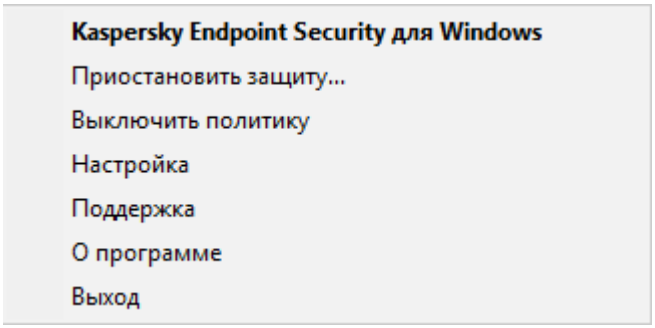


Рисунок 8. Контекстное меню значка программы

► *Чтобы возобновить защиту и контроль компьютера, выполните следующие действия:*

1. По правой клавише мыши откройте контекстное меню значка программы, который расположен в области уведомлений панели задач.
2. В контекстном меню выберите пункт **Возобновить защиту**.

Вы можете возобновить защиту и контроль компьютера в любой момент, независимо от того, какой вариант приостановки защиты и контроля компьютера вы выбрали ранее.

kaspersky

Проверка компьютера

Антивирусная проверка является важным фактором для обеспечения безопасности компьютера. Требуется регулярно выполнять антивирусную проверку, чтобы исключить возможность распространения вредоносных программ, которые не были обнаружены компонентами защиты, например, из-за установленного низкого уровня защиты или по другим причинам.

Kaspersky Endpoint Security не проверяет файлы, содержимое которых расположено в облачном хранилище OneDrive, и создает в журнале записи о том, что эти файлы не были проверены.

Полная проверка

Тщательная проверка всей системы. Kaspersky Endpoint Security проверяет следующие объекты:

- память ядра;
- объекты, загрузка которых осуществляется при запуске операционной системы;
- загрузочные секторы;
- резервное хранилище операционной системы;
- все жесткие и съемные диски.

Специалисты "Лаборатории Касперского" рекомендуют не изменять область проверки задачи *Полная проверка*.
Для экономии ресурсов компьютера рекомендуется вместо задачи полной проверки запускать задачу фоновой проверки. Уровень защиты компьютера при этом не изменится.

Проверка важных областей

По умолчанию Kaspersky Endpoint Security проверяет память ядра, запущенные процессы и загрузочные секторы.

Специалисты "Лаборатории Касперского" рекомендуют не изменять область проверки задачи *Проверка важных областей*.

Выборочная проверка

Kaspersky Endpoint Security проверяет объекты, выбранные пользователем. Вы можете проверить любой объект из следующего списка:

- память ядра;
- объекты, загрузка которых осуществляется при запуске операционной системы;
- резервное хранилище операционной системы;
- почтовый ящик Microsoft Outlook;
- жесткие, съемные и сетевые диски;
- любой выбранный файл.

kaspersky

Фоновая проверка

Фоновая проверка – это режим проверки Kaspersky Endpoint Security без отображения уведомлений для пользователя. Фоновая проверка требует меньше ресурсов компьютера, чем другие виды проверок (например, полная проверка). В этом режиме Kaspersky Endpoint Security проверяет объекты автозапуска, памяти ядра и системного раздела.

Проверка целостности

Kaspersky Endpoint Security проверяет модули программы на наличие повреждений или изменений.

В этом разделе

Запуск и остановка задачи проверки

Независимо от выбранного режима запуска задачи проверки вы можете запустить или остановить задачу проверки в любой момент.

► *Чтобы запустить или остановить задачу проверки, выполните следующие действия:*

1. В главном окне программы нажмите на кнопку **Задачи**.
2. Нажмите на кнопку **Запустить проверку**, если вы хотите запустить задачу проверки.

Kaspersky Endpoint Security запустит проверку компьютера. Программа покажет процесс проверки, количество проверенных файлов и оставшиеся время. Вы можете остановить выполнение задачи в любое время по кнопке **Остановить**.

► *Чтобы запустить или остановить задачу проверки при отображении упрощенного интерфейса программы, выполните следующие действия:*

1. По правой клавише мыши откройте контекстное меню значка программы, который расположен в области уведомлений панели задач.
2. В контекстном меню в раскрывающемся списке **Задачи** выполните одно из следующих действий:
   - выберите незапущенную задачу проверки, чтобы запустить ее;
   - выберите запущенную задачу проверки, чтобы остановить ее;
   - выберите остановленную задачу проверки, чтобы возобновить ее или запустить ее заново.

Изменение уровня безопасности

Для проверки Kaspersky Endpoint Security применяет разные наборы настроек. Наборы настроек, сохраненные в программе, называются *уровнями безопасности*: **Высокий**, **Рекомендуемый**, **Низкий**. Параметры уровня безопасности **Рекомендуемый** считаются оптимальными. Они рекомендованы специалистами "Лаборатории Касперского". Вы можете выбрать один из предустановленных уровней безопасности или настроить параметры уровня безопасности самостоятельно. После того как вы изменили параметры уровня безопасности, вы всегда можете вернуться к рекомендуемым параметрам уровня безопасности.

► *Чтобы изменить уровень безопасности, выполните следующие действия:*

1. В главном окне программы нажмите на кнопку **Задачи**.
2. В открывшемся окне выберите задачу проверки и нажмите на кнопку ⚙.
3. В блоке **Уровень безопасности** выполните одно из следующих действий:
   - Если вы хотите применить один из предустановленных уровней безопасности, выберите его при помощи ползунка:
     - **Высокий**. Kaspersky Endpoint Security проверяет файлы всех типов. Во время проверки составных файлов Kaspersky Endpoint Security дополнительно проверяет файлы почтовых форматов.
     - **Рекомендуемый**. Kaspersky Endpoint Security проверяет только файлы определенных форматов на всех жестких, сменных и сетевых дисках компьютера, а также вложенные OLE-объекты. Kaspersky Endpoint Security не проверяет архивы и установочные пакеты.
     - **Низкий**. Kaspersky Endpoint Security проверяет только новые и измененные файлы с определенными расширениями на всех жестких, сменных и сетевых дисках компьютера. Kaspersky Endpoint Security не проверяет составные файлы.
   - Если вы хотите настроить уровень безопасности самостоятельно, нажмите на кнопку **Расширенная настройка** и задайте параметры работы компонента.

     Вы можете восстановить значения предустановленных уровней безопасности по кнопке **Восстановить рекомендуемый уровень безопасности** в верхней части окна.
4. Сохраните внесенные изменения.

kaspersky

Изменение действия над зараженными файлами

По умолчанию при обнаружении зараженных файлов Kaspersky Endpoint Security пытается вылечить их или удаляет их, если лечение невозможно.

► *Чтобы изменить действие над зараженными файлами, выполните следующие действия:*

1. В главном окне программы нажмите на кнопку **Задачи**.
2. В открывшемся окне выберите задачу проверки и нажмите на кнопку ⚙.
3. В блоке **Действие при обнаружении угрозы** выберите один из следующих вариантов:
   - **Лечить; удалять, если лечение невозможно**. Если выбран этот вариант действия, то Kaspersky Endpoint Security автоматически пытается вылечить все обнаруженные зараженные файлы. Если лечение невозможно, то Kaspersky Endpoint Security их удаляет.
   - **Лечить; блокировать, если лечение невозможно**. Если выбран этот вариант действия, то Kaspersky Endpoint Security автоматически пытается вылечить все обнаруженные зараженные файлы. Если лечение невозможно, то Kaspersky Endpoint Security добавляет информацию об обнаруженных зараженных файлах в список активных угроз.
   - **Информировать**. Если выбран этот вариант действия, то при обнаружении зараженных файлов Kaspersky Endpoint Security добавляет информацию об этих файлах в список активных угроз.

   Перед лечением или удалением зараженного файла Kaspersky Endpoint Security формирует его резервную копию на тот случай, если впоследствии понадобится восстановить файл или появится возможность его вылечить (см. раздел "Восстановление файлов из резервного хранилища" на стр. 205).
   При обнаружении зараженных файлов, являющихся частью приложения Windows Store, Kaspersky Endpoint Security пытается удалить файл.
4. Сохраните внесенные изменения.

Формирование списка проверяемых объектов

► *Чтобы сформировать список проверяемых объектов, выполните следующие действия:*

1. В главном окне программы нажмите на кнопку **Задачи**.
2. В открывшемся окне выберите задачу проверки и нажмите на кнопку ⚙.
3. Перейдите по ссылке **Изменить область проверки**.
4. В открывшемся окне выберите объекты, которые вы хотите добавить в область проверки или исключить из нее.

   Вы не можете удалить или изменить объекты, включенные в область проверки по умолчанию.

5. Если вы хотите добавить новый объект в область проверки, выполните следующие действия:
   a. Нажмите на кнопку **Добавить**.

      Откроется дерево папок.

   b. Выберите объект и нажмите на кнопку **Выбрать**.

   Вы можете исключить объект из проверки, не удаляя его из списка объектов области проверки. Для этого снимите флажок рядом с ним.
6. Сохраните внесенные изменения.

Выбор типа проверяемых файлов

Выбирая тип проверяемых файлов, нужно учитывать следующее:

1. Вероятность внедрения вредоносного кода в файлы некоторых форматов и его последующей активации низка (например, формат TXT). В то же время существуют форматы файлов, которые содержат исполняемый код (например, форматы EXE, DLL). Также исполняемый код могут содержать форматы файлов, которые для этого не предназначены (например, формат DOC). Риск внедрения в такие файлы вредоносного кода и его активации высок.
2. Злоумышленник может отправить вирус или другую программу, представляющую угрозу, на ваш компьютер в исполняемом файле, переименованном в файл с расширением txt. Если вы выбрали проверку файлов по расширению, то в процессе проверки программа пропускает такой файл. Если же выбрана проверка файлов по формату, то вне зависимости от расширения Kaspersky Endpoint Security анализирует заголовок файла. Если в результате выясняется, что файл имеет формат исполняемого файла (например, EXE), то программа проверяет его.

► *Чтобы выбрать тип проверяемых файлов выполните следующие действия:*

1. В главном окне программы нажмите на кнопку **Задачи**.
2. В открывшемся окне выберите задачу проверки и нажмите на кнопку ⚙.
3. Нажмите на кнопку **Расширенная настройка**.
4. В блоке **Типы файлов** укажите тип файлов, которые вы хотите проверять во время выполнения выбранной задачи проверки:
   - **Все файлы**. Если выбран этот параметр, Kaspersky Endpoint Security проверяет все файлы без исключения (любых форматов и расширений).
   - **Файлы, проверяемые по формату**. Если выбран этот параметр, Kaspersky Endpoint Security проверяет только потенциально заражаемые файлы. Перед началом поиска вредоносного кода в файле выполняется анализ его внутреннего заголовка на предмет формата файла (например, TXT, DOC, EXE). В процессе проверки учитывается также расширение файла.
   - **Файлы, проверяемые по расширению**. Если выбран этот параметр, Kaspersky Endpoint Security проверяет только потенциально заражаемые файлы. Формат файла определяется на основании его расширения.

> Файлы без расширения Kaspersky Endpoint Security считает исполняемыми. Kaspersky Endpoint Security проверяет исполняемые файлы всегда, независимо от того, файлы какого типа вы выбрали для проверки.

5. Сохраните внесенные изменения.

Оптимизация проверки файлов

Вы можете оптимизировать проверку файлов: сократить время проверки и увеличить скорость работы Kaspersky Endpoint Security. Этого можно достичь, если проверять только новые файлы и те файлы, что изменились с момента их предыдущего анализа. Такой режим проверки распространяется как на простые, так и на составные файлы. Вы можете также ограничить длительность проверки одного файла. По истечении заданного времени Kaspersky Endpoint Security исключает файл из текущей проверки (кроме архивов и объектов, в состав которых входит несколько файлов).

Вы также можете включить использование технологий iChecker и iSwift (см. раздел "Использование технологий проверки" на стр. 59). Технологии iChecker и iSwift позволяют оптимизировать скорость проверки файлов за счет исключения из проверки файлов, не измененных с момента их последней проверки.

► *Чтобы оптимизировать проверку файлов, выполните следующие действия:*

1. В главном окне программы нажмите на кнопку **Задачи**.
2. В открывшемся окне выберите задачу проверки и нажмите на кнопку ⚙.
3. Нажмите на кнопку **Расширенная настройка**.
4. В блоке **Оптимизация проверки** настройте параметры проверки:
   - **Проверять только новые и измененные файлы**. Проверка только новых файлов и тех файлов, которые изменились после предыдущей проверки. Это позволит сократить время выполнения проверки. Такой режим проверки распространяется как на простые, так и на составные файлы.
   - **Пропускать файлы, если их проверка длится более N секунд**. Ограничение длительности проверки одного объекта. По истечении заданного времени Kaspersky Endpoint Security прекращает проверку файла. Это позволит сократить время выполнения проверки.
5. Сохраните внесенные изменения.

Проверка составных файлов

Распространенной практикой сокрытия вирусов и других программ, представляющих угрозу, является внедрение их в составные файлы, например, архивы или базы данных. Чтобы обнаружить скрытые таким образом вирусы и другие программы, представляющие угрозу, составной файл нужно распаковать, что может привести к снижению скорости проверки. Вы можете ограничить типы проверяемых составных файлов, таким образом увеличив скорость проверки.

► *Чтобы настроить проверку составных файлов, выполните следующие действия:*

1. В главном окне программы нажмите на кнопку **Задачи**.
2. В открывшемся окне выберите задачу проверки и нажмите на кнопку ⚙.
3. Нажмите на кнопку **Расширенная настройка**.
4. В блоке **Проверка составных файлов** укажите, какие составные файлы вы хотите проверять: архивы, установочные пакеты, файлы офисных форматов, файлы почтовых форматов, защищенные паролем архивы.
5. Если режим проверки только новых и измененных файлов выключен (см. раздел "Оптимизация проверки файлов" на стр. 57), настройте параметры проверки каждого типа составных файлов: проверка всех файлов этого типа или только новых файлов.

   Если режим проверки только новых и измененных файлов включен, Kaspersky Endpoint Security проверяет только новые и измененные файлы всех типов составных файлов.
6. В блоке **Ограничение по размеру**, выполните одно из следующих действий:
   - Если вы не хотите распаковывать составные файлы большого размера, установите флажок **Не распаковывать составные файлы большого размера** и в поле **Максимальный размер файла** укажите нужное значение.
   - Если вы хотите распаковывать составные файлы независимо от размера, снимите флажок **Не распаковывать составные файлы большого размера**.

   Kaspersky Endpoint Security проверяет файлы больших размеров, извлеченные из архивов, независимо от того, установлен ли флажок **Не распаковывать составные файлы большого размера**.
7. Сохраните внесенные изменения.

Использование методов проверки

Во время своей работы Kaspersky Endpoint Security использует метод проверки Машинное обучение и сигнатурный анализ. В процессе сигнатурного анализа Kaspersky Endpoint Security сравнивает найденный объект с записями в базах программы. В соответствии с рекомендациями специалистов "Лаборатории Касперского" метод проверки Машинное обучение и сигнатурный анализ всегда включен.

Чтобы повысить эффективность защиты, вы можете использовать эвристический анализ. Во время проверки файлов на наличие вредоносного кода эвристический анализатор выполняет инструкции в исполняемых файлах. Количество инструкций, которые выполняет эвристический анализатор, зависит от заданного уровня эвристического анализа. Уровень эвристического анализа обеспечивает баланс между тщательностью поиска новых угроз, степенью загрузки ресурсов операционной системы и длительностью эвристического анализа.

► *Чтобы использовать методы проверки, выполните следующие действия:*

1. В главном окне программы нажмите на кнопку **Задачи**.
2. В открывшемся окне выберите задачу проверки и нажмите на кнопку ⚙.
3. Нажмите на кнопку **Расширенная настройка**.

4. В блоке **Методы проверки** установите флажок **Эвристический анализ**, если вы хотите, чтобы программа использовала эвристический анализ во время выполнения задачи проверки. Далее при помощи ползунка задайте уровень эвристического анализа: **Поверхностный**, **Средний** или **Глубокий**.
5. Сохраните внесенные изменения.

Использование технологий проверки

► *Чтобы использовать технологии проверки, выполните следующие действия:*

1. В главном окне программы нажмите на кнопку **Задачи**.
2. В открывшемся окне выберите задачу проверки и нажмите на кнопку ⚙.
3. Нажмите на кнопку **Расширенная настройка**.
4. В блоке **Технологии проверки** установите флажки около названий технологий, которые вы хотите использовать во время проверки:
   - **Технология iSwift**. Технология, позволяющая увеличить скорость проверки за счет исключения из нее некоторых файлов. Файлы исключаются из проверки по специальному алгоритму, учитывающему дату выпуска баз Kaspersky Endpoint Security, дату предыдущей проверки файла, а также изменение параметров проверки. Технология iSwift является развитием технологии iChecker для файловой системы NTFS.
   - **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 Endpoint Security, 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).
5. Сохраните внесенные изменения.

Выбор режима запуска для задачи проверки

Если по каким-либо причинам запуск задачи проверки невозможен (например, в это время компьютер выключен), вы можете настроить автоматический запуск пропущенной задачи проверки, как только это станет возможным.

Вы можете отложить запуск задачи проверки после старта программы для случаев, если вы выбрали режим запуска задачи проверки **По расписанию** и время запуска Kaspersky Endpoint Security совпадает с расписанием запуска задачи проверки. Задача проверки запускается только по истечении указанного времени после старта Kaspersky Endpoint Security.

► *Чтобы выбрать режим запуска для задачи проверки, выполните следующие действия:*

1. В главном окне программы нажмите на кнопку **Задачи**.
2. В открывшемся окне выберите задачу проверки и нажмите на кнопку ⚙.

3. Нажмите на кнопку **Расписание проверки**.
4. В открывшемся окне настройте расписание запуска задачи проверки.
5. В зависимости от выбранной периодичности настройте дополнительные параметры, которые уточняют расписание запуска задачи.
   a. Установите флажок **Запускать пропущенные задачи**, если вы хотите, чтобы Kaspersky Endpoint Security запускал при первой возможности не запущенные вовремя задачи проверки.

      Если в раскрывающемся списке **Периодичность** выбран элемент **Минуты**, **Часы**, **После запуска программы** или **После каждого обновления**, то флажок **Запускать пропущенные задачи** недоступен.

   b. Установите флажок **Выполнять только во время простоя компьютера**, если вы хотите, чтобы Kaspersky Endpoint Security приостанавливал задачу, когда ресурсы компьютера заняты. Kaspersky Endpoint Security запускает задачу проверки, если компьютер заблокирован или включена экранная заставка.

      Этот вариант расписания позволяет экономить вычислительную мощность компьютера во время работы.
6. Сохраните внесенные изменения.

Настройка запуска задачи проверки с правами другого пользователя

По умолчанию задача проверки запускается с правами учетной записи, под которой пользователь зарегистрирован в операционной системе. Однако может возникнуть необходимость запустить задачу проверки с правами другого пользователя. Вы можете указать пользователя, обладающего этими правами, в параметрах задачи проверки и запускать задачу проверки от имени этого пользователя.

► *Чтобы настроить запуск задачи проверки с правами другого пользователя, выполните следующие действия:*

1. В главном окне программы нажмите на кнопку **Задачи**.
2. В открывшемся окне выберите задачу проверки и нажмите на кнопку ⚙.
3. Нажмите на кнопку **Расширенная настройка** → **Запускать проверку с правами**.
4. В открывшемся окне выберите пользователя, права которого требуется использовать для запуска задачи проверки.
5. Сохраните внесенные изменения.

kaspersky

Проверка съемных дисков при подключении к компьютеру

Некоторые вредоносные программы используют уязвимости операционной системы для распространения через локальные сети и съемные диски. Kaspersky Endpoint Security позволяет проверять на вирусы и другие программы, представляющие угрозу, съемные диски при их подключении к компьютеру.

► *Чтобы настроить проверку съемных дисков при их подключении к компьютеру, выполните следующие действия:*

1. В главном окне программы нажмите на кнопку **Задачи**.
2. В открывшемся окне выберите задачу проверки съемных дисков и нажмите на кнопку .
3. Используйте переключатель **Проверка съемных дисков**, чтобы включить или выключить проверку съемных дисков при подключении к компьютеру.
4. Выберите режим проверки съемных дисков при подключении к компьютеру:
   - **Подробная проверка**. Если выбран этот вариант, то после подключения съемного диска Kaspersky Endpoint Security проверяет все файлы, расположенные на съемном диске, в том числе вложенные файлы внутри составных объектов.
   - **Быстрая проверка**. Если выбран этот вариант, то после подключения съемного диска Kaspersky Endpoint Security проверяет только файлы определенных форматов (см. раздел "Приложение 3. Расширения файлов для быстрой проверки съемных дисков" на стр. 280), наиболее подверженные заражению, а также не распаковывает составные объекты.
5. Если вы хотите, чтобы Kaspersky Endpoint Security проверял только те съемные диски, размер которых не превышает указанного значения, установите флажок **Максимальный размер съемного диска** и укажите в соседнем поле значение в мегабайтах.
6. Настройте отображение хода проверки съемного диска. Выполните одно из следующих действий:
   - Если вы хотите, чтобы программа Kaspersky Endpoint Security отображала ход проверки съемных дисков в отдельном окне, установите флажок **Отображать ход проверки**.

     В окне проверки съемного диска пользователь может остановить проверку. Чтобы сделать проверку съемных дисков обязательной и запретить пользователю останавливать проверку, установите флажок **Запретить остановку задачи проверки**.
   - Если вы хотите, чтобы программа Kaspersky Endpoint Security запускала проверку съемных дисков в фоновом режиме, снимите флажок **Отображать ход проверки**.
7. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

kaspersky

Фоновая проверка

Фоновая проверка – это режим проверки Kaspersky Endpoint Security без отображения уведомлений для пользователя. Фоновая проверка требует меньше ресурсов компьютера, чем другие виды проверок (например, полная проверка). В этом режиме Kaspersky Endpoint Security проверяет объекты автозапуска, памяти ядра и системного раздела. Фоновая проверка запускается в следующих случаях:

- после обновления антивирусных баз;
- через 30 минут после запуска Kaspersky Endpoint Security;
- каждые шесть часов;
- при простое компьютера в течение пяти и более минут (компьютер заблокирован или включена экранная заставка).

Фоновая проверка при простое компьютера прерывается при выполнении любого из следующих условий:

- Компьютер перешел в активный режим.

  Если фоновая проверка не выполнялась более десяти дней, проверка не прерывается.

- Компьютер (ноутбук) перешел в режим питания от батареи.

При выполнении фоновой проверки Kaspersky Endpoint Security не проверяет файлы, содержимое которых расположено в облачном хранилище OneDrive.

► *Чтобы включить фоновую проверку компьютера, выполните следующие действия:*

1. В главном окне программы нажмите на кнопку **Задачи**.
2. В открывшемся окне выберите задачу проверки и нажмите на кнопку ⚙.
3. Используйте переключатель **Фоновая проверка**, чтобы включить или выключить фоновую проверку.
4. Сохраните внесенные изменения.

Проверка целостности программы

Kaspersky Endpoint Security проверяет файлы программы, находящиеся в папке установки программы, на наличие повреждений или изменений. Например, если библиотека программы имеет некорректную цифровую подпись, то такая библиотека считается поврежденной. Для проверки файлов программы предназначена задача *Проверка целостности*. Запускайте задачу *Проверка целостности*, если программа Kaspersky Endpoint Security обнаружила вредоносный объект и не обезвредила его.

Вы можете создать задачу *Проверка целостности* в Kaspersky Security Center 12 Web Console и Консоли администрирования. Создать задачу в программе Kaspersky Security Center Cloud Console невозможно.

Как выполнить проверку целостности программы через Консоль администрирования (MMC):

1. В Консоли администрирования перейдите в папку **Сервер администрирования → Задачи**.

   Откроется список задач.

2. Нажмите на кнопку **Новая задача**.

Запустится мастер создания задачи. Следуйте его указаниям.

Шаг 1. Выбор типа задачи

Выберите **Kaspersky Endpoint Security для Windows (11.6.0) → Проверка целостности**.

Шаг 2. Выбор устройств, которым будет назначена задача

Выберите компьютеры, на которых будет выполнена задача. Доступны следующие способы:

- Назначить задачу группе администрирования. В этом случае задача назначается компьютерам, входящим в ранее созданную группу администрирования.
- Выбрать компьютеры, обнаруженные в сети Сервером администрирования, – *нераспределенные устройства*. В набор устройств вы можете включать как устройства в группах администрирования, так и нераспределенные устройства.
- Задать адреса устройств вручную или импортировать из списка. Вы можете задавать NetBIOS-имена, IP-адреса, а также диапазоны IP-адресов устройств, которым нужно назначить задачу.

Шаг 3. Настройка расписания запуска задачи

Настройте расписание запуска задачи, например, вручную или при обнаружении вирусной атаки.

Шаг 4. Определение названия задачи

Введите название задачи, например, `Проверка целостности программы после заражения компьютера`.

Шаг 5. Завершение создания задачи

Завершите работу мастера. Если требуется, установите флажок **Запустить задачу после завершения работы мастера**. Вы можете следить за ходом выполнения задачи в свойствах задачи. В результате Kaspersky Endpoint Security выполнит проверку целостности программы. Вы также можете настроить расписание проверки целостности программы в свойствах задачи.

Нарушения целостности программы могут, например, возникать в следующих случаях:

- Вредоносный объект внес изменения в файлы Kaspersky Endpoint Security. В этом случае выполните процедуру восстановления Kaspersky Endpoint Security средствами операционной системы. После восстановления запустите полную проверку компьютера и повторите проверку целостности.
- Истек срок действия цифровой подписи. В этом случае обновите Kaspersky Endpoint Security.

kaspersky

Работа с активными угрозами

Программа Kaspersky Endpoint Security фиксирует информацию о файлах, которые она по каким-либо причинам не обработала. Эта информация записывается в виде событий в список активных угроз.

Зараженный файл считается *обработанным*, если Kaspersky Endpoint Security в процессе проверки компьютера на вирусы и другие программы, представляющие угрозу, совершил одно из следующих действий с этим файлом согласно заданным настройкам программы:

- Лечить.
- Удалять.
- Удалять, если лечение невозможно.

Kaspersky Endpoint Security помещает файл в список активных угроз, если в процессе проверки компьютера на вирусы и другие программы, представляющие угрозу, Kaspersky Endpoint Security по каким-либо причинам не совершил действие с этим файлом согласно заданным настройкам программы.

Такая ситуация возможна в следующих случаях:

- Проверяемый файл недоступен (например, находится на сетевом диске или внешнем диске без прав на запись данных).
- В настройках программы для задач проверки в блоке **Действие при обнаружении угрозы** выбрано действие **Информировать**, и когда на экране отобразилось уведомление о зараженном файле, пользователь выбрал вариант **Пропустить**.

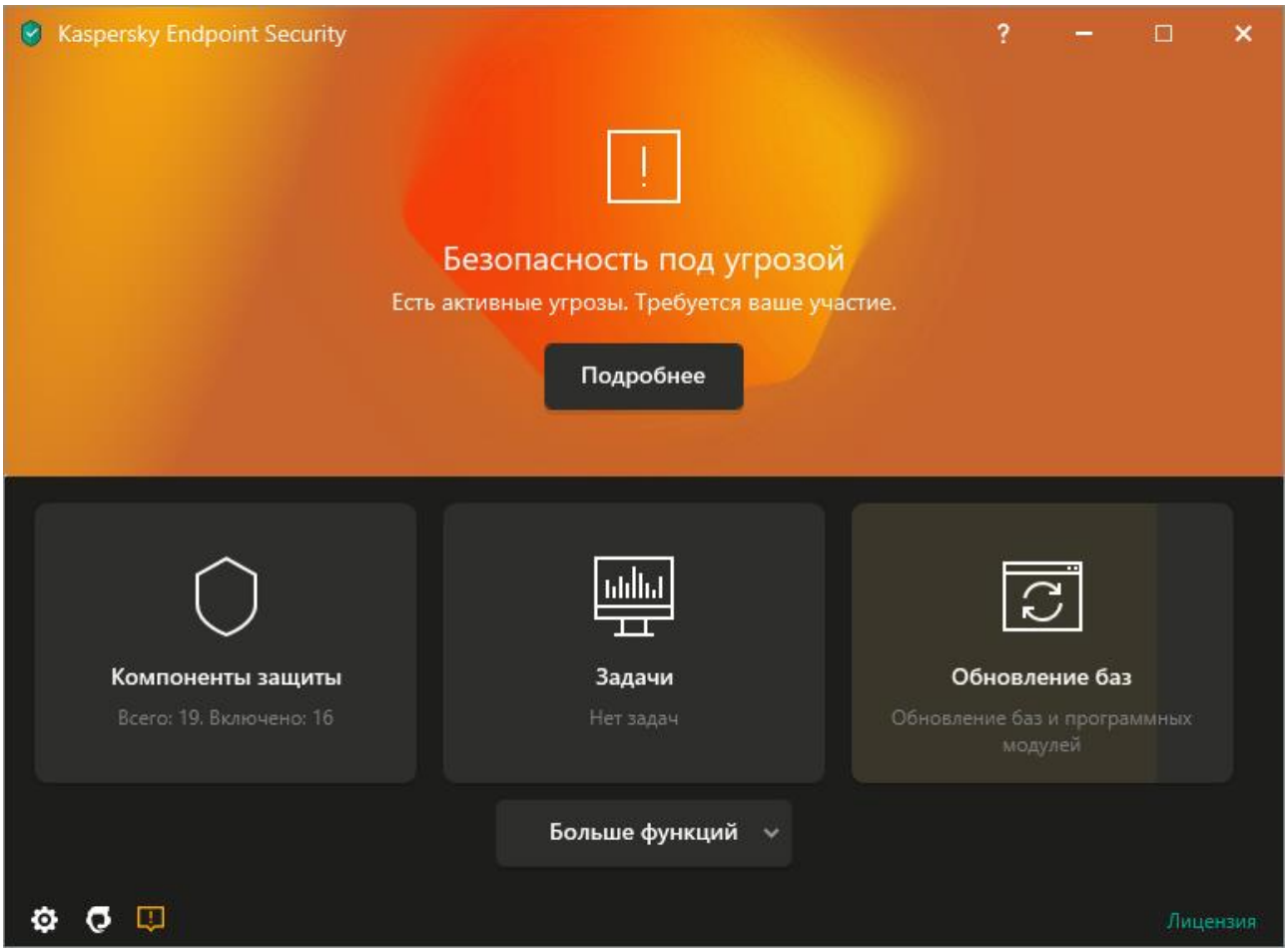


Рисунок 9. Главное окно программы при обнаружении угрозы

► *Чтобы обработать активные угрозы, выполните следующие действия:*

1. В главном окне программы нажмите на кнопку **Подробнее**.

   Откроется список активных угроз.

2. Выберите объект, который вы хотите устранить.
3. Выберите способ устранения угрозы:

   - **Устранить**. Если выбран этот вариант действия, то Kaspersky Endpoint Security автоматически пытается вылечить все обнаруженные зараженные файлы. Если лечение невозможно, то Kaspersky Endpoint Security их удаляет.
   - **Игнорировать**. Если выбран этот вариант действия, то Kaspersky Endpoint Security удалить запись из списка активных угроз. Если в списке не осталось активных угроз, статус компьютера будет изменен на *ОК*. При повторном обнаружении объекта Kaspersky Endpoint Security снова добавит запись в список активных угроз.

- **Открыть папку с файлом**. Если выбран этот вариант действия, то Kaspersky Endpoint Security откроет папку с объектом в файловом менеджере. Далее вы можете вручную удалить объект или переместить объект в папку, которая не входит в область защиты.
- **Узнать больше**. Если выбран этот вариант действия, то Kaspersky Endpoint Security откроет сайт Вирусной энциклопедии "Лаборатории Касперского" https://encyclopedia.kaspersky.ru/knowledge/classification/the-classification-tree/.

kaspersky

Обновление баз и модулей программы

В сертифицированной конфигурации не допускается загружать и устанавливать обновления модулей программы. Изменение модулей программы может привести к выходу из безопасного состояния.

Обновление баз и модулей программы Kaspersky Endpoint Security обеспечивает актуальность защиты компьютера. Каждый день в мире появляются новые вирусы и другие программы, представляющие угрозу. Информация об угрозах и способах их нейтрализации содержится в базах Kaspersky Endpoint Security. Чтобы своевременно обнаруживать угрозы, вам нужно регулярно обновлять базы и модули программы.

Для регулярного обновления требуется действующая лицензия на использование программы. Если лицензия отсутствует, вы сможете выполнить обновление только один раз.

Основным источником обновлений Kaspersky Endpoint Security служат серверы обновлений "Лаборатории Касперского".

Для успешной загрузки пакета обновлений с серверов обновлений "Лаборатории Касперского" компьютер должен быть подключен к интернету. По умолчанию параметры подключения к интернету определяются автоматически. Если вы используете прокси-сервер, требуется настроить параметры прокси-сервера.

Загрузка обновлений осуществляется по протоколу HTTPS. Загрузка по протоколу HTTP может осуществляться в случае, когда загрузка обновлений по протоколу HTTPS невозможна.

В процессе обновления на ваш компьютер загружаются и устанавливаются следующие объекты:

- Базы Kaspersky Endpoint Security. Защита компьютера обеспечивается на основании баз данных, содержащих сигнатуры вирусов и других программ, представляющих угрозу, и информацию о способах борьбы с ними. Компоненты защиты используют эту информацию при поиске и обезвреживании зараженных файлов на компьютере. Базы регулярно пополняются записями о появляющихся угрозах и способах борьбы с ними. Поэтому рекомендуется регулярно обновлять базы.

  Наряду с базами Kaspersky Endpoint Security обновляются сетевые драйверы, обеспечивающие функциональность для перехвата сетевого трафика компонентами защиты.

- Модули программы. Помимо баз Kaspersky Endpoint Security, можно обновлять и модули программы. Обновления модулей программы устраняют уязвимости Kaspersky Endpoint Security, добавляют новые функции или улучшают существующие.

В процессе обновления базы и модули программы на вашем компьютере сравниваются с их актуальной версией, расположенной в источнике обновлений. Если текущие базы и модули программы отличаются от актуальной версии, на компьютер устанавливается недостающая часть обновлений.

Вместе с обновлением модулей программы может быть обновлена и контекстная справка программы.

Если базы сильно устарели, то пакет обновлений может иметь значительный размер и создать дополнительный интернет-трафик (до нескольких десятков мегабайт).

Информация о текущем состоянии баз Kaspersky Endpoint Security отображается в блоке **Обновление** в окне **Задачи**.

Информация о результатах обновления и обо всех событиях, произошедших при выполнении задачи обновления, записывается в отчет Kaspersky Endpoint Security (см. раздел "Работа с отчетами" на стр. 210).

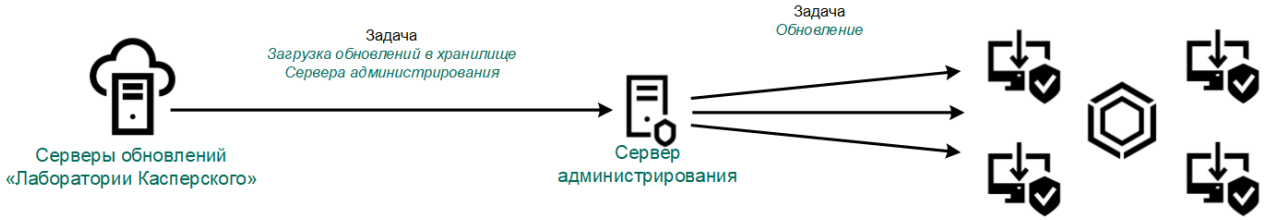
В этом разделе

Схема обновления с серверного хранилища

Для экономии интернет-трафика вы можете настроить обновление баз и модулей программы на компьютерах локальной сети организации с серверного хранилища. Для этого Kaspersky Security Center должен загружать пакет обновлений в хранилище (FTP-, HTTP-сервер, сетевая или локальная папка) с серверов обновлений "Лаборатории Касперского". В этом случае остальные компьютеры локальной сети организации смогут получать пакет обновлений с серверного хранилища.

Настройка обновления баз и модулей программы с серверного хранилища состоит из следующих этапов:

1. Настройка перемещения пакета обновлений в хранилище на Сервере администрирования (задача *Загрузка обновлений в хранилище Сервера администрирования*).
2. Настройка обновления баз и модулей программы из указанного серверного хранилища на остальных компьютерах локальной сети организации (задача *Обновление*).



► *Чтобы настроить загрузку пакета обновлений в серверное хранилище, выполните следующие действия:*

1. В главном окне Web Console выберите **Устройства → Задачи**.

   Откроется список задач.

2. Нажмите на задачу Сервера администрирования **Загрузка обновлений в хранилище Сервера администрирования**.

   Откроется окно свойств задачи.

   Задача *Загрузка обновлений в хранилище Сервера администрирования* создается автоматически мастером первоначальной настройки Kaspersky Security Center 12 Web Console и может существовать только в единственном экземпляре.

3. Выберите закладку **Параметры программы**.
4. В блоке **Прочие параметры** нажмите на кнопку **Настроить**.
5. В поле **Папка для хранения обновлений** укажите адрес FTP- или HTTP-сервера, сетевой или локальной папки, в которую Kaspersky Security Center копирует пакет обновлений, полученный с серверов обновлений "Лаборатории Касперского".

   Формат пути для источника обновлений следующий:

   - Для FTP- или HTTP-сервера введите веб-адрес или IP-адрес сайта.

     Например, `http://dnl-01.geo.kaspersky.com/` или `93.191.13.103`.

     Для FTP-сервера в адресе можно указывать параметры аутентификации в формате `ftp://<имя пользователя>:<пароль>@<узел>:<порт>`.

   - Для сетевой папки введите UNC-путь.

     Например, `\\Server\Share\Update distribution`.

   - Для локальной папки введите полный путь к папке.

     Например, `C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP11\Update distribution\`.

6. Сохраните внесенные изменения.

► *Чтобы настроить обновление Kaspersky Endpoint Security из указанного серверного хранилища, выполните следующие действия:*

1. В главном окне Web Console выберите **Устройства** → **Задачи**.

   Откроется список задач.

2. Нажмите на задачу Kaspersky Endpoint Security **Обновление**.

   Откроется окно свойств задачи.

   Задача *Обновление* создается автоматически мастером первоначальной настройки Kaspersky Security Center. Для создания задачи *Обновления* во время работы мастера установите веб-плагин Kaspersky Endpoint Security для Windows.

3. Выберите закладку **Параметры программы** → **Локальный режим**.
4. В списке источников обновления нажмите на кнопку **Добавить**.
5. В поле **Источник** укажите адрес FTP- или HTTP-сервера, сетевой или локальной папки, в которую Kaspersky Security Center копирует пакет обновлений, полученный с серверов обновлений "Лаборатории Касперского".

   Адрес источника должен совпадать с адресом, указанный ранее в поле **Папка для хранения обновлений** при настройке загрузки обновлений в серверное хранилище (см. *инструкцию выше*).

6. В блоке **Статус** выберите вариант **Включено**.
7. Нажмите на кнопку **ОК**.
8. Настройте приоритеты источников обновлений с помощью кнопок **Вверх** и **Вниз**.
9. Нажмите на кнопку **Сохранить**.

Если обновление не может быть выполнено из первого источника обновлений, Kaspersky Endpoint Security переключается к следующему автоматически.

Запуск и остановка задачи обновления

Независимо от выбранного режима запуска задачи обновления вы можете запустить или остановить задачу обновления Kaspersky Endpoint Security в любой момент.

► *Чтобы запустить или остановить задачу обновления, выполните следующие действия:*

1. В главном окне программы нажмите на кнопку **Обновление баз**.
2. В блоке **Обновление баз и программных модулей** нажмите на кнопку **Обновить**, если вы хотите запустить задачу обновления.

Kaspersky Endpoint Security запустит обновление баз и модулей программы. Программа покажет процесс проверки, размер загруженных файлов и источник обновления. Вы можете остановить выполнение задачи в любое время по кнопке  .

► *Чтобы запустить или остановить задачу обновления при отображении упрощенного интерфейса программы (см. раздел "Упрощенный интерфейс программы" на стр. 44), выполните следующие действия:*

1. По правой клавише мыши откройте контекстное меню значка программы, который расположен в области уведомлений панели задач.
2. В контекстном меню в раскрывающемся списке **Задачи** выполните одно из следующих действий:
   - выберите незапущенную задачу обновления, чтобы запустить ее;
   - выберите запущенную задачу обновления, чтобы остановить ее;
   - выберите остановленную задачу обновления, чтобы возобновить ее или запустить ее заново.

Запуск задачи обновления с правами другого пользователя

По умолчанию задача обновления Kaspersky Endpoint Security запускается от имени пользователя, с правами которого вы зарегистрированы в операционной системе. Однако обновление Kaspersky Endpoint Security может производиться из источника обновления, к которому у пользователя нет прав доступа (например, из папки общего доступа, содержащей пакет обновлений) или для которого не настроено использование аутентификации на прокси-сервере. Вы можете указать пользователя, обладающего этими правами, в параметрах Kaspersky Endpoint Security и запускать задачу обновления Kaspersky Endpoint Security от имени этого пользователя.

► *Чтобы запускать задачу обновления с правами другого пользователя, выполните следующие действия:*

1. В главном окне программы нажмите на кнопку **Обновление баз**.
2. Выберите задачу *Обновление* и перейдите по ссылке **Режим запуска: <режим>**.

   Откроются свойства задачи *Обновление*.
3. Нажмите на кнопку **Настройки учетной записи**.
4. В открывшемся окне выберите вариант **Запускать обновление баз с правами другого пользователя**.
5. Введите учетные данные пользователя, права которого требуется использовать для доступа к источнику обновлений.
6. Сохраните внесенные изменения.

Выбор режима запуска для задачи обновления

Если по каким-либо причинам запуск задачи обновления невозможен (например, в это время компьютер выключен), вы можете настроить автоматический запуск пропущенной задачи обновления, как только это станет возможным.

Вы можете отложить запуск задачи обновления после старта программы для случаев, если вы выбрали режим запуска задачи обновления **По расписанию** и время запуска Kaspersky Endpoint Security совпадает с расписанием запуска задачи обновления. Задача обновления запускается только по истечении указанного времени после старта Kaspersky Endpoint Security.

► *Чтобы выбрать режим запуска для задачи обновления, выполните следующие действия:*

1. В главном окне программы нажмите на кнопку **Обновление баз**.
2. Выберите задачу *Обновление* и перейдите по ссылке **Режим запуска: <режим>**.

   Откроются свойства задачи *Обновление*.
3. Нажмите на кнопку **Задать режим запуска обновления баз**.
4. В открывшемся окне выберите режим запуска задачи обновления:
   - Выберите вариант **Автоматически**, если вы хотите, чтобы Kaspersky Endpoint Security запускал задачу обновления в зависимости от наличия пакета обновлений в источнике обновления. Частота проверки Kaspersky Endpoint Security наличия пакета обновлений увеличивается во время вирусных эпидемий и сокращается при их отсутствии.
   - Выберите вариант **Вручную**, если вы хотите запускать задачу обновления вручную.
   - Выберите вариант **<По расписанию>**, если вы хотите настроить расписание запуска задачи обновления. Настройте дополнительные параметры запуска задачи обновления:
     - В поле **Отложить запуск после старта программы на** укажите время, на которое следует отложить запуск задачи обновления после старта Kaspersky Endpoint Security.
     - Установите флажок **Запускать пропущенные задачи**, если вы хотите, чтобы Kaspersky Endpoint Security запускал при первой возможности не запущенные вовремя задачи обновления.
5. Сохраните внесенные изменения.

Добавление источника обновлений

Источник обновлений – это ресурс, содержащий обновления баз и модулей программы Kaspersky Endpoint Security.

Источником обновлений могут быть сервер Kaspersky Security Center, серверы обновлений "Лаборатории Касперского", сетевая или локальная папка.

По умолчанию список источников обновлений содержит сервер Kaspersky Security Center и серверы обновлений "Лаборатории Касперского". Вы можете добавлять в список другие источники обновлений. В качестве источников обновлений можно указывать HTTP- или FTP-серверы, папки общего доступа.

Если в качестве источников обновлений выбрано несколько ресурсов, в процессе обновления Kaspersky Endpoint Security обращается к ним строго по списку и выполняет задачу обновления, используя пакет обновлений первого доступного источника обновлений.

Если серверы обновлений "Лаборатории Касперского" вам недоступны (например, ограничен доступ в интернет), вы можете обратиться в центральный офис "Лаборатории Касперского" (https://www.kaspersky.ru/about/contact) и узнать адреса партнеров "Лаборатории Касперского". Партнеры "Лаборатории Касперского" предоставят вам обновления на съемном диске.

Заказывая обновления на съемном диске, вам следует уточнить, хотите ли вы получить обновления модулей программы.

► *Чтобы добавить источник обновлений, выполните следующие действия:*

1. В главном окне программы нажмите на кнопку **Обновление баз**.
2. Выберите задачу *Обновление* и перейдите по ссылке **Режим запуска: <режим>**.

   Откроются свойства задачи *Обновление*.
3. Нажмите на кнопку **Настроить источники обновлений**.
4. В открывшемся окне нажмите на кнопку **Добавить**.
5. В открывшемся окне укажите адрес FTP- или HTTP-сервера, сетевой или локальной папки, которая содержит пакет обновлений.

   Формат пути для источника обновлений следующий:

   - Для FTP- или HTTP-сервера введите веб-адрес или IP-адрес сайта.

     Например, `http://dnl-01.geo.kaspersky.com/` или `93.191.13.103`.

     Для FTP-сервера в адресе можно указывать параметры аутентификации в формате `ftp://<имя пользователя>:<пароль>@<узел>:<порт>`.
   - Для сетевой папки введите UNC-путь.

     Например, `\\Server\Share\Update distribution`.
   - Для локальной папки введите полный путь к папке.

     Например, `C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP11\Update distribution\`.
6. Нажмите на кнопку **Выбрать**.
7. Настройте приоритеты источников обновлений с помощью кнопок **Вверх** и **Вниз**.
8. Сохраните внесенные изменения.

Настройка обновления из папки общего доступа

Для экономии интернет-трафика вы можете настроить обновление баз и модулей программы на компьютерах локальной сети организации из папки общего доступа. Для этого один из компьютеров локальной сети организации должен получать пакеты обновлений с Сервера администрирования Kaspersky Security Center или серверов обновлений "Лаборатории Касперского" и копировать полученный пакет обновлений в папку общего доступа. В этом случае остальные компьютеры локальной сети организации смогут получать пакет обновлений из папки общего доступа.

Настройка обновления баз и модулей программы из папки общего доступа состоит из следующих этапов:

1. Включение режима копирования пакета обновлений в папку общего доступа на одном из компьютеров локальной сети организации.
2. Настройка обновления баз и модулей программы из указанной папки общего доступа на остальных компьютерах локальной сети организации.

► *Чтобы включить режим копирования пакета обновлений в папку общего доступа, выполните следующие действия:*

1. В главном окне программы нажмите на кнопку **Обновление баз**.
2. Выберите задачу *Обновление* и перейдите по ссылке **Режим запуска: <режим>**.

   Откроются свойства задачи *Обновление*.
3. В блоке **Копирование обновлений** установите флажок **Копировать обновления в папку**.
4. Введите UNC-путь к папке общего доступа (например, `\\Server\Share\Update distribution`).
5. Сохраните внесенные изменения.

► *Чтобы настроить обновление из папки общего доступа, выполните следующие действия:*

1. В главном окне программы нажмите на кнопку **Обновление баз**.
2. Выберите задачу *Обновление* и перейдите по ссылке **Режим запуска: <режим>**.

   Откроются свойства задачи *Обновление*.
3. Нажмите на кнопку **Настроить источники обновлений**.
4. В открывшемся окне нажмите на кнопку **Добавить**.
5. В открывшемся окне укажите путь к папке общего доступа.

   Адрес источника должен совпадать с адресом, указанным ранее при настройке режима копирования пакета обновлений в папку общего доступа (см. *инструкцию выше*).
6. Нажмите на кнопку **Выбрать**.
7. Настройте приоритеты источников обновлений с помощью кнопок **Вверх** и **Вниз**.
8. Сохраните внесенные изменения.

Обновление модулей программы

Обновления модулей программы исправляют ошибки, улучшают производительность, а также добавляют новые функции. При появлении нового обновления модулей программы вам необходимо подтвердить установку обновления. Вы можете подтвердить установку обновления модулей программы в интерфейсе программы или в Kaspersky Security Center. При появлении обновления программа покажет уведомление в главном окне Kaspersky Endpoint Security: важное обновление – , или критическое обновление – . Если обновление модулей программы предполагает ознакомление и согласие с положениями Лицензионного соглашения, то программа устанавливает обновление после согласия с положениями Лицензионного соглашения. Подробнее об отслеживании обновлений модулей программы и подтверждении обновления в Kaspersky Security Center *см. в справке Kaspersky Security Center* https://help.kaspersky.com/KSC/12/ru-RU/.

После установки обновления программы может потребоваться перезагрузка компьютера.

► *Чтобы настроить обновление модулей программы, выполните следующие действия:*

1. В главном окне программы нажмите на кнопку **Обновление баз**.
2. Выберите задачу *Обновление* и перейдите по ссылке **Режим запуска: <режим>**.

   Откроются свойства задачи *Обновление*.
3. В блоке **Загрузка и установка обновлений модулей программы** установите флажок **Загружать обновления модулей программы**.
4. Выберите обновления модулей программы, которые вы хотите устанавливать:
   - **Устанавливать критические и одобренные обновления**. Если выбран этот вариант, то при наличии обновлений модулей программы Kaspersky Endpoint Security устанавливает критические обновления автоматически, а остальные обновления модулей программы – после одобрения их установки, локально через интерфейс программы или на стороне Kaspersky Security Center.
   - **Устанавливать только одобренные обновления**. Если выбран этот вариант, то при наличии обновлений модулей программы Kaspersky Endpoint Security устанавливает их после одобрения их установки, локально через интерфейс программы или на стороне Kaspersky Security Center. Этот вариант выбран по умолчанию.
5. Сохраните внесенные изменения.

Использование прокси-сервера при обновлении

Для загрузки обновлений баз и модулей программы из источника обновлений может потребоваться указать параметры прокси-сервера. Если источников обновлений несколько, параметры прокси-сервера применяются для всех источников. Если для некоторых источников обновлений прокси-сервер не нужен, вы можете выключить использование прокси-сервера в свойствах политики. Kaspersky Endpoint Security также будет использовать прокси-сервер для доступа к Kaspersky Security Network и серверам активации.

► *Чтобы настроить подключение к источникам обновлений через прокси-сервер, выполните следующие действия:*

1. В главном окне Web Console нажмите  .

   Откроется окно свойств Сервера администрирования.
2. Перейдите в раздел **Параметры доступа к сети Интернет**.
3. Установите флажок **Использовать прокси-сервер**.
4. Настройте параметры подключения к прокси-серверу: адрес прокси-сервера, порт и параметры аутентификации (имя пользователя и пароль).
5. Нажмите на кнопку **Сохранить**.

► *Чтобы выключить использование прокси-сервера для определенной группы администрирования, выполните следующие действия:*

1. В главном окне Web Console выберите **Устройства** → **Политики и профили политик**.
2. Нажмите на название политики Kaspersky Endpoint Security для компьютеров, на которых вы хотите выключить использование прокси-сервера.

   Откроется окно свойств политики.
3. Выберите закладку **Параметры программы**.

4. Перейдите в раздел **Общие настройки** → **Настройки сети**.
5. В блоке **Настройки прокси-сервера** выберите вариант **Не использовать прокси-сервер**.
6. Нажмите на кнопку **ОК**.
7. Подтвердите изменения по кнопке **Сохранить**.

► *Чтобы настроить параметры прокси-сервера в интерфейсе программы, выполните следующие действия:*

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Настройки сети**.
3. В блоке **Прокси-сервер** перейдите по ссылке **Настройка прокси-сервера**.
4. В открывшемся окне выберите один из следующих вариантов определения адреса прокси-сервера:
   - **Автоматически определять настройки прокси-сервера**.

     Этот вариант выбран по умолчанию. Kaspersky Endpoint Security использует параметры прокси-сервера заданные в параметрах операционной системы.
   - **Использовать указанные настройки прокси-сервера**.

     Если вы выбрали этот вариант, настройте параметры подключения к прокси-серверу: адрес прокси-сервера и порт.
5. Если вы хотите включить использование аутентификации на прокси-сервере, установите флажок **Использовать аутентификации на прокси-сервере** и укажите учетные данные пользователя.
6. Если вы хотите выключить использование прокси-сервера при обновлении баз и модулей программы из папки общего доступа (см. раздел "Настройка обновления из папки общего доступа" на стр. 73), установите флажок **Не использовать прокси-сервер для локальных адресов**.
7. Сохраните внесенные изменения.

В результате Kaspersky Endpoint Security будет использовать прокси-сервер для загрузки обновлений баз и модулей программы. Также Kaspersky Endpoint Security использует прокси-сервер для доступа к серверам KSN и серверам активации "Лаборатории Касперского". Если требуется аутентификация на прокси-сервере, а учетные данные пользователя не указаны или указаны неверно, Kaspersky Endpoint Security запросит имя пользователя и пароль.

Откат последнего обновления

После первого обновления баз и модулей программы становится доступна функция отката к предыдущим базам и модулям программы.

Каждый раз, когда пользователь запускает обновление, Kaspersky Endpoint Security создает резервную копию используемых баз и модулей программы и только потом приступает к их обновлению. Это позволяет вернуться к использованию предыдущих баз и модулей программы при необходимости. Возможность отката последнего обновления полезна, например, в том случае, если новая версия баз содержит некорректную сигнатуру, из-за которой Kaspersky Endpoint Security блокирует безопасную программу.

► *Чтобы откатить последнее обновление, выполните следующие действия:*

1. В главном окне программы нажмите на кнопку **Обновление баз**.
2. В блоке **Откат к предыдущей версии баз** нажмите на кнопку **Откатить**.

Kaspersky Endpoint Security запустит откат последнего обновления баз. Программа покажет процесс отката, размер загруженных файлов и источник обновления. Вы можете остановить выполнение задачи в любое время по кнопке  .

► *Чтобы запустить или остановить задачу отката обновления при отображении упрощенного интерфейса программы (см. раздел "Упрощенный интерфейс программы" на стр. 44), выполните следующие действия:*

1. По правой клавише мыши откройте контекстное меню значка программы, который расположен в области уведомлений панели задач.
2. В контекстном меню в раскрывающемся списке **Задачи** выполните одно из следующих действий:
   - Выберите незапущенную задачу отката обновления, чтобы запустить ее.
   - Выберите запущенную задачу отката обновления, чтобы остановить ее.
   - Выберите остановленную задачу отката обновления, чтобы возобновить ее или запустить ее заново.

Обновление антивирусных баз в ручном режиме

Для обновления антивирусных баз, находящихся в изолированном сегменте сети, рекомендуется использовать следующий порядок действий:

1. В программе Kaspersky Security Center, находящейся в открытом сегменте сети, настроить задачу загрузки обновлений в хранилище.
2. Убедиться в том, что под управлением Kaspersky Security Center в открытом сегменте есть управляемые машины с установленными программами, базы для которых необходимо обновить.
3. Запустить задачу. В процессе загрузки обновлений с открытых серверов «Лаборатории Касперского» Kaspersky Security Center проведет проверку контроля целостности обновлений, прежде чем добавит их в свое хранилище.
4. Удобным вам способом перенесите содержимое хранилища Kaspersky Security Center в изолированный сегмент сети.

Запустите на средствах антивирусной защиты внутри изолированного сегмента сети задачу обновления с указанием перенесенного хранилища как источника обновлений. При загрузке обновлений из хранилища, программы еще раз проведут контроль целостности загружаемых обновлений.

Если вам недоступны серверы обновлений "Лаборатории Касперского" (например, нет доступа к интернету), обратитесь в Службу технической поддержки "Лаборатории Касперского" для получения обновлений программы на дисках.

kaspersky

Устранение уязвимостей и установка критических обновлений в программе

"Лаборатория Касперского" может выпускать обновления программного обеспечения, направленные на устранение уязвимостей и недостатков безопасности (критические обновления). Срочные пакеты обновлений публикуются на серверах автоматизированной установки обновлений "Лаборатории Касперского". Уведомления о выпуске критических обновлений публикуются на веб-сайте (https://support.kaspersky.ru/general/certificates) и рассылаются по адресам электронной почты, указанным при заказе программы, а также подписчикам рассылки (подписаться на рассылку можно по ссылке: http://support.kaspersky.ru/subscribe). Порядок получения критических обновлений изложен в формуляре.

Программу необходимо периодически (не реже одного раза в полгода) подвергать анализу уязвимостей: организация, осуществляющая эксплуатацию программы, должна проводить такой анализ с помощью открытых источников, содержащих базу уязвимостей, в том числе с веб-сайта "Лаборатории Касперского" (http://www.bdu.fstec.ru, https://support.kaspersky.ru/vulnerability).

Вы можете сообщать об обнаруженных недостатках безопасности или уязвимостях программы следующими способами:

- Через веб-форму на веб-сайте Службы технической поддержки (https://support.kaspersky.ru/vulnerability.aspx?el=12429).
- По адресу электронной почты vulnerability@kaspersky.com.
- В сообществе пользователей "Лаборатории Касперского" (https://community.kaspersky.com/).

kaspersky

Kaspersky Security Network

Чтобы повысить эффективность защиты компьютера пользователя, Kaspersky Endpoint Security использует данные, полученные от пользователей во всем мире. Для получения этих данных предназначена сеть *Kaspersky Security Network*.

Kaspersky Security Network (KSN) – это инфраструктура облачных служб, предоставляющая доступ к оперативной базе знаний "Лаборатории Касперского" о репутации файлов, интернет-ресурсов и программного обеспечения. Использование данных Kaspersky Security Network обеспечивает более высокую скорость реакции Kaspersky Endpoint Security на неизвестные угрозы, повышает эффективность работы некоторых компонентов защиты, а также снижает вероятность ложных срабатываний.

В зависимости от расположения инфраструктуры различают Глобальный KSN (инфраструктура расположена на серверах "Лаборатории Касперского") и Локальный KSN.

В сертифицированной версии программы Kaspersky Endpoint Security используется только Локальный KSN (KPSN). Использование Глобального KSN не допускается.

Участие пользователей в KSN позволяет "Лаборатории Касперского" оперативно получать информацию о типах и источниках угроз, разрабатывать способы нейтрализации угроз, уменьшать количество ложных срабатываний компонентов программы.

При использовании расширенного режима KSN программа автоматически отправляет в KSN статистическую информацию, полученную в результате своей работы. Также программа может отправлять в "Лабораторию Касперского" для дополнительной проверки файлы (или части файлов), которые злоумышленники могут использовать для нанесения вреда компьютеру или данным.

Более подробную информацию об отправке в "Лабораторию Касперского", хранении и уничтожении статистической информации, полученной во время использования KSN, вы можете прочитать в Положении о Kaspersky Security Network и на веб-сайте "Лаборатории Касперского" (https://www.kaspersky.ru/products-and-services-privacy-policy). Файл ksn_<ID языка>.txt с текстом Положения о Kaspersky Security Network входит в комплект поставки программы.
Для снижения нагрузки на серверы KSN специалисты "Лаборатории Касперского" могут выпускать антивирусные базы программы, которые временно выключают или частично ограничивают обращения в Kaspersky Security Network. В этом случае статус подключения к KSN – *Включено с ограничениями* (см. раздел "*Проверка подключения к Kaspersky Security Network*" на стр. 83).

Компьютеры пользователей, работающие под управлением Сервера администрирования Kaspersky Security Center, могут взаимодействовать с KSN при помощи службы KSN Proxy.

Служба KSN Proxy предоставляет следующие возможности:

- Компьютер пользователя может выполнять запросы к KSN и передавать в KSN информацию, даже если он не имеет прямого доступа в интернет.
- Служба KSN Proxy кеширует обработанные данные, снижая тем самым нагрузку на канал во внешнюю сеть и ускоряя получение компьютером пользователя запрошенной информации.

Подробнее о службе KSN Proxy вы можете прочитать в *Руководстве администратора для Kaspersky*

Security Center.

Настройка параметров использования службы KSN Proxy доступна в свойствах политики *Kaspersky Security Center*.

Использование Kaspersky Security Network является добровольным. Программа предлагает использовать KSN во время первоначальной настройки программы. Начать или прекратить использование KSN можно в любой момент.

В этом разделе

Включение и выключение использования Kaspersky Security Network

► *Чтобы включить или выключить использование Kaspersky Security Network, выполните следующие действия:*

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Защита** → **Продвинутая защита** → **Kaspersky Security Network**.
3. Используйте переключатель **Kaspersky Security Network**, чтобы включить или выключить компонент.

   Если вы включили использование KSN, Kaspersky Endpoint Security покажет Положение о Kaspersky Security Network. Если вы согласны, примите условия использования KSN.

   По умолчанию Kaspersky Endpoint Security использует расширенный режим KSN. *Расширенный режим KSN* – режим работы программы, при котором Kaspersky Endpoint Security передает в "Лабораторию Касперского" дополнительные данные.
4. Если требуется, выключите переключатель **Включить расширенный режим KSN**.
5. Сохраните внесенные изменения.

В результате, если использование KSN включено, Kaspersky Endpoint Security использует информацию о репутации файлов, веб-ресурсов и программ, полученную из Kaspersky Security Network.

kaspersky

Ограничения работы с Локальным KSN

В сертифицированной версии программы Kaspersky Endpoint Security используется только Локальный KSN (KPSN). Использование Глобального KSN не допускается.

Локальный KSN (далее также "KPSN") позволяет использовать собственную базу данных репутаций объектов (файлов или веб-адресов) с помощью локальной репутационной базы. Репутация объекта, добавленного в локальную репутационную базу, имеет приоритет выше, чем в KSN / KPSN. То есть, если Kaspersky Endpoint Security при проверке компьютера запросит репутацию файла в KSN / KPSN, и в локальной репутационной базе файл имеет репутацию "недоверенный", а в KSN / KPSN объект имеет репутацию "доверенный", то Kaspersky Endpoint Security обнаружит файл как "недоверенный" и выполнит действие, заданное для обнаруженных угроз.

Однако в некоторых случаях Kaspersky Endpoint Security может не запрашивать репутацию объекта в KSN / KPSN. В результате Kaspersky Endpoint Security не получит данные из локальной репутационной базы KPSN. Kaspersky Endpoint Security может не запрашивать репутацию объекта в KSN / KPSN, например, по следующим причинам:

- Программы "Лаборатории Касперского" используют офлайн репутационные базы. Офлайн репутационные базы предназначены для оптимизации ресурсов при работе программ "Лаборатории Касперского" и защите критически важных объектов компьютера. Офлайн репутационные базы формируют специалисты "Лаборатории Касперского" на основании данных Kaspersky Security Network. Программы "Лаборатории Касперского" обновляют офлайн репутационные базы с антивирусными базами программы. Если информация о проверяемом объекте содержится в офлайн репутационных базах, программа не запрашивает репутацию этого объекта в KSN / KPSN.
- В параметрах программы настроены исключения из проверки (доверенная зона (на стр. 197)). В этом случае программа не учитывает репутацию объекта в локальной репутационной базе.
- Программа использует технологии оптимизации проверки, например, технологии iSwift, iChecker или кеширование запросов репутации в KSN / KPSN. В этом случае программа может не запрашивать репутацию ранее проверенных объектов.
- Для оптимизации нагрузки программа проверяет файлы определенного формата и размера. Список форматов и ограничения по размеру определяют специалисты "Лаборатории Касперского". Этот список обновляется с антивирусными базами программы. Также вы можете настроить параметры оптимизации проверки в интерфейсе программы, например, для компонента Защита от файловых угроз (см. раздел "Оптимизация проверки файлов" на стр. 113).

Включение и выключение облачного режима для компонентов защиты

Облачный режим – режим работы программы, при котором Kaspersky Endpoint Security использует облегченную версию антивирусных баз. Работу программы с облегченными антивирусными базами обеспечивает Kaspersky Security Network. Облегченная версия антивирусных баз позволяет снизить нагрузку на оперативную память компьютера примерно в два раза. Если вы не участвуете в Kaspersky Security Network или облачный режим выключен, Kaspersky Endpoint Security загружает полную версию антивирусных баз с серверов "Лаборатории Касперского".

При использовании Kaspersky Private Security Network функциональность облачного режима доступна начиная с версии Kaspersky Private Security Network 3.0.

► *Чтобы включить или выключить облачный режим для компонентов защиты, выполните следующие действия:*

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Защита** → **Продвинутая защита** → **Kaspersky Security Network**.
3. Используйте переключатель **Включить Облачный режим**, чтобы включить или выключить компонент.
4. Сохраните внесенные изменения.

В результате Kaspersky Endpoint Security загружает облегченную или полную версию антивирусных баз в ходе ближайшего обновления.

Если облегченная версия антивирусных баз недоступна для использования, Kaspersky Endpoint Security автоматически переключается на использование полной версии антивирусных баз.

Проверка подключения к Kaspersky Security Network

Подключение к Kaspersky Security Network может отсутствовать по следующим причинам:

- Вы не участвуете в Kaspersky Security Network.
- Ваш компьютер не подключен к интернету.
- Текущий статус ключа не позволяет осуществить подключение к Kaspersky Security Network. Например, подключение к KSN может отсутствовать по следующим причинам:
  - Программа не активирована.
  - Срок действия лицензии или подписки истек.
  - Выявлены проблемы, связанные с лицензионным ключом (например, ключ попал в список запрещенных ключей).

► *Чтобы проверить подключение к Kaspersky Security Network,*

в главном окне программы нажмите на кнопку **Больше функций** → **Kaspersky Security Network**.

Откроется окно **Kaspersky Security Network**, в котором представлена информация о работе Kaspersky Security Network. Получение статистических данных по использованию KSN программа производит при открытии окна **Kaspersky Security Network**. Обновление глобальной статистики инфраструктуры облачных служб Kaspersky Security Network, а также времени синхронизации в режиме реального времени не производится.

В левой части окна **Kaspersky Security Network** отображается один из следующих статусов подключения компьютера к Kaspersky Security Network:

- *Включено.*

  Статус означает, что Kaspersky Security Network используется в работе Kaspersky Endpoint Security и серверы KSN доступны.

- *Включено. Доступно с ограничениями*.

  Статус означает, что Kaspersky Security Network используется в работе Kaspersky Endpoint Security и серверы KSN недоступны.

  Серверы KSN могут быть недоступны по следующим причинам:

  - На компьютере не запущена служба прокси-сервера KSN (ksnproxy).
  - Сетевой экран блокирует порт 13111.

  Если время, прошедшее после последней синхронизации с серверами KSN, превышает 15 минут или отображается статус *Неизвестно*, то статус подключения Kaspersky Endpoint Security к Kaspersky Security Network принимает значение *Включено. Недоступно*.

- *Выключено*.

  Статус означает, что Kaspersky Security Network не используется в работе Kaspersky Endpoint Security.

Если восстановить связь с серверами Kaspersky Security Network не удается, то рекомендуется обратиться в Службу технической поддержки или к поставщику услуг.

Проверка репутации файла в Kaspersky Security Network

Если вы сомневаетесь в безопасности файла, вы можете проверить его репутацию в Kaspersky Security Network.

Проверка репутации файла доступна, если вы приняли условия Положения о Kaspersky Security Network (см. раздел "Включение и выключение использования Kaspersky Security Network" на стр. 81).

► *Чтобы проверить репутацию файла в Kaspersky Security Network,*

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

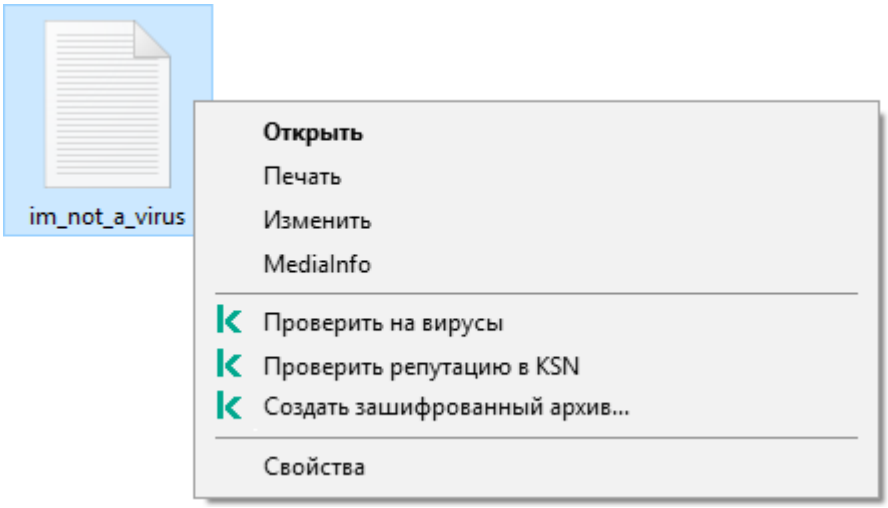


Рисунок 10. Контекстное меню файла

Kaspersky Endpoint Security отображает репутацию файла:

Доверенный. Большинство пользователей Kaspersky Security Network подтвердили, что файл доверенный.

Легальная программа, которая может быть использована для нанесения вреда компьютеру или данным. Такие программы сами по себе не имеют вредоносных функций, но эти программы могут быть использованы злоумышленниками. Подробную информацию о легальных программах, которые могут быть использованы злоумышленниками для нанесения вреда компьютеру или данным пользователя, вы можете получить на сайте Вирусной энциклопедии "Лаборатории Касперского" https://encyclopedia.kaspersky.ru/knowledge/classification/the-classification-tree/. Вы можете добавить эти программы в список доверенных (см. раздел "Формирование списка доверенных программ" на стр. 201).

Недоверенный. Вирус или другая программа, представляющая угрозу (см. раздел "Работа с активными угрозами" на стр. 64).

Неизвестный. В Kaspersky Security Network отсутствует информация о файле. Вы можете проверить файл с помощью антивирусных баз (пункт контекстного меню **Проверить на вирусы**).

Kaspersky Endpoint Security отображает решение KSN, которое было использовано для определения репутации файла: *Глобальный KSN* или *Локальный KSN*.

Также Kaspersky Endpoint Security отображает дополнительную информацию о файле (см. рис. ниже).

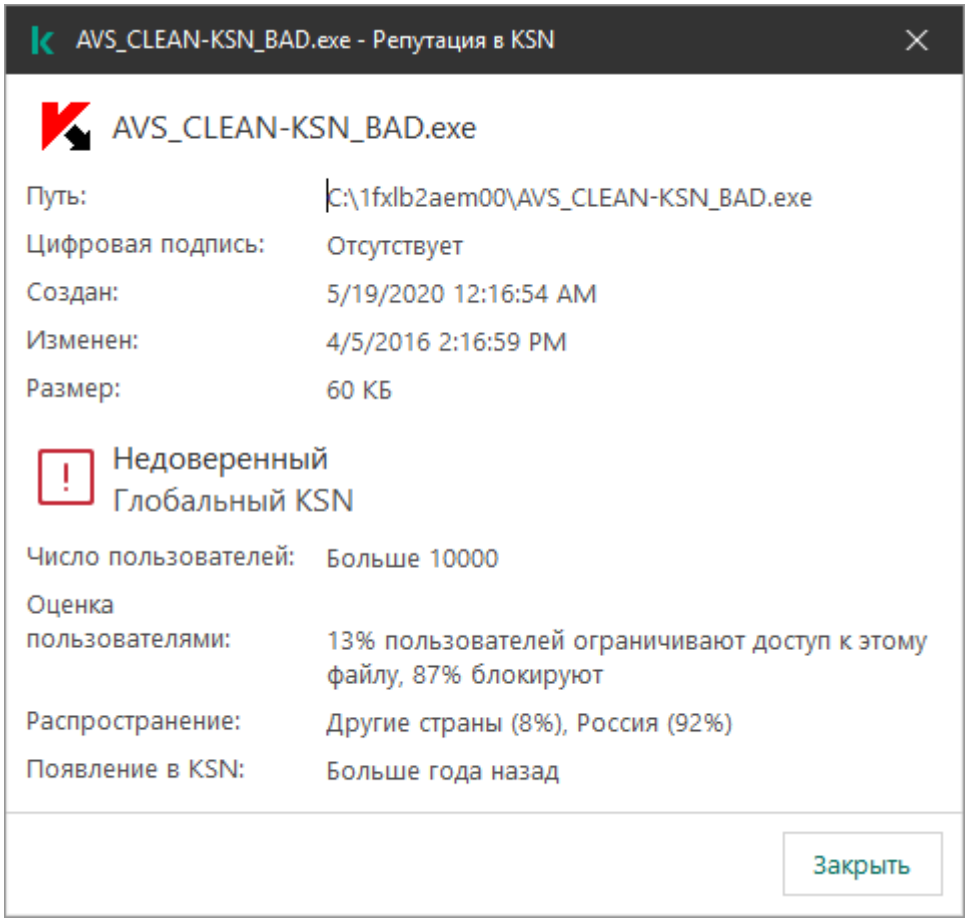


Рисунок 11. Репутация файла в Kaspersky Security Network

kaspersky

Анализ поведения

Компонент Анализ поведения получает данные о действиях программ на вашем компьютере и предоставляет эту информацию другим компонентам защиты для повышения эффективности их работы.

Компонент Анализ поведения использует шаблоны опасного поведения программ. Если активность программы совпадает с одним из шаблонов опасного поведения, Kaspersky Endpoint Security выполняет выбранное ответное действие. Функциональность Kaspersky Endpoint Security, основанная на шаблонах опасного поведения, обеспечивает проактивную защиту компьютера.

В этом разделе

Включение и выключение Анализа поведения

По умолчанию Анализ поведения включен и работает в режиме, рекомендованном специалистами "Лаборатории Касперского". Вы можете выключить Анализ поведения при необходимости.

Не рекомендуется выключать Анализ поведения без необходимости, так как это снижает эффективность работы компонентов защиты. Компоненты защиты могут запрашивать данные, полученные компонентом Анализ поведения, для обнаружения угроз.

► *Чтобы включить или выключить Анализ поведения, выполните следующие действия:*

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Защита** → **Продвинутая защита** → **Анализ поведения**.
3. Используйте переключатель **Анализ поведения**, чтобы включить или выключить компонент.
4. Сохраните внесенные изменения.

В результате, если Анализ поведения включен, Kaspersky Endpoint Security будет анализировать активность программ в операционной системе, используя шаблоны опасного поведения.

kaspersky

Выбор действия при обнаружении вредоносной активности программы

► *Чтобы выбрать действие при обнаружении вредоносной активности программы, выполните следующие действия:*

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Защита** → **Продвинутая защита** → **Анализ поведения**.
3. В блоке **При обнаружении вредоносной активности программы** выберите нужное действие:
   - **Удалять файл**. Если выбран этот элемент, то, обнаружив вредоносную активность программы, Kaspersky Endpoint Security удаляет исполняемый файл вредоносной программы и создает резервную копию файла в резервном хранилище.
   - **Завершать работу программы**. Если выбран этот элемент, то, обнаружив вредоносную активность программы, Kaspersky Endpoint Security завершает работу этой программы.
   - **Информировать**. Если выбран этот элемент, то, обнаружив вредоносную активность программы, Kaspersky Endpoint Security добавляет информацию о вредоносной активности этой программы в список активных угроз.
4. Сохраните внесенные изменения.

Защита папок общего доступа от внешнего шифрования

Компонент обеспечивает отслеживание операций только над теми файлами, которые расположены на запоминающих устройствах с файловой системой NTFS и не зашифрованы системой EFS.

Функция защиты папок общего доступа от внешнего шифрования обеспечивает анализ активности в папках общего доступа. Если активность совпадает с одним из шаблонов поведения, характерного для внешнего шифрования, Kaspersky Endpoint Security выполняет выбранное действие.

По умолчанию защита папок общего доступа от внешнего шифрования выключена.

После установки Kaspersky Endpoint Security функция защиты папок общего доступа от внешнего шифрования будет ограничена до перезагрузки компьютера.

kaspersky

В этом разделе

Включение и выключение защиты папок общего доступа от внешнего шифрования

После установки Kaspersky Endpoint Security функция защиты папок общего доступа от внешнего шифрования будет ограничена до перезагрузки компьютера.

► *Чтобы включить или выключить защиту папок общего доступа от внешнего шифрования, выполните следующие действия:*

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Защита** → **Продвинутая защита** → **Анализ поведения**.
3. Используйте переключатель **Включить защиту папок общего доступа от внешнего шифрования**, чтобы включить или выключить анализ активности, характерную для внешнего шифрования.
4. Сохраните внесенные изменения.

Выбор действия при обнаружении внешнего шифрования папок общего доступа

► *Чтобы выбрать действие при обнаружении внешнего шифрования папок общего доступа, выполните следующие действия:*

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Защита** → **Продвинутая защита** → **Анализ поведения**.
3. В блоке **Защита папок общего доступа от внешнего шифрования** выберите нужное действие:
   - **Блокировать соединение на N мин**. Если выбран этот вариант, то при обнаружении попытки изменения файлов в папках общего доступа, Kaspersky Endpoint Security выполняет следующие действия:
     - блокирует сетевую активность компьютера, осуществляющего изменение;
     - создает резервные копии подверженных изменению файлов;

- добавляет запись в отчеты локального интерфейса программы (см. раздел "Работа с отчетами" на стр. 210);
- отправляет в Kaspersky Security Center информацию об обнаружении вредоносной активности.

Если при этом включен компонент Откат вредоносных действий, то выполняется восстановление измененных файлов из резервных копий.

- **Информировать**. Если выбран этот вариант, то при обнаружении попытки изменения файлов в папках общего доступа, Kaspersky Endpoint Security выполняет следующие действия:
  - добавляет запись в отчеты локального интерфейса программы (см. раздел "Работа с отчетами" на стр. 210);
  - добавляет запись в список активных угроз;
  - отправляет в Kaspersky Security Center информацию об обнаружении вредоносной активности.

4. Сохраните внесенные изменения.

Настройка адресов исключений из защиты папок общего доступа от внешнего шифрования

Для работы функциональности исключений адресов из защиты папок общего доступа от внешнего шифрования необходимо включить службу Аудит входа в систему. По умолчанию служба Аудит входа в систему выключена (подробную информацию о включении службы Аудит входа в систему см. на сайте корпорации Microsoft).
Функциональность исключений адресов из защиты папок общего доступа не работает на удаленном компьютере, если этот удаленный компьютер был включен до запуска Kaspersky Endpoint Security. Вы можете перезагрузить этот удаленный компьютер после запуска Kaspersky Endpoint Security, чтобы обеспечить работу функциональности исключений адресов из защиты папок общего доступа на этом удаленном компьютере.

► *Чтобы исключить из защиты удаленные компьютеры, осуществляющие внешнее шифрование папок общего доступа, выполните следующие действия:*

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Защита** → **Продвинутая защита** → **Анализ поведения**.
3. В блоке **Исключения** перейдите по ссылке **Настройка адресов исключений**.
4. Если вы хотите добавить IP-адрес или имя компьютера в список исключений, нажмите на кнопку **Добавить**.
5. Введите IP-адрес компьютера или имя компьютера, попытки внешнего шифрования с которого не должны обрабатываться.
6. Сохраните внесенные изменения.

kaspersky

Защита от эксплойтов

Компонент Защита от эксплойтов отслеживает программный код, который использует уязвимости на компьютере для получения эксплойтом прав администратора или выполнения вредоносных действий. Эксплойты, например, используют атаку на переполнение буфера обмена. Для этого эксплойт отправляет большой объем данных в уязвимую программу. При обработке этих данных уязвимая программа выполняет вредоносный код. В результате этой атаки эксплойт может запустить несанкционированную установку вредоносного ПО.

Если попытка запустить исполняемый файл из уязвимой программы не была произведена пользователем, то Kaspersky Endpoint Security блокирует запуск этого файла или информирует пользователя.

В этом разделе

Включение и выключение Защиты от эксплойтов

По умолчанию Защита от эксплойтов включена и работает в режиме, рекомендованном специалистами "Лаборатории Касперского". Вы можете выключить Защиту от эксплойтов при необходимости.

► *Чтобы включить или выключить Защиту от эксплойтов, выполните следующие действия:*

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Защита** → **Продвинутая защита** → **Защита от эксплойтов**.
3. Используйте переключатель **Защита от эксплойтов**, чтобы включить или выключить компонент.
4. Сохраните внесенные изменения.

В результате, если Защита от эксплойтов включена, Kaspersky Endpoint Security будет отслеживать исполняемые файлы, запускаемые уязвимыми программами. Если Kaspersky Endpoint Security обнаруживает, что исполняемый файл из уязвимой программы был запущен не пользователем, то Kaspersky Endpoint Security выполняет выбранное действие (например, блокирует операцию).

Выбор действия при обнаружении эксплойта

По умолчанию, обнаружив эксплойт, Kaspersky Endpoint Security блокирует операции этого эксплойта.

► *Чтобы выбрать действие при обнаружении эксплойта, выполните следующие действия:*

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Защита** → **Продвинутая защита** → **Защита от эксплойтов**.

3. В блоке **При обнаружении эксплойта** выберите нужное действие:
   - **Блокировать операцию**. Если выбран этот элемент, то, обнаружив эксплойт, Kaspersky Endpoint Security блокирует операции этого эксплойта и создает в журнале запись, содержащую информацию об этом эксплойте.
   - **Информировать**. Если выбран этот элемент, то, обнаружив эксплойт, Kaspersky Endpoint Security создает в журнале запись, содержащую информацию об этом эксплойте, и добавляет информацию об этом эксплойте в список активных угроз.
4. Сохраните внесенные изменения.

Защита памяти системных процессов

По умолчанию защита памяти системных процессов включена.

► *Чтобы включить или выключить защиту памяти системных процессов, выполните следующие действия:*

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Защита** → **Продвинутая защита** → **Защита от эксплойтов**.
3. Используйте переключатель **Включить защиту памяти системных процессов**, чтобы включить или выключить функцию.
4. Сохраните внесенные изменения.

В результате Kaspersky Endpoint Security будет блокировать сторонние процессы, осуществляющие попытки доступа к системным процессам.

kaspersky

Предотвращение вторжений

Этот компонент доступен, если программа Kaspersky Endpoint Security установлена на компьютере под управлением операционной системы Windows для рабочих станций. Этот компонент недоступен, если программа Kaspersky Endpoint Security установлена на компьютере под управлением операционной системы Windows для серверов.

Компонент Предотвращение вторжений (англ. HIPS – Host Intrusion Prevention System) предотвращает выполнение программами опасных для системы действий, а также обеспечивает контроль доступа к ресурсам операционной системы и персональным данным. Компонент обеспечивает защиту компьютера с помощью антивирусных баз и облачной службы Kaspersky Security Network.

Компонент контролирует работу программ с помощью *прав программ*. Права программ включают в себя следующие параметры доступа:

- доступ к ресурсам операционной системы (например, параметры автозапуска, ключи реестра);
- доступ к персональным данным (например, к файлам, программам).

Сетевую активность программ контролирует Сетевой экран с помощью *сетевых правил*.

Во время первого запуска программы компонент Предотвращение вторжений выполняет следующие действия:

1. Проверяет безопасность программы с помощью загруженных антивирусных баз.
2. Проверяет безопасность программы в Kaspersky Security Network.

   Для более эффективной работы компонента Предотвращение вторжений вам рекомендуется принять участие в Kaspersky Security Network (см. раздел "Включение и выключение использования Kaspersky Security Network" на стр. 81).

3. Помещает программу в одну из *групп доверия*: Доверенные, Слабые ограничения, Сильные ограничения, Недоверенные.

   Группа доверия определяет права (см. раздел "Приложение 2. Группы доверия программ" на стр. 279), которые Kaspersky Endpoint Security использует для контроля активности программ. Kaspersky Endpoint Security помещает программу в группу доверия в зависимости от уровня опасности, которую эта программа может представлять для компьютера.

   Kaspersky Endpoint Security помещает программу в группу доверия для компонентов Сетевой экран и Предотвращение вторжений. Изменить группу доверия только для Сетевого экрана или только для Предотвращения вторжений невозможно.

> Если вы отказались принимать участие в KSN или отсутствует сеть, Kaspersky Endpoint Security помещает программу в группу доверия в зависимости от параметров компонента Предотвращение вторжений (см. раздел "Выбор группы доверия для неизвестных программ" на стр. 97). После получения данных о репутации программы от KSN группа доверия может быть изменена автоматически.

4. Блокирует действия программы в зависимости от группы доверия. Например, программам из группы доверия "Сильные ограничения" запрещен доступ к модулям операционной системы.

При следующем запуске программы Kaspersky Endpoint Security проверяет целостность программы. Если программа не была изменена, компонент применяет к ней текущие права программ. Если программа была изменена, Kaspersky Endpoint Security исследует программу как при первом запуске.

В этом разделе

Включение и выключение Предотвращения вторжений

По умолчанию компонент Предотвращение вторжений включен и работает в рекомендованном специалистами "Лаборатории Касперского" режиме.

Как включить или выключить компонент Предотвращение вторжений в интерфейсе программы:

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Защита** → **Продвинутая защита** → **Предотвращение вторжений**.
3. Используйте переключатель **Предотвращение вторжений**, чтобы включить или выключить компонент.
4. Сохраните внесенные изменения.

В результате, если компонент Предотвращение вторжений включен, Kaspersky Endpoint Security помещает программу в группу доверия (см. раздел "Приложение 2. Группы доверия программ" на стр. 279) в зависимости от уровня опасности, которую эта программа может представлять для компьютера. Далее Kaspersky Endpoint Security будет блокировать действия программы в зависимости от группы доверия.

kaspersky

Работа с группами доверия программ

Во время первого запуска каждой программы компонент Предотвращение вторжений проверяет безопасность программы и помещает программу в одну из групп доверия (см. раздел "Приложение 2. Группы доверия программ" на стр. 279).

На первом этапе проверки программы Kaspersky Endpoint Security ищет запись о программе во внутренней базе известных программ и одновременно отправляет запрос в базу Kaspersky Security Network (при наличии подключения к интернету). По результатам проверки по внутренней базе и по базе Kaspersky Security Network программа помещается в группу доверия. При каждом повторном запуске программы Kaspersky Endpoint Security отправляет новый запрос в базу KSN и перемещает программу в другую группу доверия, если репутация программы в базе KSN изменилась.

Вы можете выбрать группу доверия, в которую Kaspersky Endpoint Security должен автоматически помещать все неизвестные программы (см. раздел "Выбор группы доверия для неизвестных программ" на стр. 97). Программы, которые были запущены до Kaspersky Endpoint Security, автоматически помещаются в группу доверия, установленную в параметрах компонента Предотвращение вторжений (см. раздел "Выбор группы доверия для программ, запускаемых до Kaspersky Endpoint Security" на стр. 97).

Для программ, запущенных до Kaspersky Endpoint Security, контролируется только сетевая активность. Контроль осуществляется согласно сетевым правилам, установленным в параметрах Сетевого экрана.

В этом разделе

Изменение группы доверия для программы

Во время первого запуска каждой программы компонент Предотвращение вторжений проверяет безопасность программы и помещает программу в одну из групп доверия (см. раздел "Приложение 2. Группы доверия программ" на стр. 279).

Специалисты "Лаборатории Касперского" не рекомендуют перемещать программы из группы доверия, определенной автоматически, в другую группу доверия. Вместо этого при необходимости измените права отдельной программы (см. раздел "Работа с правами программ" на стр. 98).

Как изменить группу доверия для программы в интерфейсе программы:

1. В нижней части главного окна программы нажмите на кнопку .
2. В окне параметров программы выберите раздел **Защита** → **Продвинутая защита** → **Предотвращение вторжений**.
3. Нажмите на кнопку **Управление программами**.

   Откроется список установленных программ.
4. Выберите нужную программу.
5. В контекстном меню программы выберите пункт **Ограничения** → **<группа доверия>**.
6. Сохраните внесенные изменения.

В результате программа будет перемещена в другую группу доверия. Далее Kaspersky Endpoint Security будет блокировать действия программы в зависимости от группы доверия. Программе будет присвоен статус *(задано пользователем)*. При изменении репутации программы в Kaspersky Security Network компонент Предотвращение вторжений оставит группу доверия для этой программы без изменений.

Настройка прав группы доверия

По умолчанию для разных групп доверия созданы оптимальные права программ (см. раздел "Приложение 2. Группы доверия программ" на стр. 279). Параметры прав групп программ, входящих в группу доверия, наследуют значения параметров прав групп доверия.

Как изменить права группы доверия в интерфейсе программы:

1. В нижней части главного окна программы нажмите на кнопку .
2. В окне параметров программы выберите раздел **Защита** → **Продвинутая защита** → **Предотвращение вторжений**.
3. Нажмите на кнопку **Управление программами**.

   Откроется список установленных программ.
4. Выберите нужную группу доверия.
5. В контекстном меню группы доверия выберите пункт **Подробности и правила**.

   Откроются свойства группы доверия.
6. Выполните одно из следующих действий:
   - Выберите закладку **Файлы и системный реестр**, если вы хотите изменить права группы доверия, регулирующие операции с реестром операционной системы, файлами пользователя и параметрами программ.
   - Выберите закладку **Права**, если вы хотите изменить права группы доверия, регулирующие доступ к процессам и объектам операционной системы.

   Сетевую активность программ контролирует Сетевой экран с помощью *сетевых правил*.
7. Для нужного ресурса в графе соответствующего действия по правой клавише мыши откройте контекстное меню и выберите нужный пункт: **Наследовать**, **Разрешать** (), **Запрещать** ().

8. Если вы хотите контролировать использование ресурсов компьютера, выберите пункт **Записывать в отчет** ( ).

   Kaspersky Endpoint Security будет записывать информацию о работе компонента Предотвращение вторжений. Отчеты содержат информацию о выполнении программой операций с ресурсами компьютера (разрешено или запрещено). Также отчеты содержат информацию о программах, которые используют каждый ресурс.

9. Сохраните внесенные изменения.

В результате права группы доверия будут изменены. Далее Kaspersky Endpoint Security будет блокировать действия программы в зависимости от группы доверия. Группе доверия будет присвоен статус (*Настройки пользователя*).

Выбор группы доверия для программ, запускаемых до Kaspersky Endpoint Security

Для программ, запущенных до Kaspersky Endpoint Security, контролируется только сетевая активность. Контроль осуществляется согласно сетевым правилам, установленным в параметрах Сетевого экрана. Чтобы указать, какими сетевыми правилами должен регулироваться контроль сетевой активности таких программ, необходимо выбрать группу доверия.

Как выбрать группу доверия для программ, запускаемых до Kaspersky Endpoint Security, в интерфейсе программы:

1. В нижней части главного окна программы нажмите на кнопку .
2. В окне параметров программы выберите раздел **Защита → Продвинутая защита → Предотвращение вторжений**.
3. В блоке **Программы, запускаемые до Kaspersky Endpoint Security для Windows, автоматически помещаются в группу доверия: <группа доверия>** выберите нужную группу доверия (см. раздел "Приложение 2. Группы доверия программ" на стр. 279).
4. Сохраните внесенные изменения.

В результате программа, запускаемая до Kaspersky Endpoint Security, будет помещена в другую группу доверия. Далее Kaspersky Endpoint Security будет блокировать действия программы в зависимости от группы доверия.

Выбор группы доверия для неизвестных программ

Во время первого запуска программы компонент Предотвращение вторжений определяет группу доверия (см. раздел "Приложение 2. Группы доверия программ" на стр. 279) для программы. Если у вас отсутствует доступ в интернет или в Kaspersky Security Network нет информации об этой программе, то Kaspersky Endpoint Security по умолчанию помещает программу в группу "Слабые ограничения". При обнаружении в KSN информации о ранее неизвестной программе Kaspersky Endpoint Security обновит права программы. После этого вы можете изменить права программы вручную (см. раздел "Работа с правами программ" на стр. 98).

Как выбрать группу доверия для неизвестных программ в интерфейсе программы:

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Защита** → **Продвинутая защита** → **Предотвращение вторжений**.
3. В блоке **Группа доверия для неизвестных программ** выберите нужную группу доверия.

   Если участие в Kaspersky Security Network включено (см. раздел "Включение и выключение использования Kaspersky Security Network" на стр. 81), Kaspersky Endpoint Security отправляет запрос о репутации программы в KSN при каждом запуске программы. На основе полученного ответа программа может быть перемещена в группу доверия, отличную от заданной в параметрах компонента Предотвращение вторжений.
4. Используйте флажок **Обновлять права для ранее неизвестных программ из базы KSN**, чтобы настроить автоматическое обновление прав неизвестных программы.
5. Сохраните внесенные изменения.

Выбор группы доверия для программ с цифровой подписью

Kaspersky Endpoint Security всегда помещает программы, подписанные сертификатами Microsoft или сертификатами "Лаборатории Касперского", в группу доверия "Доверенные".

Как выбрать группу доверия для программ с цифровой подписью в интерфейсе программы:

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Защита** → **Продвинутая защита** → **Предотвращение вторжений**.
3. В блоке **Правила обработки программ** используйте флажок **Доверять программам, имеющим цифровую подпись**, чтобы включить или выключить автоматическое перемещение программ с цифровой подписью доверенных производителей в группу доверия "Доверенные".

   Доверенные производители – производители, которые включены в список доверенных "Лабораторией Касперского". Также вы можете добавить сертификат производителя в доверенное системное хранилище сертификатов вручную (см. раздел "Использование доверенного системного хранилища сертификатов" на стр. 203).

   Если флажок снят, компонент Предотвращение вторжений не считает программы с цифровой подписью доверенными и распределяет их по группам доверия (см. раздел "Приложение 2. Группы доверия программ" на стр. 279) на основании других параметров.
4. Сохраните внесенные изменения.

Работа с правами программ

По умолчанию для контроля работы программы применяются права программ, определенные для той группы доверия (см. раздел "Приложение 2. Группы доверия программ" на стр. 279), в которую Kaspersky Endpoint Security поместил программу при первом ее запуске. При необходимости вы можете изменить права программ для всей группы доверия (см. раздел "Настройка прав группы доверия" на стр. 96), для отдельной программы или группы программ внутри группы доверия.

Права программ, заданные вручную, имеют более высокий приоритет, чем права программ, определенные для группы доверия. То есть, если права программы, заданные вручную, отличаются от прав программ, определенных для группы доверия, компонент Предотвращение вторжения контролирует работу программы в соответствии с правами программ, заданными вручную.

Правила, которые вы создаете для программ, наследуются дочерними программами. Например, если вы запретили любую сетевую активность программе cmd.exe, этот запрет будет распространятся на программу notepad.exe, если она была запущена с помощью cmd.exe. При опосредованном запуске программы (если программа не является дочерней по отношению к программе, из которой она запускается), правила унаследованы не будут.

Как изменить права программы в интерфейсе программы:

1. В нижней части главного окна программы нажмите на кнопку .
2. В окне параметров программы выберите раздел **Защита** → **Продвинутая защита** → **Предотвращение вторжений**.
3. Нажмите на кнопку **Управление программами**.

   Откроется список установленных программ.
4. Выберите нужную программу.
5. В контекстном меню программы выберите пункт **Подробности и правила**.

   Откроются свойства программы.
6. Выполните одно из следующих действий:
   - Выберите закладку **Файлы и системный реестр**, если вы хотите изменить права группы доверия, регулирующие операции с реестром операционной системы, файлами пользователя и параметрами программ.
   - Выберите закладку **Права**, если вы хотите изменить права группы доверия, регулирующие доступ к процессам и объектам операционной системы.
7. Для нужного ресурса в графе соответствующего действия по правой клавише мыши откройте контекстное меню и выберите нужный пункт: **Наследовать**, **Разрешать** (), **Запрещать** ().
8. Если вы хотите контролировать использование ресурсов компьютера, выберите пункт **Записывать в отчет** ().

   Kaspersky Endpoint Security будет записывать информацию о работе компонента Предотвращение вторжений. Отчеты содержат информацию о выполнении программой операций с ресурсами компьютера (разрешено или запрещено). Также отчеты содержат информацию о программах, которые используют каждый ресурс.
9. Выберите закладку **Исключения** и настройте дополнительные параметры программы (см. таблицу ниже).
10. Сохраните внесенные изменения.

Таблица 3. Дополнительные параметры программы

Параметр	Описание
Не проверять открываемые файлы	Kaspersky Endpoint Security исключает из проверки все файлы, открываемые с помощью программы. Например, если вы используете программы резервного копирования файлов, функция позволит снизить потребление ресурсов компьютера Kaspersky Endpoint Security.

Параметр	Описание
Не контролировать активные программы	Kaspersky Endpoint Security не контролирует файловую и сетевую активности программы в операционной системе. Контроль за активностью программы выполняют следующие компоненты: Анализ поведения (на стр. 87), Защита от эксплойтов (на стр. 91), Предотвращение вторжений (на стр. 93), Откат вредоносных действий (на стр. 105) и Сетевой экран.
Не наследовать ограничения родительского процесса (программы)	Kaspersky Endpoint Security не применяет ограничения к процессу, которые настроены для родительского процесса. Родительский процесс запускает программа, для которой настроены права программы (см. раздел "Работа с правами программ" на стр. 98) (Предотвращение вторжений) и сетевые правила программы (Сетевой экран).
Не контролировать активность дочерних программ	Kaspersky Endpoint Security не контролирует файловую и сетевую активности программ, которые запускает программа.
Разрешить взаимодействие с интерфейсом Kaspersky Endpoint Security	Самозащита Kaspersky Endpoint Security (на стр. 214) блокирует все попытки управления службами программы с удаленного компьютера. Если флажок установлен, то программе удаленного доступа к компьютеру разрешено управлять параметрами Kaspersky Endpoint Security через интерфейс Kaspersky Endpoint Security.
Не проверять зашифрованный трафик / Не проверять весь трафик	Kaspersky Endpoint Security исключает из проверки сетевой трафик, инициируемый программой. Вы можете исключить из проверки весь трафик или только зашифрованный трафик. Также вы можете исключить из проверки отдельные IP-адреса или номера портов.

Защита ресурсов ОС и персональных данных

Компонент Предотвращение вторжений управляет правами программ на операции над различными категориями ресурсов операционной системы и персональных данных. Специалисты "Лаборатории Касперского" выделили предустановленные категории защищаемых ресурсов. Например, в категории *Операционная система* есть подкатегория *Параметры автозапуска*, где перечислены все ключи реестра, относящиеся к автозапуску программ. Вы не можете изменять или удалять предустановленные категории защищаемых ресурсов и относящиеся к ним защищаемые ресурсы.

Как добавить защищаемый ресурс в интерфейсе программы:

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Защита** → **Продвинутая защита** → **Предотвращение вторжений**.
3. Нажмите на кнопку **Управление ресурсами**.

   Откроется список защищаемых ресурсов.

4. Выберите категорию защищаемых ресурсов, в которую вы хотите добавить новый защищаемый ресурс.

   Если вы хотите добавить вложенную категорию, нажмите на кнопку **Добавить** → **Категорию**.

5. Нажмите на кнопку **Добавить** и в раскрывающемся списке выберите тип ресурса, который вы хотите добавить: **Файл или папку** или **Ключ реестра**.

6. В открывшемся окне выберите файл, папку или ключ реестра.

   Вы можете посмотреть права доступа программ к добавленным ресурсам. Для этого выберите добавленный ресурс в левой части окна и Kaspersky Endpoint Security покажет список программ и права доступа для каждой из программ. Также вы можете выключить контроль действия программ на операции с ресурсами кнопкой **Выключить контроль** в графе **Статус**.

7. Сохраните внесенные изменения.

В результате Kaspersky Endpoint Security будет контролировать доступ к добавленным ресурсам операционной системы и персональных данных. Kaspersky Endpoint Security контролирует доступ программы к ресурсам на основании присвоенной группы доверия. Вы также можете изменить группу доверия для программы (см. раздел "Изменение группы доверия для программы" на стр. 95).

Удаление информации о неиспользуемых программах

Kaspersky Endpoint Security контролирует работу программ с помощью прав программ. Права программы определены группой доверия. Kaspersky Endpoint Security помещает программу в группу доверия (см. раздел "Приложение 2. Группы доверия программ" на стр. 279) при первом запуске. Вы можете изменить группу доверия для программы вручную (см. раздел "Работа с правами программ" на стр. 98). Также вы можете настроить права для отдельной программы вручную (см. раздел "Работа с правами программ" на стр. 98). Таким образом, Kaspersky Endpoint Security хранит следующую информацию о программе: группа доверия и права программы.

Kaspersky Endpoint Security автоматически удаляет информацию о неиспользуемых программах для экономии ресурсов компьютера. Kaspersky Endpoint Security удаляет информацию о программах по следующим правилам:

- Если группа доверия и права программы определены автоматически, Kaspersky Endpoint Security удаляет информацию об этой программе через 30 дней. Изменить время хранения информации о программе или выключить автоматическое удаление невозможно.
- Если вы вручную поместили программу в группу доверия или настроили права доступа, Kaspersky Endpoint Security удаляет информацию об этой программе через 60 дней (значение по умолчанию). Вы можете изменить время хранения информации о программе или выключить автоматическое удаление (см. инструкцию ниже).

При запуске программы, информация о которой была удалена, Kaspersky Endpoint Security исследует программу как при первом запуске.

Как настроить автоматическое удаление информации о неиспользуемых программах в интерфейсе программы:

1. В нижней части главного окна программы нажмите на кнопку .
2. В окне параметров программы выберите раздел **Защита** → **Продвинутая защита** → **Предотвращение вторжений**.

3. В блоке **Правила обработки программ** выполните одно из следующих действий:
   - Если вы хотите настроить автоматическое удаление, установите флажок **Удалять права для программ, не запускавшихся более N дней** и укажите нужное количество дней.

     Kaspersky Endpoint Security будет удалять информацию о тех программах, которые вы вручную поместили в группу доверия или для которых вы настроили права доступа, через заданное количество дней. Также Kaspersky Endpoint Security будет удалять информацию о программах, для которых группа доверия и права программы определены автоматически, через 30 дней.
   - Если вы хотите выключить автоматическое удаление, снимите флажок **Удалять права для программ, не запускавшихся более N дней**.

     Kaspersky Endpoint Security будет хранить информацию о тех программах, которые вы вручную поместили в группу доверия или для которых вы настроили права доступа, без ограничений по времени. Kaspersky Endpoint Security будет удалять информацию только о программах, для которых группа доверия и права программы определены автоматически, через 30 дней.
4. Сохраните внесенные изменения.

Мониторинг работы Предотвращения вторжений

Вы можете получать отчеты о работе компонента Предотвращение вторжений. Отчеты содержат информацию о выполнении программой операций с ресурсами компьютера (разрешено или запрещено). Также отчеты содержат информацию о программах, которые используют каждый ресурс.

Для мониторинга работы Предотвращения вторжений вам нужно включить запись в отчет. Например, вы можете включить отправку отчетов для отдельных программ в параметрах компонента Предотвращение вторжений (см. раздел "Работа с правами программ" на стр. 98).

При настройке мониторинга работы Предотвращения вторжения учитывайте нагрузку на сеть при отправке событий в Kaspersky Security Center. Также вы можете включить сохранение отчетов только в локальном журнале Kaspersky Endpoint Security.

Защита доступа к аудио и видео

Злоумышленники могут с помощью специальных программ пытаться получить доступ к устройствам записи аудио и видео (например, микрофоны или веб-камеры). Kaspersky Endpoint Security контролирует получение программами аудиосигнала и видеосигнала и защищает данные от несанкционированного перехвата.

По умолчанию Kaspersky Endpoint Security контролирует доступ программ к аудиосагналу и видеосигналу следующим образом:

- "Доверенные" и "Слабые ограничения" – получение аудиосигнала и видеосигнала с устройств разрешено по умолчанию.
- "Сильные ограничения" и "Недоверенные" – получение аудиосигнала и видеосигнала с устройств запрещено по умолчанию.

Вы можете вручную разрешать программам получать аудиосигнал и видеосигнал (см. раздел "Работа с правами программ" на стр. 98).

Особенности защиты аудиосигнала

Функциональность защиты аудиосигнала имеет следующие особенности:

- Для работы функциональности необходимо, чтобы был включен компонент Предотвращение вторжений (см. раздел "Включение и выключение Предотвращения вторжений" на стр. 94).
- Если программа начала получать аудиосигнал до запуска компонента Предотвращение вторжений, то Kaspersky Endpoint Security разрешает программе получение аудиосигнала и не показывает никаких уведомлений.
- Если вы поместили программу в группу "Недоверенные" или "Сильные ограничения" после того, как программа начала получать аудиосигнал, то Kaspersky Endpoint Security разрешает программе получение аудиосигнала и не показывает никаких уведомлений.
- При изменении параметров доступа программы к устройствам записи звука (например, программе было запрещено получение аудиосигнала (см. раздел "Работа с правами программ" на стр. 98)) требуется перезапуск этой программы, чтобы она перестала получать аудиосигнал.
- Контроль получения аудиосигнала с устройств записи звука не зависит от параметров доступа программ к веб-камере.
- Kaspersky Endpoint Security защищает доступ только к встроенным и внешним микрофонам. Другие устройства передачи звука не поддерживаются.
- Kaspersky Endpoint Security не гарантирует защиту аудиосигнала, передаваемого с таких устройств, как DSLR-камеры, портативные видеокамеры, экшн-камеры.
- При первом запуске программы Kaspersky Endpoint Security с момента ее установки воспроизведение или запись аудио и видео могут быть прерваны в программах записи или воспроизведения аудио и видео. Это необходимо для того, чтобы включилась функциональность контроля доступа программ к устройствам записи звука. Системная служба управления средствами работы со звуком будет перезапущена при первом запуске программы Kaspersky Endpoint Security.

Особенности доступа программ к веб-камерам

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

- Программа контролирует видео и статические изображения, полученные в результате обработки данных веб-камеры.
- Программа контролирует аудиосигнал, если он является частью видеопотока, получаемого с веб-камеры.
- Программа контролирует только веб-камеры, подключаемые по интерфейсу USB или IEEE1394 и отображаемые в Диспетчере устройств Windows как **Устройства обработки изображений** (англ. Imaging Device).
- Kaspersky Endpoint Security поддерживает следующие веб-камеры:
  - Logitech HD Webcam C270;
  - Logitech HD Webcam C310;
  - Logitech Webcam C210;
  - Logitech Webcam Pro 9000;
  - Logitech HD Webcam C525;

- Microsoft LifeCam VX-1000;
- Microsoft LifeCam VX-2000;
- Microsoft LifeCam VX-3000;
- Microsoft LifeCam VX-800;
- Microsoft LifeCam Cinema.

"Лаборатория Касперского" не гарантирует поддержку веб-камер, не указанных в этом списке.

kaspersky

Откат вредоносных действий

Компонент Откат вредоносных действий позволяет Kaspersky Endpoint Security выполнить откат действий, произведенных вредоносными программами в операционной системе.

Во время отката действий вредоносной программы в операционной системе Kaspersky Endpoint Security обрабатывает следующие типы активности вредоносной программы:

- **Файловая активность**

  Kaspersky Endpoint Security выполняет следующие действия:

  - удаляет исполняемые файлы, созданные вредоносной программой (на всех носителях, кроме сетевых дисков);
  - удаляет исполняемые файлы, созданные программами, в которые внедрилась вредоносная программа;
  - восстанавливает измененные или удаленные вредоносной программой файлы.

  Функциональность восстановления файлов имеет ряд ограничений.

- **Реестровая активность**

  Kaspersky Endpoint Security выполняет следующие действия:

  - удаляет разделы и ключи реестра, созданные вредоносной программой;
  - не восстанавливает измененные или удаленные вредоносной программой разделы и ключи реестра.

- **Системная активность**

  Kaspersky Endpoint Security выполняет следующие действия:

  - завершает процессы, которые запускала вредоносная программа;
  - завершает процессы, в которые внедрялась вредоносная программа;
  - не возобновляет процессы, которые остановила вредоносная программа.

- **Сетевая активность**

  Kaspersky Endpoint Security выполняет следующие действия:

  - запрещает сетевую активность вредоносной программы;
  - запрещает сетевую активность тех процессов, в которые внедрялась вредоносная программа.

Откат действий вредоносной программы может быть запущен компонентом Защита от файловых угроз (см. стр. 107), Анализ поведения (на стр. 87) или при антивирусной проверке (см. раздел "Проверка компьютера" на стр. 52).

Откат действий вредоносной программы затрагивает строго ограниченный набор данных. Откат не оказывает негативного влияния на работу операционной системы и целостность информации на вашем компьютере.

Как включить или выключить компонент Откат вредоносных действий в интерфейсе программы:

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Защита** → **Продвинутая защита** → **Откат вредоносных действий**.
3. Используйте переключатель **Откат вредоносных действий**, чтобы включить или выключить компонент.
4. Сохраните внесенные изменения.

В результате, если Откат вредоносных действий включен, Kaspersky Endpoint Security будет откатывать действия, которые вредоносные программы совершили в операционной системе.

kaspersky

Защита от файловых угроз

Компонент Защита от файловых угроз позволяет избежать заражения файловой системы компьютера. По умолчанию компонент Защита от файловых угроз постоянно находится в оперативной памяти компьютера. Компонент проверяет файлы на всех дисках компьютера, а также на подключенных дисках. Компонент обеспечивает защиту компьютера с помощью антивирусных баз, облачной службы Kaspersky Security Network (см. раздел "Включение и выключение использования Kaspersky Security Network" на стр. 81) и эвристического анализа.

Компонент проверяет файлы, к которым обращается пользователь или программа. При обнаружении вредоносного файла Kaspersky Endpoint Security блокирует операцию с файлом. Далее программа лечит или удаляет вредоносный файл, в зависимости от настройки компонента Защита от файловых угроз.

При обращении к файлу, содержимое которого расположено в облачном хранилище OneDrive, Kaspersky Endpoint Security загружает и проверяет содержимое этого файла.

В этом разделе

Включение и выключение Защиты от файловых угроз

По умолчанию компонент Защита от файловых угроз включен и работает в рекомендованном специалистами "Лаборатории Касперского" режиме. Для работы Защиты от файловых угроз Kaspersky Endpoint Security применяет разные наборы настроек. Наборы настроек, сохраненные в программе, называются *уровнями безопасности*: **Высокий**, **Рекомендуемый**, **Низкий**. Параметры уровня безопасности **Рекомендуемый** считаются оптимальными, они рекомендованы специалистами "Лаборатории Касперского" (см. таблицу ниже). Вы можете выбрать один из предустановленных уровней безопасности или настроить параметры уровня безопасности самостоятельно. После того как вы изменили параметры уровня безопасности, вы всегда можете вернуться к рекомендуемым параметрам уровня безопасности.

► *Чтобы включить или выключить компонент Защита от файловых угроз, выполните следующие действия:*

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Защита → Базовая защита → Защита от файловых угроз**.
3. Используйте переключатель **Защита от файловых угроз**, чтобы включить или выключить компонент.
4. Если вы включили компонент, в блоке **Уровень безопасности** выполните одно из следующих действий:
   - Если вы хотите применить один из предустановленных уровней безопасности, выберите его при помощи ползунка:
     - **Высокий**. Уровень безопасности файлов, при котором компонент Защита от файловых угроз максимально контролирует все открываемые, сохраняемые и запускаемые файлы. Компонент Защита от файловых угроз проверяет все типы файлов на всех жестких, сменных и сетевых дисках компьютера, а также архивы, установочные пакеты и вложенные OLE-объекты.
     - **Рекомендуемый**. Уровень безопасности файлов, который рекомендован для использования специалистами "Лаборатории Касперского". Компонент Защита от файловых угроз проверяет только файлы определенных форматов на всех жестких, сменных и сетевых дисках компьютера, а также вложенные OLE-объекты, компонент Защита от файловых угроз не проверяет архивы и установочные пакеты. Значения параметров для рекомендуемого уровня безопасности см. в таблице ниже.
     - **Низкий**. Уровень безопасности файлов, параметры которого обеспечивают максимальную скорость проверки. Компонент Защита от файловых угроз проверяет только файлы с определенными расширениями на всех жестких, сменных и сетевых дисках компьютера, компонент Защита от файловых угроз не проверяет составные файлы.
   - Если вы хотите настроить уровень безопасности самостоятельно, нажмите на кнопку **Расширенная настройка** и задайте параметры работы компонента.

     Вы можете восстановить значения предустановленных уровней безопасности по кнопке **Восстановить рекомендуемый уровень безопасности** в верхней части окна.
5. Сохраните внесенные изменения.

Таблица 4. Параметры Защиты от файловых угроз, рекомендованные специалистами "Лаборатории Касперского", (рекомендованный уровень безопасности)

Параметр	Значение	Описание
Типы файлов	**Файлы, проверяемые по формату**	Если выбран этот параметр, Kaspersky Endpoint Security проверяет только потенциально заражаемые файлы. Перед началом поиска вредоносного кода в файле выполняется анализ его внутреннего заголовка на предмет формата файла (например, TXT, DOC, EXE). В процессе проверки учитывается также расширение файла.

Параметр	Значение	Описание
Эвристический анализ	**Поверхностный**	Технология обнаружения угроз, которые невозможно определить с помощью текущей версии баз программ "Лаборатории Касперского". Позволяет находить файлы, которые могут содержать неизвестный вирус или новую модификацию известного вируса. Во время проверки файлов на наличие вредоносного кода эвристический анализатор выполняет инструкции в исполняемых файлах. Количество инструкций, которые выполняет эвристический анализатор, зависит от заданного уровня эвристического анализа. Уровень эвристического анализа обеспечивает баланс между тщательностью поиска новых угроз, степенью загрузки ресурсов операционной системы и длительностью эвристического анализа.
Проверять только новые и измененные файлы	**Включено**	Проверка только новых файлов и тех файлов, которые изменились после предыдущей проверки. Это позволит сократить время выполнения проверки. Такой режим проверки распространяется как на простые, так и на составные файлы.
Технология iSwift	**Включено**	Технология, позволяющая увеличить скорость проверки за счет исключения из нее некоторых файлов. Файлы исключаются из проверки по специальному алгоритму, учитывающему дату выпуска баз Kaspersky Endpoint Security, дату предыдущей проверки файла, а также изменение параметров проверки. Технология iSwift является развитием технологии iChecker для файловой системы NTFS.
Технология iChecker	**Включено**	Технология, позволяющая увеличить скорость проверки за счет исключения из нее некоторых файлов. Файлы исключаются из проверки по специальному алгоритму, учитывающему дату выпуска баз Kaspersky Endpoint Security, 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).
Проверять файлы офисных форматов	**Включено**	Проверка файлов Microsoft Office (DOC, DOCX, XLS, PPT и других). К файлам Microsoft Office также относятся OLE-объекты.
Режим проверки	**Интеллектуальный**	Режим проверки, при котором Защита от файловых угроз проверяет объект на основании анализа операций, выполняемых над объектом. Например, при работе с документом Microsoft Office Kaspersky Endpoint Security проверяет файл при первом открытии и при последнем закрытии. Все промежуточные операции перезаписи файла из проверки исключаются.

Параметр	Значение	Описание
Действие при обнаружении угрозы	**Лечить; удалять, если лечение невозможно**	Если выбран этот вариант действия, то Kaspersky Endpoint Security автоматически пытается вылечить все обнаруженные зараженные файлы. Если лечение невозможно, то Kaspersky Endpoint Security их удаляет.

Автоматическая приостановка Защиты от файловых угроз

Вы можете настроить автоматическую приостановку Защиты от файловых угроз в указанное время или во время работы с определенными программами.

Приостановка работы Защиты от файловых угроз при конфликте с определенными программами является экстренной мерой. Если во время работы компонента возникают какие-либо конфликты, рекомендуется обратиться в Службу технической поддержки "Лаборатории Касперского" (https://companyaccount.kaspersky.com). Специалисты помогут вам наладить совместную работу компонента Защита от файловых угроз с другими программами на вашем компьютере.

► *Чтобы настроить автоматическую приостановку работы Защиты от файловых угроз, выполните следующие действия:*

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Защита → Базовая защита → Защита от файловых угроз**.
3. Нажмите на кнопку **Расширенная настройка**.
4. В блоке **Приостановка Защиты от файловых угроз** перейдите по ссылке **Приостановить Защиту от файловых угроз**.
5. В открывшемся окне настройте параметры приостановки работы Защиты от файловых угроз:
   a. Настройте расписание автоматической приостановки Защиты от файловых угроз.
   b. Сформируйте список программ, во время работы которых Защиту от файловых угроз следует приостанавливать.
6. Сохраните внесенные изменения.

Изменение действия компонента Защита от файловых угроз над зараженными файлами

По умолчанию компонент Защита от файловых угроз автоматически пытается вылечить все обнаруженные зараженные файлы. Если лечение невозможно, то компонент Защита от файловых угроз удаляет эти файлы.

► *Чтобы изменить действие компонента Защита от файловых угроз над зараженными файлами, выполните следующие действия:*

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Защита → Базовая защита → Защита от файловых угроз**.
3. В блоке **Действие при обнаружении угрозы** выберите нужный вариант:
   - **Лечить; удалять, если лечение невозможно**. Если выбран этот вариант действия, то Kaspersky Endpoint Security автоматически пытается вылечить все обнаруженные зараженные файлы. Если лечение невозможно, то Kaspersky Endpoint Security их удаляет.
   - **Лечить; блокировать, если лечение невозможно**. Если выбран этот вариант действия, то Kaspersky Endpoint Security автоматически пытается вылечить все обнаруженные зараженные файлы. Если лечение невозможно, то Kaspersky Endpoint Security добавляет информацию об обнаруженных зараженных файлах в список активных угроз.
   - **Блокировать**. Если выбран этот вариант действия, то компонент Защита от файловых угроз автоматически блокирует зараженные файлы без попытки их вылечить.

   Перед лечением или удалением зараженного файла Kaspersky Endpoint Security формирует его резервную копию на тот случай, если впоследствии понадобится восстановить файл или появится возможность его вылечить (см. раздел "Восстановление файлов из резервного хранилища" на стр. 205).
4. Сохраните внесенные изменения.

Формирование области защиты компонента Защита от файловых угроз

Под областью защиты подразумеваются объекты, которые проверяет компонент во время своей работы. Область защиты разных компонентов имеет разные свойства. Свойствами области защиты компонента Защита от файловых угроз являются местоположение и тип проверяемых файлов. По умолчанию компонент Защита от файловых угроз проверяет только потенциально заражаемые файлы, запускаемые со всех жестких, съемных и сетевых дисков компьютера.

Выбирая тип проверяемых файлов, нужно учитывать следующее:

1. Вероятность внедрения вредоносного кода в файлы некоторых форматов и его последующей активации низка (например, формат TXT). В то же время существуют форматы файлов, которые содержат исполняемый код (например, форматы EXE, DLL). Также исполняемый код могут содержать форматы файлов, которые для этого не предназначены (например, формат DOC). Риск внедрения в такие файлы вредоносного кода и его активации высок.
2. Злоумышленник может отправить вирус или другую программу, представляющую угрозу, на ваш компьютер в исполняемом файле, переименованном в файл с расширением txt. Если вы выбрали проверку файлов по расширению, то в процессе проверки программа пропускает такой файл. Если же выбрана проверка файлов по формату, то вне зависимости от расширения Kaspersky Endpoint Security анализирует заголовок файла. Если в результате выясняется, что файл имеет формат исполняемого файла (например, EXE), то программа проверяет его.

► *Чтобы сформировать область защиты, выполните следующие действия:*

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Защита → Базовая защита → Защита от файловых угроз**.
3. Нажмите на кнопку **Расширенная настройка**.
4. В блоке **Типы файлов** укажите тип файлов, которые вы хотите проверять компонентом Защита от файловых угроз:
   - **Все файлы**. Если выбран этот параметр, Kaspersky Endpoint Security проверяет все файлы без исключения (любых форматов и расширений).
   - **Файлы, проверяемые по формату**. Если выбран этот параметр, Kaspersky Endpoint Security проверяет только потенциально заражаемые файлы. Перед началом поиска вредоносного кода в файле выполняется анализ его внутреннего заголовка на предмет формата файла (например, TXT, DOC, EXE). В процессе проверки учитывается также расширение файла.
   - **Файлы, проверяемые по расширению**. Если выбран этот параметр, Kaspersky Endpoint Security проверяет только потенциально заражаемые файлы. Формат файла определяется на основании его расширения.
5. Перейдите по ссылке **Изменить область защиты**.
6. В открывшемся окне выберите объекты, которые вы хотите добавить в область защиты или исключить из нее.

   Вы не можете удалить или изменить объекты, включенные в область защиты по умолчанию.

7. Если вы хотите добавить новый объект в область защиты, выполните следующие действия:
   a. Нажмите на кнопку **Добавить**.

      Откроется дерево папок.

   b. Выберите объект и нажмите на кнопку **Выбрать**.

   Вы можете исключить объект из проверки, не удаляя его из списка объектов области проверки. Для этого снимите флажок рядом с ним.
8. Сохраните внесенные изменения.

Использование методов проверки

Во время своей работы Kaspersky Endpoint Security использует метод проверки Машинное обучение и сигнатурный анализ. В процессе сигнатурного анализа Kaspersky Endpoint Security сравнивает найденный объект с записями в базах программы. В соответствии с рекомендациями специалистов "Лаборатории Касперского" метод проверки Машинное обучение и сигнатурный анализ всегда включен.

Чтобы повысить эффективность защиты, вы можете использовать эвристический анализ. Во время проверки файлов на наличие вредоносного кода эвристический анализатор выполняет инструкции в исполняемых файлах. Количество инструкций, которые выполняет эвристический анализатор, зависит от заданного уровня эвристического анализа. Уровень эвристического анализа обеспечивает баланс между тщательностью поиска новых угроз, степенью загрузки ресурсов операционной системы и длительностью эвристического анализа.

► *Чтобы настроить использование эвристического анализа в работе компонента Защита от файловых угроз, выполните следующие действия:*

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Защита** → **Базовая защита** → **Защита от файловых угроз**.
3. Нажмите на кнопку **Расширенная настройка**.
4. В блоке **Методы проверки** установите флажок **Эвристический анализ**, если вы хотите, чтобы программа использовала эвристический анализ для защиты от файловых угроз. Далее при помощи ползунка задайте уровень эвристического анализа: **Поверхностный**, **Средний** или **Глубокий**.
5. Сохраните внесенные изменения.

Использование технологий проверки в работе компонента Защита от файловых угроз

► *Чтобы настроить использование технологий проверки в работе компонента Защита от файловых угроз, выполните следующие действия:*

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Защита** → **Базовая защита** → **Защита от файловых угроз**.
3. Нажмите на кнопку **Расширенная настройка**.
4. В блоке **Технологии проверки** установите флажки около названий технологий, которые вы хотите использовать для защиты от файловых угроз:
   - **Технология iSwift**. Технология, позволяющая увеличить скорость проверки за счет исключения из нее некоторых файлов. Файлы исключаются из проверки по специальному алгоритму, учитывающему дату выпуска баз Kaspersky Endpoint Security, дату предыдущей проверки файла, а также изменение параметров проверки. Технология iSwift является развитием технологии iChecker для файловой системы NTFS.
   - **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 Endpoint Security, 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).
5. Сохраните внесенные изменения.

kaspersky

Оптимизация проверки файлов

Вы можете оптимизировать проверку файлов компонентом Защита от файловых угроз: сократить время проверки и увеличить скорость работы Kaspersky Endpoint Security. Этого можно достичь, если проверять только новые файлы и те файлы, которые изменились с момента их предыдущего анализа. Такой режим проверки распространяется как на простые, так и на составные файлы.

Вы также можете включить использование технологий iChecker и iSwift (см. раздел "Использование технологий проверки в работе компонента Защита от файловых угроз" на стр. 113), которые позволяют оптимизировать скорость проверки файлов за счет исключения из проверки файлов, не измененных с момента их последней проверки.

► *Чтобы оптимизировать проверку файлов, выполните следующие действия:*

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Защита → Базовая защита → Защита от файловых угроз**.
3. Нажмите на кнопку **Расширенная настройка**.
4. В блоке **Оптимизация проверки** установите флажок **Проверять только новые и измененные файлы**.
5. Сохраните внесенные изменения.

Проверка составных файлов

Распространенной практикой сокрытия вирусов и других программ, представляющих угрозу, является внедрение их в составные файлы, например, архивы или базы данных. Чтобы обнаружить скрытые таким образом вирусы и другие программы, представляющие угрозу, составной файл нужно распаковать, что может привести к снижению скорости проверки. Вы можете ограничить типы проверяемых составных файлов, таким образом увеличив скорость проверки.

Способ обработки зараженного составного файла (лечение или удаление) зависит от типа файла. Компонент Защита от файловых угроз лечит составные файлы форматов RAR, ARJ, ZIP, CAB, LHA и удаляет файлы всех остальных форматов (кроме почтовых баз).

► *Чтобы настроить проверку составных файлов, выполните следующие действия:*

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Защита → Базовая защита → Защита от файловых угроз**.
3. Нажмите на кнопку **Расширенная настройка**.
4. В блоке **Проверка составных файлов** укажите, какие составные файлы вы хотите проверять: архивы, установочные пакеты или файлы офисных форматов.

5. Если режим проверки только новых и измененных файлов выключен (см. раздел "Оптимизация проверки файлов" на стр. 113), настройте параметры проверки каждого типа составных файлов: проверка всех файлов этого типа или только новых файлов.

   Если режим проверки только новых и измененных файлов включен, Kaspersky Endpoint Security проверяет только новые и измененные файлы всех типов составных файлов.

6. Настройте дополнительные параметры проверки составных файлов:

   - **Не распаковывать составные файлы большого размера**.

     Если флажок установлен, то Kaspersky Endpoint Security не проверяет составные файлы, размеры которых больше заданного значения.

     Если флажок снят, Kaspersky Endpoint Security проверяет составные файлы любого размера.

     > Kaspersky Endpoint Security проверяет файлы больших размеров, извлеченные из архивов, независимо от того, установлен ли флажок **Не распаковывать составные файлы большого размера**.

   - **Распаковывать составные файлы в фоновом режиме**.

     Если флажок установлен, Kaspersky Endpoint Security предоставляет доступ к составным файлам, размер которых превышает заданное значение, до проверки этих файлов. При этом Kaspersky Endpoint Security в фоновом режиме распаковывает и проверяет составные файлы.

     Kaspersky Endpoint Security предоставляет доступ к составным файлам, размер которых меньше данного значения, только после распаковки и проверки этих файлов.

     Если флажок снят, Kaspersky Endpoint Security предоставляет доступ к составным файлам только после распаковки и проверки файлов любого размера.

7. Сохраните внесенные изменения.

Изменение режима проверки файлов

Под *режимом проверки* подразумевается условие, при котором компонент Защита от файловых угроз начинает проверять файлы. По умолчанию Kaspersky Endpoint Security использует интеллектуальный режим проверки файлов. Работая в этом режиме проверки файлов, компонент Защита от файловых угроз принимает решение о проверке файлов на основании анализа операций, которые пользователь, программа от имени пользователя (под учетными данными которого был осуществлен вход в операционную систему или другого пользователя) или операционная система выполняет над файлами. Например, работая с документом Microsoft Office Word, Kaspersky Endpoint Security проверяет файл при первом открытии и при последнем закрытии. Все промежуточные операции перезаписи файла из проверки исключаются.

► *Чтобы изменить режим проверки файлов, выполните следующие действия:*

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Защита → Базовая защита → Защита от файловых угроз**.
3. Нажмите на кнопку **Расширенная настройка**.

4. В блоке **Режим проверки** выберите нужный режим:
   - **Интеллектуальный**. Режим проверки, при котором Защита от файловых угроз проверяет объект на основании анализа операций, выполняемых над объектом. Например, при работе с документом Microsoft Office Kaspersky Endpoint Security 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 Защита от файловых угроз проверяет объекты при попытке их открыть или изменить.
   - **При доступе**. Режим проверки, при котором Защита от файловых угроз проверяет объекты только при попытке их открыть.
   - **При выполнении**. Режим проверки, при котором Защита от файловых угроз проверяет объекты только при попытке их запустить.
5. Сохраните внесенные изменения.

Защита от веб-угроз

Этот компонент доступен, если программа Kaspersky Endpoint Security установлена на компьютере под управлением операционной системы Windows для рабочих станций. Этот компонент недоступен, если программа Kaspersky Endpoint Security установлена на компьютере под управлением операционной системы Windows для серверов.

Компонент Защита от веб-угроз предотвращает загрузку вредоносных файлов из интернета, а также блокирует вредоносные и фишинговые веб-сайты. Компонент обеспечивает защиту компьютера с помощью антивирусных баз, облачной службы Kaspersky Security Network (см. раздел "Включение и выключение использования Kaspersky Security Network" на стр. 81) и эвристического анализа.

Kaspersky Endpoint Security проверяет HTTP-, HTTPS- и FTP-трафик. Kaspersky Endpoint Security проверяет URL- и IP-адреса. Вы можете задать порты, которые Kaspersky Endpoint Security будет контролировать, (см. раздел "Контроль сетевых портов" на стр. 182) или выбрать все порты.

Для контроля HTTPS-трафика нужно включить проверку защищенных соединений (см. раздел "Настройка параметров проверки защищенных соединений" на стр. 140).

При попытке пользователя открыть вредоносный или фишинговый веб-сайт, Kaspersky Endpoint Security заблокирует доступ и покажет предупреждение (см. рис. ниже).

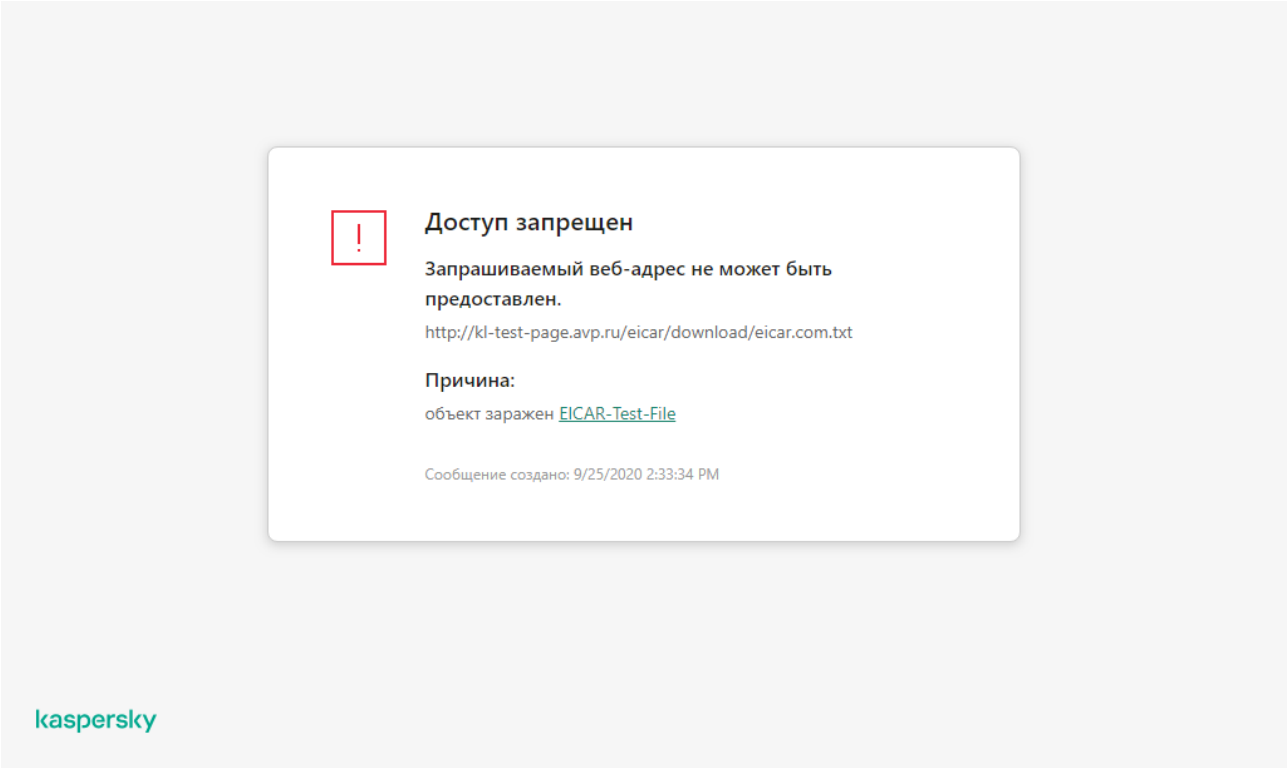


Рисунок 12. Сообщение о запрете доступа к веб-сайту

kaspersky

В этом разделе

Включение и выключение Защиты от веб-угроз

По умолчанию компонент Защита от веб-угроз включен и работает в рекомендованном специалистами "Лаборатории Касперского" режиме. Для работы Защиты от веб-угроз Kaspersky Endpoint Security применяет разные наборы настроек. Наборы настроек, сохраненные в программе, называются *уровнями безопасности*: **Высокий**, **Рекомендуемый**, **Низкий**. Параметры уровня безопасности веб-трафика **Рекомендуемый** считаются оптимальными, они рекомендованы специалистами "Лаборатории Касперского" (см. таблицу ниже). Вы можете выбрать один из предустановленных уровней безопасности веб-трафика, получаемых или передаваемых по протоколам HTTP и FTP, или настроить уровень безопасности веб-трафика самостоятельно. После того как вы изменили параметры уровня безопасности веб-трафика, вы всегда можете вернуться к рекомендуемым параметрам уровня безопасности веб-трафика.

► *Чтобы включить или выключить компонент Защита от веб-угроз выполните следующие действия:*

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Защита** → **Базовая защита** → **Защита от веб-угроз**.
3. Используйте переключатель **Защита от веб-угроз**, чтобы включить или выключить компонент.
4. Если вы включили компонент, в блоке **Уровень безопасности** выполните одно из следующих действий:
   - Если вы хотите применить один из предустановленных уровней безопасности, выберите его при помощи ползунка:
     - **Высокий**. Уровень безопасности веб-трафика, при котором компонент Защита от веб-угроз максимально проверяет веб-трафик, поступающий на компьютер по HTTP- и FTP-протоколам. Защита от веб-угроз детально проверяет все объекты веб-трафика, используя полный набор баз программы, а также выполняет максимально глубокий эвристический анализ.
     - **Рекомендуемый**. Уровень безопасности веб-трафика, обеспечивающий оптимальный баланс между производительностью Kaspersky Endpoint Security и безопасностью веб-трафика. Компонент Защита от веб-угроз выполняет эвристический анализ на уровне **Средний**. Этот уровень безопасности веб-трафика рекомендован для использования специалистами "Лаборатории Касперского". Значения параметров для рекомендуемого уровня безопасности см. в таблице ниже.

- **Низкий**. Уровень безопасности веб-трафика, параметры которого обеспечивают максимальную скорость проверки веб-трафика. Компонент Защита от веб-угроз выполняет эвристический анализ на уровне **Поверхностный**.

- Если вы хотите настроить уровень безопасности самостоятельно, нажмите на кнопку **Расширенная настройка** и задайте параметры работы компонента.

  Вы можете восстановить значения предустановленных уровней безопасности по кнопке **Восстановить рекомендуемый уровень безопасности** в верхней части окна.

5. Сохраните внесенные изменения.

Таблица 5. Параметры Защиты от веб-угроз, рекомендованные специалистами "Лаборатории Касперского", (рекомендованный уровень безопасности)

Параметр	Значение	Описание
Проверять ссылки по базе вредоносных веб-адресов	**Включено**	Проверка ссылок на принадлежность к базе вредоносных веб-адресов позволяет отследить веб-сайты, которые находятся в списке запрещенных веб-адресов. База вредоносных веб-адресов формируется специалистами "Лаборатории Касперского", входит в комплект поставки программы и пополняется при обновлении баз Kaspersky Endpoint Security.
Проверять веб-адрес по базе фишинговых веб-адресов	**Включено**	В состав базы фишинговых веб-адресов включены веб-адреса известных на настоящее время веб-сайтов, которые используются для фишинг-атак. Базу фишинговых веб-адресов специалисты "Лаборатории Касперского" пополняют веб-адресами, предоставленными международной организацией по борьбе с фишингом The Anti-Phishing Working Group. База фишинговых веб-адресов входит в комплект поставки программы и пополняется при обновлении баз Kaspersky Endpoint Security.

Параметр	Значение	Описание
Использовать эвристический анализ (Защита от веб-угроз)	**Средний**	Технология обнаружения угроз, которые невозможно определить с помощью текущей версии баз программ "Лаборатории Касперского". Позволяет находить файлы, которые могут содержать неизвестный вирус или новую модификацию известного вируса. Во время проверки веб-трафика на наличие вирусов и других программ, представляющих угрозу эвристический анализатор выполняет инструкции в исполняемых файлах. Количество инструкций, которые выполняет эвристический анализатор, зависит от заданного уровня эвристического анализа. Уровень эвристического анализа обеспечивает баланс между тщательностью поиска новых угроз, степенью загрузки ресурсов операционной системы и длительностью эвристического анализа.
Использовать эвристический анализ (Анти-Фишинг)	**Включено**	Технология обнаружения угроз, которые невозможно определить с помощью текущей версии баз программ "Лаборатории Касперского". Позволяет находить файлы, которые могут содержать неизвестный вирус или новую модификацию известного вируса.
Действие при обнаружении угрозы	**Запрещать загрузку**	Если выбран этот вариант, то в случае обнаружения в веб-трафике зараженного объекта компонент Защита от веб-угроз блокирует доступ к объекту и показывает сообщение в браузере.

Изменение действия над вредоносными объектами веб-трафика

По умолчанию в случае обнаружения в веб-трафике зараженного объекта компонент Защита от веб-угроз блокирует доступ к объекту и выводит на экран окно уведомления о блокировке.

► *Чтобы изменить действие над вредоносными объектами веб-трафика, выполните следующие действия:*

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Защита → Базовая защита → Защита от веб-угроз**.

3. В блоке **Действие при обнаружении угрозы** выберите вариант действия, которое Kaspersky Endpoint Security выполняет над вредоносными объектами веб-трафика:
   - **Запрещать загрузку**. Если выбран этот вариант, то в случае обнаружения в веб-трафике зараженного объекта компонент Защита от веб-угроз блокирует доступ к объекту и показывает сообщение в браузере.
   - **Информировать**. Если выбран этот вариант, то в случае обнаружения в веб-трафике зараженного объекта, Kaspersky Endpoint Security разрешает загрузку этого объекта на компьютер и добавляет информацию о зараженном объекте в список активных угроз.
4. Сохраните внесенные изменения.

Проверка ссылок по базам фишинговых и вредоносных веб-адресов

Проверка ссылок на принадлежность к фишинговым веб-адресам позволяет избежать *фишинговых атак*. Частным примером фишинговых атак может служить сообщение электронной почты якобы от банка, клиентом которого вы являетесь, со ссылкой на официальный веб-сайт банка в интернете. Воспользовавшись ссылкой, вы попадаете на точную копию веб-сайта банка и даже можете видеть его веб-адрес в браузере, однако находитесь на фиктивном веб-сайте. Все ваши дальнейшие действия на веб-сайте отслеживаются и могут быть использованы для кражи ваших денежных средств.

Поскольку ссылка на фишинговый веб-сайт может содержаться не только в сообщении электронной почты, но и, например, в тексте ICQ-сообщения, компонент Защита от веб-угроз отслеживает попытки перейти на фишинговый веб-сайт на уровне проверки веб-трафика и блокирует доступ к таким веб-сайтам. Списки фишинговых веб-адресов включены в комплект поставки Kaspersky Endpoint Security.

► *Чтобы настроить проверку компонентом Защита от веб-угроз ссылок по базам фишинговых и вредоносных веб-адресов, выполните следующие действия:*

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Защита → Базовая защита → Защита от веб-угроз**.
3. Нажмите на кнопку **Расширенная настройка**.
4. Выполните следующие действия:
   - В блоке **Методы проверки** установите флажок **Проверять веб-адрес по базе вредоносных веб-адресов**, если вы хотите, чтобы компонент Защита от веб-угроз проверял ссылки по базам вредоносных веб-адресов. Проверка ссылок на принадлежность к базе вредоносных веб-адресов позволяет отследить веб-сайты, которые находятся в списке запрещенных веб-адресов. База вредоносных веб-адресов формируется специалистами "Лаборатории Касперского", входит в комплект поставки программы и пополняется при обновлении баз Kaspersky Endpoint Security.

Kaspersky Endpoint Security проверяет все ссылки по базам вредоносных веб-адресов. Параметры проверки защищенных соединений программы не влияют на проверку ссылок. То есть, если проверка защищенных соединений выключена (см. раздел "Настройка параметров проверки защищенных соединений" на стр. 140), Kaspersky Endpoint Security проверяет ссылки по базам вредоносных веб-адресов, даже если сетевой трафик передается по защищенному соединению.

- В блоке **Анти-Фишинг** установите флажок **Проверять веб-адрес по базе фишинговых веб-адресов**, если вы хотите, чтобы компонент Защита от веб-угроз проверял ссылки по базам фишинговых веб-адресов. В состав базы фишинговых веб-адресов включены веб-адреса известных на настоящее время веб-сайтов, которые используются для фишинг-атак. Базу фишинговых веб-адресов специалисты "Лаборатории Касперского" пополняют веб-адресами, предоставленными международной организацией по борьбе с фишингом The Anti-Phishing Working Group. База фишинговых веб-адресов входит в комплект поставки программы и пополняется при обновлении баз Kaspersky Endpoint Security.

  Для проверки ссылок вы также можете использовать репутационные базы Kaspersky Security Network (см. раздел "Включение и выключение использования Kaspersky Security Network" на стр. 81).

5. Сохраните внесенные изменения.

Использование эвристического анализа в работе компонента Защита от веб-угроз

Чтобы повысить эффективность защиты, вы можете использовать эвристический анализ. В процессе эвристического анализа Kaspersky Endpoint Security анализирует активность, которую программы производят в операционной системе. Эвристический анализ позволяет обнаруживать угрозы, записей о которых еще нет в базах Kaspersky Endpoint Security.

► *Чтобы настроить использование эвристического анализа, выполните следующие действия:*

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Защита → Базовая защита → Защита от веб-угроз**.
3. Нажмите на кнопку **Расширенная настройка**.
4. В блоке **Методы проверки** установите флажок **Использовать эвристический анализ**, если вы хотите, чтобы программа использовала эвристический анализ при проверке веб-трафика на наличие вирусов и других программ, представляющих угрозу. Далее при помощи ползунка задайте уровень эвристического анализа: **Поверхностный**, **Средний** или **Глубокий**.
5. В блоке **Анти-Фишинг** установите флажок **Использовать эвристический анализ**, если вы хотите, чтобы программа использовала эвристический анализ при проверке веб-страниц на наличие фишинговых ссылок.
6. Сохраните внесенные изменения.

kaspersky

Формирование списка доверенных веб-адресов

Вы можете сформировать список веб-адресов, содержанию которых вы доверяете. Компонент Защита от веб-угроз не анализирует информацию, поступающую с доверенных веб-адресов, на присутствие вирусов и других программ, представляющих угрозу. Такая возможность может быть использована, например, в том случае, если компонент Защита от веб-угроз препятствует загрузке файла с известного вам веб-сайта.

Под веб-адресом подразумевается адрес как отдельной веб-страницы, так и веб-сайта.

► *Чтобы сформировать список доверенных веб-адресов, выполните следующие действия:*

1. В нижней части главного окна программы нажмите на кнопку .
2. В окне параметров программы выберите раздел **Защита** → **Базовая защита** → **Защита от веб-угроз**.
3. Нажмите на кнопку **Расширенная настройка**.
4. Установите флажок **Не проверять веб-трафик с доверенных веб-адресов**.

   Если флажок установлен, компонент Защита от веб-угроз не проверяет содержимое веб-страниц / веб-сайтов, адреса которых включены в список доверенных веб-адресов. Вы можете добавить в список доверенных веб-адресов как конкретный адрес веб-страницы / веб-сайта, так и маску адреса веб-страницы / веб-сайта.
5. Сформируйте список адресов веб-сайтов / веб-страниц, содержимому которых вы доверяете.
6. Сохраните внесенные изменения.

kaspersky

Защита от почтовых угроз

Этот компонент доступен, если программа Kaspersky Endpoint Security установлена на компьютере под управлением операционной системы Windows для рабочих станций. Этот компонент недоступен, если программа Kaspersky Endpoint Security установлена на компьютере под управлением операционной системы Windows для серверов.

Компонент Защита от почтовых угроз проверяет вложения входящих и исходящих сообщений электронной почты на наличие в них вирусов и других программ, представляющих угрозу. Также компонент проверяет сообщения на наличие вредоносных и фишинговых ссылок. По умолчанию компонент Защита от почтовых угроз постоянно находится в оперативной памяти компьютера и проверяет все сообщения, получаемые или отправляемые по протоколам POP3, SMTP, IMAP, NNTP или в почтовом клиенте Microsoft Office Outlook (MAPI). Компонент обеспечивает защиту компьютера с помощью антивирусных баз, облачной службы Kaspersky Security Network (см. раздел "Включение и выключение использования Kaspersky Security Network" на стр. 81) и эвристического анализа.

Компонент Защита от почтовых угроз не проверяет сообщения, если почтовый клиент открыт в браузере.

При обнаружении вредоносного файла во вложении Kaspersky Endpoint Security меняет тему сообщения: `[Сообщение заражено] <тема сообщения>` или `[Зараженный объект удален] <тема сообщения>`.

Компонент взаимодействует с почтовыми клиентами, установленными на компьютере. Для почтового клиента Microsoft Office Outlook предусмотрено расширение с дополнительными параметрами. Расширение компонента Защита от почтовых угроз встраивается в почтовый клиент Microsoft Office Outlook во время установки Kaspersky Endpoint Security.

В этом разделе

kaspersky

Включение и выключение Защиты от почтовых угроз

По умолчанию компонент Защита от почтовых угроз включен и работает в рекомендованном специалистами "Лаборатории Касперского" режиме. Для работы Защиты от почтовых угроз Kaspersky Endpoint Security применяет разные наборы параметров. Наборы параметров, сохраненные в программе, называются *уровнями безопасности*: **Высокий**, **Рекомендуемый**, **Низкий**. Параметры уровня безопасности почты **Рекомендуемый** считаются оптимальными, они рекомендованы специалистами "Лаборатории Касперского" (см. таблицу ниже). Вы можете выбрать один из предустановленных уровней безопасности почты или настроить уровень безопасности почты самостоятельно. После того как вы изменили параметры уровня безопасности почты, вы всегда можете вернуться к рекомендуемым параметрам уровня безопасности почты.

► *Чтобы включить или выключить компонент Защита от почтовых угроз выполните следующие действия:*

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Защита → Базовая защита → Защита от почтовых угроз**.
3. Используйте переключатель **Защита от почтовых угроз**, чтобы включить или выключить компонент.
4. Если вы включили компонент, в блоке **Уровень безопасности** выполните одно из следующих действий:
   - Если вы хотите применить один из предустановленных уровней безопасности, выберите его при помощи ползунка:
     - **Высокий**. Уровень безопасности почты, при котором компонент Защита от почтовых угроз максимально контролирует сообщения. Компонент Защита от почтовых угроз проверяет входящие и исходящие сообщения электронной почты, а также выполняет глубокий эвристический анализ. Уровень безопасности почты **Высокий** рекомендуется применять для работы в опасной среде. Примером опасной среды может служить подключение к одному из бесплатных почтовых сервисов из домашней сети, не обеспечивающей централизованной защиты почты.
     - **Рекомендуемый**. Уровень безопасности почты, обеспечивающий оптимальный баланс между производительностью Kaspersky Endpoint Security и безопасностью почты. Компонент Защита от почтовых угроз проверяет входящие и исходящие сообщения электронной почты, а также выполняет эвристический анализ среднего уровня. Этот уровень безопасности почты рекомендован для использования специалистами "Лаборатории Касперского". Значения параметров для рекомендуемого уровня безопасности см. в таблице ниже.
     - **Низкий**. Уровень безопасности почты, при котором компонент Защита от почтовых угроз проверяет только входящие сообщения электронной почты, а также выполняет поверхностный эвристический анализ и не проверяет архивы, вложенные в сообщения. Если используется этот уровень безопасности почты, компонент Защита от почтовых угроз проверяет сообщения электронной почты максимально быстро и затрачивает минимум ресурсов операционной системы. Уровень безопасности почты **Низкий** рекомендуется применять для работы в хорошо защищенной среде. Примером такой среды может служить локальная сеть организации с централизованным обеспечением безопасности почты.

- Если вы хотите настроить уровень безопасности самостоятельно, нажмите на кнопку **Расширенная настройка** и задайте параметры работы компонента.

  Вы можете восстановить значения предустановленных уровней безопасности по кнопке **Восстановить рекомендуемый уровень безопасности** в верхней части окна.

5. Сохраните внесенные изменения.

Таблица 6. Параметры Защиты от почтовых угроз, рекомендованные специалистами "Лаборатории Касперского", (рекомендованный уровень безопасности)

Параметр	Значение	Описание
Область защиты	**Входящие и исходящие сообщения**	*Область защиты* – это объекты, которые проверяет компонент во время своей работы: **Входящие и исходящие сообщения** или **Только входящие сообщения**. Для защиты компьютеров достаточно проверять только входящие сообщения. Вы можете включить проверку исходящих сообщений для предотвращения отправки зараженных файлов в архивах. Вы также можете включить проверку исходящих сообщений, если вы хотите запретить обмен файлами определенных форматов, например, аудио или видео.
Подключить расширение для Microsoft Outlook	**Включено**	Если флажок установлен, включена проверка сообщений электронной почты, передающихся по протоколам POP3, SMTP, NNTP, IMAP на стороне расширения, интегрированного в Microsoft Outlook. В случае проверки почты с помощью расширения для Microsoft Outlook рекомендуется использовать режим кеширования Exchange (Cached Exchange Mode). Более подробную информацию о режиме кеширования Exchange и рекомендации по его использованию вы можете найти в базе знаний Microsoft https://technet.microsoft.com/ru-ru/library/cc179175.aspx.
Проверять вложенные архивы	**Включено**	Проверка архивов форматов RAR, ARJ, ZIP, CAB, LHA, JAR, ICE.
Проверять вложенные файлы офисных форматов	**Включено**	Проверка файлов Microsoft Office (DOC, DOCX, XLS, PPT и других). К файлам Microsoft Office также относятся OLE-объекты.
Фильтр вложений	**Переименовывать вложения указанных типов**	Если выбран этот вариант, компонент Защита от почтовых угроз заменяет последний символ расширения вложенных файлов указанных типов на символ подчеркивания (например, attachment.doc_). Таким образом, чтобы открыть файл, пользователю нужно переименовать файл.

Параметр	Значение	Описание
Эвристический анализ	**Средний**	Технология обнаружения угроз, которые невозможно определить с помощью текущей версии баз программ "Лаборатории Касперского". Позволяет находить файлы, которые могут содержать неизвестный вирус или новую модификацию известного вируса. Во время проверки файлов на наличие вредоносного кода эвристический анализатор выполняет инструкции в исполняемых файлах. Количество инструкций, которые выполняет эвристический анализатор, зависит от заданного уровня эвристического анализа. Уровень эвристического анализа обеспечивает баланс между тщательностью поиска новых угроз, степенью загрузки ресурсов операционной системы и длительностью эвристического анализа.
Действие при обнаружении угрозы	**Лечить; удалять, если лечение невозможно**	При обнаружении зараженного объекта во входящем или исходящем сообщении Kaspersky Endpoint Security пытается вылечить обнаруженный объект. Пользователю будет доступно сообщение с безопасным вложением. Если вылечить объект не удалось, Kaspersky Endpoint Security удаляет зараженный объект. Kaspersky Endpoint Security добавит информацию о выполненном действии в тему сообщения: `[Зараженный объект удален] <тема сообщения>`.

Изменение действия над зараженными сообщениями электронной почты

По умолчанию компонент Защита от почтовых угроз автоматически пытается вылечить все обнаруженные зараженные сообщения электронной почты. Если лечение невозможно, то компонент Защита от почтовых угроз удаляет зараженные сообщения электронной почты.

► *Чтобы изменить действие над зараженными сообщениями электронной почты, выполните следующие действия:*

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Защита → Базовая защита → Защита от почтовых угроз**.
3. В блоке **Действие при обнаружении угрозы** выберите вариант действия, которое выполняет Kaspersky Endpoint Security при обнаружении зараженного сообщения:
   - **Лечить; удалять, если лечение невозможно**. При обнаружении зараженного объекта во входящем или исходящем сообщении Kaspersky Endpoint Security пытается вылечить обнаруженный объект. Пользователю будет доступно сообщение с безопасным вложением. Если вылечить объект не удалось, Kaspersky Endpoint Security удаляет зараженный объект. Kaspersky Endpoint Security добавит информацию о выполненном действии в тему сообщения: `[Зараженный объект удален] <тема сообщения>`.

- **Лечить; блокировать, если лечение невозможно**. При обнаружении зараженного объекта во входящем сообщении Kaspersky Endpoint Security пытается вылечить обнаруженный объект. Пользователю будет доступно сообщение с безопасным вложением. Если вылечить объект не удалось, Kaspersky Endpoint Security добавит предупреждение к теме сообщения: `[Сообщение заражено] <тема сообщения>`. Пользователю будет доступно сообщение с исходным вложением. При обнаружении зараженного объекта в исходящем сообщении Kaspersky Endpoint Security пытается вылечить обнаруженный объект. Если вылечить объект не удалось, Kaspersky Endpoint Security блокирует отправку сообщения, почтовый клиент показывает ошибку.
- **Блокировать**. При обнаружении зараженного объекта во входящем сообщении Kaspersky Endpoint Security добавит предупреждение к теме сообщения: `[Сообщение заражено] <тема сообщения>`. Пользователю будет доступно сообщение с исходным вложением. При обнаружении зараженного объекта в исходящем сообщении Kaspersky Endpoint Security блокирует отправку сообщения, почтовый клиент показывает ошибку.

4. Сохраните внесенные изменения.

Формирование области защиты компонента Защита от почтовых угроз

Область защиты – это объекты, которые проверяет компонент во время своей работы. Область защиты разных компонентов имеет разные свойства. Свойствами области защиты компонента Защита от почтовых угроз являются параметры интеграции компонента Защита от почтовых угроз в почтовые клиенты, тип сообщений электронной почты и почтовые протоколы, трафик которых проверяет компонент Защита от почтовых угроз. По умолчанию Kaspersky Endpoint Security проверяет как входящие, так и исходящие сообщения электронной почты, трафик почтовых протоколов POP3, SMTP, NNTP и IMAP, а также интегрируется в почтовый клиент Microsoft Office Outlook.

► *Чтобы сформировать область защиты компонента Защита от почтовых угроз, выполните следующие действия:*

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Защита → Базовая защита → Защита от почтовых угроз**.
3. Нажмите на кнопку **Расширенная настройка**.
4. В блоке **Область защиты** выберите сообщения для проверки:
   - **Входящие и исходящие сообщения**.
   - **Только входящие сообщения**.

   Для защиты компьютеров достаточно проверять только входящие сообщения. Вы можете включить проверку исходящих сообщений для предотвращения отправки зараженных файлов в архивах. Вы также можете включить проверку исходящих сообщений, если вы хотите запретить обмен файлами определенных форматов, например, аудио или видео.

Если вы выбираете проверку только входящих сообщений, рекомендуется однократно проверить все исходящие сообщения, поскольку существует вероятность того, что на вашем компьютере есть почтовые черви, которые используют электронную почту в качестве канала распространения. Это позволит избежать проблем, связанных с неконтролируемой рассылкой зараженных сообщений с вашего компьютера.

5. В блоке **Встраивание в операционную систему** выполните следующие действия:

   - Установите флажок **Проверять трафик POP3 / SMTP / NNTP / IMAP**, если вы хотите, чтобы компонент Защита от почтовых угроз проверял сообщения, передающиеся по протоколам POP3, SMTP, NNTP и IMAP, до их получения на компьютере пользователя.

     Снимите флажок **Проверять трафик POP3 / SMTP / NNTP / IMAP**, если вы хотите, чтобы компонент Защита от почтовых угроз не проверял сообщения, передающиеся по протоколам POP3, SMTP, NNTP и IMAP, до их получения на компьютере пользователя. В этом случае сообщения проверяет расширение компонента Защита от почтовых угроз, встроенное в почтовый клиент Microsoft Office Outlook, после их получения на компьютере пользователя, если установлен флажок **Подключить расширение для Microsoft Outlook**.

     Если вы используете почтовый клиент, отличный от Microsoft Office Outlook, то при снятом флажке **Проверять трафик POP3 / SMTP / NNTP / IMAP** компонент Защита от почтовых угроз не проверяет сообщения, передающиеся по почтовым протоколам POP3, SMTP, NNTP и IMAP.

   - Установите флажок **Подключить расширение для Microsoft Outlook**, если вы хотите открыть доступ к настройке параметров компонента Защита от почтовых угроз из программы Microsoft Office Outlook и включить проверку сообщений, передающихся по протоколам POP3, SMTP, NNTP, IMAP и MAPI, после их получения на компьютере пользователя с помощью расширения, интегрированного в программу Microsoft Office Outlook.

     Снимите флажок **Подключить расширение для Microsoft Outlook**, если вы хотите закрыть доступ к настройке параметров компонента Защита от почтовых угроз из программы Microsoft Office Outlook и выключить проверку сообщений, передающихся по протоколам POP3, SMTP, NNTP, IMAP и MAPI, после их получения на компьютере пользователя с помощью расширения, интегрированного в программу Microsoft Office Outlook.

     Расширение компонента Защита от почтовых угроз встраивается в почтовый клиент Microsoft Office Outlook во время установки Kaspersky Endpoint Security.

6. Сохраните внесенные изменения.

Проверка составных файлов, вложенных в сообщения электронной почты

Вы можете включить или выключить проверку объектов, вложенных в сообщения, ограничить максимальный размер проверяемых объектов, вложенных в сообщения, и максимальную длительность проверки объектов, вложенных в сообщения.

► *Чтобы настроить проверку составных файлов, вложенных в сообщения электронной почты, выполните следующие действия:*

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Защита** → **Базовая защита** → **Защита от почтовых угроз**.
3. Нажмите на кнопку **Расширенная настройка**.
4. В блоке **Проверка составных файлов** настройте параметры проверки:
   - **Проверять вложенные файлы форматов Microsoft Office**. Проверка файлов Microsoft Office (DOC, DOCX, XLS, PPT и других). К файлам Microsoft Office также относятся OLE-объекты.
   - **Проверять вложенные архивы**. Проверка архивов форматов RAR, ARJ, ZIP, CAB, LHA, JAR, ICE.
   - **Не проверять архивы размером более N МБ**. Если флажок установлен, компонент Защита от почтовых угроз исключает из проверки вложенные в сообщения электронной почты архивы, размер которых больше заданного. Если флажок снят, компонент Защита от почтовых угроз проверяет архивы любого размера, вложенные в сообщения электронной почты.
   - **Ограничить время проверки архива до N сек**. Если флажок установлен, то время проверки архивов, вложенных в сообщения электронной почты, ограничено указанным периодом.
5. Сохраните внесенные изменения.

Фильтрация вложений в сообщениях электронной почты

Функциональность фильтрации вложений не применяется для исходящих сообщений электронной почты.

Вредоносные программы могут распространяться в виде вложений в сообщениях электронной почты. Вы можете настроить фильтрацию по типу вложений в сообщениях, чтобы автоматически переименовывать или удалять файлы указанных типов. Переименовав вложение определенного типа, Kaspersky Endpoint Security может защитить ваш компьютер от автоматического запуска вредоносной программы.

► *Чтобы настроить фильтрацию вложений, выполните следующие действия:*

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Защита** → **Базовая защита** → **Защита от почтовых угроз**.
3. Нажмите на кнопку **Расширенная настройка**.
4. В блоке **Фильтр вложений** выполните одно из следующих действий:
   - Выберите вариант **Не применять фильтр**, если вы хотите, чтобы компонент Защита от почтовых угроз не фильтровал вложения в сообщениях.

- Выберите вариант **Переименовывать вложения указанных типов**, если вы хотите, чтобы компонент Защита от почтовых угроз изменял названия вложенных в сообщения файлов указанных типов (см. раздел "Приложение 4. Типы файлов для фильтра вложений Защиты от почтовых угроз" на стр. 283).
- Выберите вариант **Удалять вложения указанных типов**, если вы хотите, чтобы компонент Защита от почтовых угроз удалял вложенные в сообщения файлы указанных типов (см. раздел "Приложение 4. Типы файлов для фильтра вложений Защиты от почтовых угроз" на стр. 283).

5. Если на предыдущем шаге инструкции вы выбрали вариант **Переименовывать вложения указанных типов** или вариант **Удалять вложения указанных типов**, установите флажки напротив нужных типов файлов.
6. Сохраните внесенные изменения.

kaspersky

Защита от сетевых угроз

Компонент Защита от сетевых угроз (англ. IDS – Intrusion Detection System) отслеживает во входящем сетевом трафике активность, характерную для сетевых атак. Обнаружив попытку сетевой атаки на компьютер пользователя, Kaspersky Endpoint Security блокирует сетевое соединение с атакующим компьютером.

Описания известных в настоящее время видов сетевых атак и методов борьбы с ними содержатся в базах Kaspersky Endpoint Security. Список сетевых атак, которые обнаруживает компонент Защита от сетевых угроз, пополняется в процессе обновления баз и модулей программы.

В этом разделе

Включение и выключение Защиты от сетевых угроз

По умолчанию Защита от сетевых угроз включена и работает в оптимальном режиме. При необходимости вы можете выключить Защиту от сетевых угроз.

► *Чтобы включить или выключить Защиту от сетевых угроз, выполните следующие действия:*

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Защита** → **Защита от сетевых угроз**.
3. Используйте переключатель **Защита от сетевых угроз**, чтобы включить или выключить компонент.
4. Сохраните внесенные изменения.

В результате, если Защита от сетевых угроз включена, Kaspersky Endpoint Security отслеживает во входящем сетевом трафике активность, характерную для сетевых атак. Обнаружив попытку сетевой атаки на компьютер пользователя, Kaspersky Endpoint Security блокирует сетевое соединение с атакующим компьютером.

Блокирование атакующего компьютера

► *Чтобы заблокировать атакующий компьютер, выполните следующие действия:*

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Защита** → **Защита от сетевых угроз**.

3. Установите флажок **Добавить атакующий компьютер в список блокирования на N минут**.

   Если флажок установлен, то компонент Защита от сетевых угроз добавляет атакующий компьютер в список блокирования. Это означает, что компонент Защита от сетевых угроз блокирует сетевое соединение с атакующим компьютером после первой попытки сетевой атаки в течение заданного времени, чтобы автоматически защитить компьютер пользователя от возможных будущих сетевых атак с этого адреса.

   Вы можете посмотреть список блокирования в окне инструмента Мониторинг сети.

   > Kaspersky Endpoint Security очищает список блокирования при перезапуске программы и при изменении параметров Защиты от сетевых угроз.

4. Измените время блокирования атакующего компьютера в поле, расположенном справа от флажка **Добавить атакующий компьютер в список блокирования на N минут**.
5. Сохраните внесенные изменения.

В результате Kaspersky Endpoint Security, обнаружив попытку сетевой атаки на компьютер пользователя, блокирует все соединения с атакующим компьютером.

Настройка адресов исключений из блокирования

Kaspersky Endpoint Security может распознать сетевую атаку и заблокировать безопасное сетевое соединение, по которому передается большое количество пакетов (например, от камер наблюдения). Для работы с доверенными устройствами вы можете добавить IP-адреса этих устройств в список исключений.

► *Чтобы настроить адреса исключений из блокирования, выполните следующие действия:*

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Защита** → **Защита от сетевых угроз**.
3. Нажмите на ссылку **Настроить исключения**.
4. В открывшемся окне нажмите на кнопку **Добавить**.
5. Введите IP-адрес компьютера, сетевые атаки с которого не должны блокироваться.
6. Сохраните внесенные изменения.

В результате Kaspersky Endpoint Security не отслеживает активность от устройств из списка исключений.

Настройка защиты от сетевых атак по типам

Kaspersky Endpoint Security позволяет управлять защитой от следующих типов сетевых атак:

- *Атака типа Интенсивные сетевые запросы (англ. Network Flooding)* – атака на сетевые ресурсы организации (например, веб-серверы). Атака заключается в отправке большого количества запросов для превышения пропускной способности сетевых ресурсов. Таким образом пользователи не могут получить доступ к сетевым ресурсам организации.

- *Атака типа Сканирование портов* заключается в сканировании UDP- и TCP-портов, а также сетевых служб на компьютере. Атака позволяет определить степень уязвимости компьютера перед более опасными видами сетевых атак. Сканирование портов также позволяет злоумышленнику определить операционную систему на компьютере и выбрать подходящие для нее сетевые атаки.
- *Атака типа MAC-спуфинг* заключается в изменении MAC-адреса сетевого устройства (сетевой карты). В результате злоумышленник может перенаправить данные, отправленные на устройство, на другое устройство и получить доступ к этим данным. Kaspersky Endpoint Security позволяет блокировать атаки MAC-спуфинга и получать уведомления об атаках.

Вы можете выключить обнаружение этих типов атак, так как некоторые разрешенные программы выполняют действия, характерные для таких атак. Таким образом, вы можете избежать ложных срабатываний.

По умолчанию Kaspersky Endpoint Security не отслеживает атаки типа Интенсивные сетевые запросы, Сканирование портов и MAC-спуфинг.

► *Чтобы настроить защиту от сетевых атак по типам, выполните следующие действия:*

1. В нижней части главного окна программы нажмите на кнопку .
2. В окне параметров программы выберите раздел **Защита** → **Защита от сетевых угроз**.
3. Используйте переключатель **Считать атаками сканирование портов и интенсивные сетевые запросы**, чтобы включить или выключить обнаружение атак.
4. Используйте переключатель **Защита от MAC-спуфинга**.
5. В блоке **При обнаружении атаки MAC-спуфинг** выберите один из следующих вариантов:
   - **Только уведомлять**.
   - **Уведомлять и блокировать**.
6. Сохраните внесенные изменения.

kaspersky

Защита от атак BadUSB

Некоторые вирусы изменяют встроенное программное обеспечение USB-устройств так, чтобы операционная система определяла USB-устройство как клавиатуру. В результате вирус может выполнять команды под вашей учетной записью, например, загрузить вредоносную программу.

Компонент Защита от атак BadUSB позволяет предотвратить подключение к компьютеру зараженных USB-устройств, имитирующих клавиатуру.

Когда к компьютеру подключается USB-устройство, определенное операционной системой как клавиатура, программа предлагает пользователю ввести с этой клавиатуры или с помощью экранной клавиатуры (если она доступна) (см. раздел "Использовании экранной клавиатуры при авторизации USB-устройств" на стр. 137) цифровой код, сформированный программой (см. рис. ниже). Эта процедура называется авторизацией клавиатуры.

Если код введен правильно, программа сохраняет идентификационные параметры – VID/PID клавиатуры и номер порта, по которому она подключена, в списке авторизованных клавиатур. Авторизация клавиатуры при ее повторном подключении или перезагрузке операционной системы не требуется.

> При подключении авторизованной клавиатуры через другой USB-порт компьютера программа снова запрашивает ее авторизацию.

Если цифровой код введен неправильно, программа формирует новый. Число попыток для ввода цифрового кода равно трем. Если цифровой код введен неправильно трижды или закрыто окно **Авторизация клавиатуры <Название клавиатуры>**, программа блокирует ввод с этой клавиатуры. При повторном подключении клавиатуры или перезагрузке операционной системы программа снова предлагает пройти авторизацию клавиатуры.

Программа разрешает использование авторизованной клавиатуры и блокирует использование клавиатуры, не прошедшей авторизацию.

Компонент Защита от атак BadUSB не устанавливается по умолчанию. Если вам нужен компонент Защита от атак BadUSB, вы можете добавить компонент в свойствах инсталляционного пакета перед установкой программы или измените состав компонентов программы после установки программы.

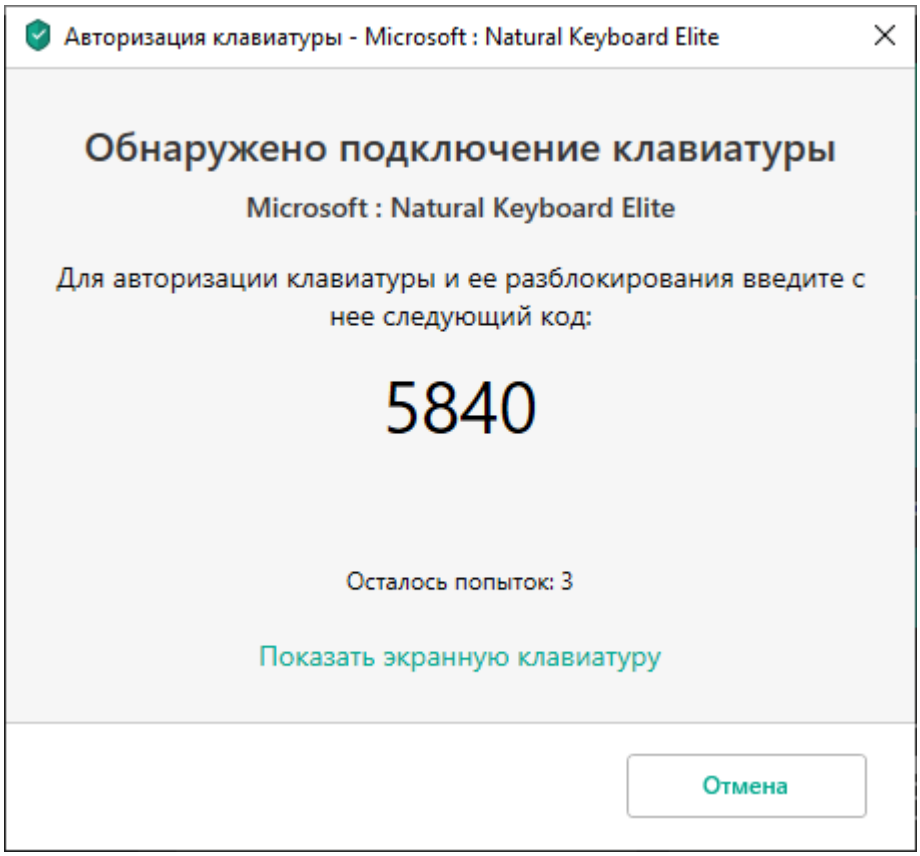


Рисунок 13. Уведомление об авторизации клавиатуры

В этом разделе

Включение и выключение Защиты от атак BadUSB

USB-устройства, определенные операционной системой как клавиатуры и подключенные к компьютеру до установки компонента Защита от атак BadUSB, считаются авторизованными после его установки.

► *Чтобы включить или выключить Защиту от атак BadUSB, выполните следующие действия:*

1. В нижней части главного окна программы нажмите на кнопку ⚙.

2. В окне параметров программы выберите раздел **Защита** → **Базовая защита** → **Защита от атак BadUSB**.
3. Используйте переключатель **Защита от атак BadUSB**, чтобы включить или выключить компонент.
4. Сохраните внесенные изменения.

В результате, если Защита от атак BadUSB включена, Kaspersky Endpoint Security требует авторизацию подключенного USB-устройства, определенного операционной системой как клавиатура. Пользователь не может использовать неавторизованную клавиатуру до тех пор, пока она не будет авторизована.

Использовании экранной клавиатуры при авторизации USB-устройств

Возможность использовать экранную клавиатуру предназначена только для авторизации USB-устройств, не поддерживающих произвольный ввод символов (например, сканеров штрих-кодов). Не рекомендуется использовать экранную клавиатуру для авторизации неизвестных вам USB-устройств.

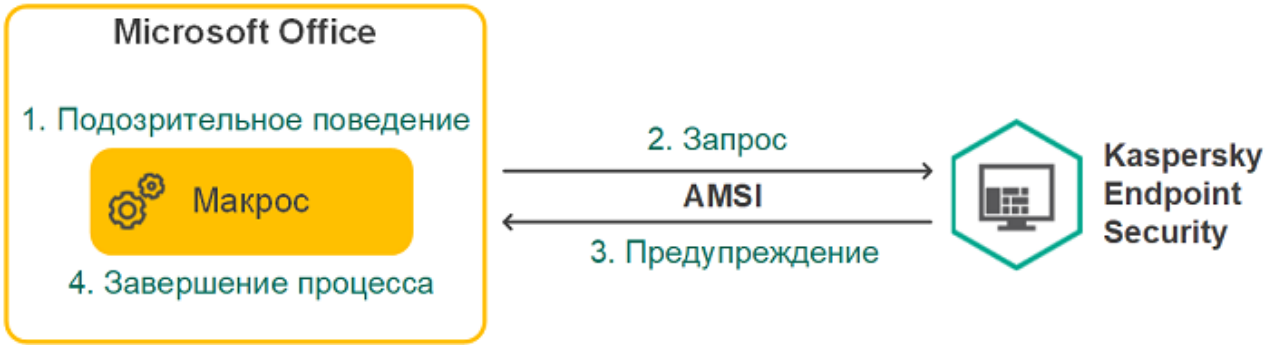
► *Чтобы разрешить или запретить использование экранной клавиатуры при авторизации, выполните следующие действия:*

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Защита** → **Базовая защита** → **Защита от атак BadUSB**.
3. Используйте флажок **Запретить использование экранной клавиатуры для авторизации USB-устройств**, чтобы запретить или разрешить использование экранной клавиатуры для авторизации.
4. Сохраните внесенные изменения.

AMSI-защита

Компонент AMSI-защита предназначен для поддержки интерфейса Antimalware Scan Interface от Microsoft. *Интерфейс Antimalware Scan Interface (AMSI)* позволяет сторонним приложениям с поддержкой AMSI отправлять объекты (например, скрипты PowerShell) в Kaspersky Endpoint Security для дополнительной проверки и получать результаты проверки этих объектов. Сторонними приложениями могут быть, например, программы Microsoft Office (см. рис. ниже). Подробнее об интерфейсе AMSI см. в *документации Microsoft* https://docs.microsoft.com/ru-ru/windows/desktop/amsi/antimalware-scan-interface-portal.

AMSI-защита может только обнаруживать угрозу и уведомлять стороннее приложение об обнаруженной угрозе. Стороннее приложение после получения уведомления об угрозе не дает выполнить вредоносные действия (например, завершает работу).



Компонент AMSI-защита может отклонить запрос от стороннего приложения, например, если это приложение превысило максимальное количество запросов за промежуток времени. Kaspersky Endpoint Security отправляет информацию об отклонении запроса от стороннего приложения на Сервер администрирования. Компонент AMSI-защита не отклоняет запросы от тех сторонних приложений, для которых установлен флажок **Не блокировать взаимодействие с AMSI-защитой** (см. раздел "**Формирование списка доверенных программ**" на стр. 201).

AMSI-защита доступна для следующих операционных систем рабочих станций и серверов:

- Windows 10 Home / Pro / Education / Enterprise;
- Windows Server 2016 Essentials / Standard / Datacenter;
- Windows Server 2019 Essentials / Standard / Datacenter.

В этом разделе

kaspersky

Включение и выключение AMSI-защиты

По умолчанию AMSI-защита включена.

► *Чтобы включить или выключить AMSI-защиту, выполните следующие действия:*

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Защита** → **Базовая защита** → **AMSI-защита**.
3. Используйте переключатель **AMSI-защита**, чтобы включить или выключить компонент.
4. Сохраните внесенные изменения.

Проверка составных файлов AMSI-защитой

Распространенной практикой сокрытия вирусов и других программ, представляющих угрозу, является внедрение их в составные файлы, например, архивы. Чтобы обнаружить скрытые таким образом вирусы и другие программы, представляющие угрозу, составной файл нужно распаковать, что может привести к снижению скорости проверки. Вы можете ограничить набор типов проверяемых составных файлов, таким образом увеличив скорость проверки.

► *Чтобы настроить проверку составных файлов AMSI-защитой, выполните следующие действия:*

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Защита** → **Базовая защита** → **AMSI-защита**.
3. В блоке **Проверка составных файлов** укажите, какие составные файлы вы хотите проверять: архивы, дистрибутивы или файлы офисных форматов.
4. В блоке **Ограничение по размеру** выполните одно из следующих действий:
   - Чтобы запретить компоненту AMSI-защита распаковывать составные файлы большого размера, установите флажок **Не распаковывать составные файлы большого размера** и в поле **Максимальный размер файла** укажите нужное значение. Компонент AMSI-защита не будет распаковывать составные файлы больше указанного размера.
   - Чтобы разрешить компоненту AMSI-защита распаковывать составные файлы большого размера, снимите флажок **Не распаковывать составные файлы большого размера**.

   Компонент AMSI-защита проверяет файлы больших размеров, извлеченные из архивов, независимо от того, установлен ли флажок **Не распаковывать составные файлы большого размера**.
5. Сохраните внесенные изменения.

kaspersky

Проверка защищенных соединений

Этот компонент доступен, если программа Kaspersky Endpoint Security установлена на компьютере под управлением операционной системы Windows для рабочих станций. Этот компонент недоступен, если программа Kaspersky Endpoint Security установлена на компьютере под управлением операционной системы Windows для серверов.

После установки Kaspersky Endpoint Security добавляет сертификат "Лаборатории Касперского" в системное хранилище доверенных сертификатов (хранилище сертификатов Windows). Также Kaspersky Endpoint Security включает использование системного хранилища доверенных сертификатов в программах Firefox и Thunderbird для проверки трафика этих программ.

Компоненты Веб-Контроль (на стр. 168), Защита от почтовых угроз (на стр. 124), Защита от веб-угроз (на стр. 117) могут расшифровывать и проверять сетевой трафик, передаваемый по защищенным соединениям с использованием следующих протоколов:

- SSL 3.0;
- TLS 1.0, TLS 1.1, TLS 1.2, TLS 1.3.

В этом разделе

Настройка параметров проверки защищенных соединений

► *Чтобы настроить параметры проверки защищенных соединений, выполните следующие действия:*

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Настройки сети**.
3. В блоке Проверка защищенных соединений выберите режим проверки защищенных соединений:
   - **Не проверять защищенные соединения**. Kaspersky Endpoint Security не имеет доступ к содержанию сайтов, адрес которых начинается с https://.
   - **Проверять защищенные соединения по запросу компонентов защиты**. Kaspersky Endpoint Security проверяет зашифрованный трафик только по запросу компонентов Защита от файловых угроз, Защита от почтовых угроз и Веб-Контроль.
   - **Всегда проверять защищенные соединения**. Kaspersky Endpoint Security проверяет зашифрованный сетевой трафик, даже если компоненты защиты выключены.

Kaspersky Endpoint Security не проверяет защищенные соединения, установленные доверенными программами, для которых выключена проверка трафика (см. раздел "Формирование списка доверенных программ" на стр. 201). Также Kaspersky Endpoint Security не проверяет защищенные соединения из предустановленного списка доверенных сайтов. Предустановленный список доверенных сайтов составляют специалисты "Лаборатории Касперского". Этот список обновляется с антивирусными базами программы. Вы можете просмотреть предустановленный список доверенных сайтов только в интерфейсе Kaspersky Endpoint Security. В консоли Kaspersky Security Center просмотреть список невозможно.

4. Если требуется, добавьте исключения из проверки: доверенные адреса и программы (см. раздел "Исключение защищенных соединений из проверки" на стр. 143).
5. Нажмите на кнопку **Дополнительные настройки**.
6. Настройте параметры проверки защищенных соединений (см. таблицу ниже).
7. Сохраните внесенные изменения.

Таблица 7. Параметры проверки защищенных соединений

Параметр	Описание
При переходе на домен с недоверенным сертификатом	**Разрешать**. Если выбран этот вариант, то при переходе на домен с недоверенным сертификатом Kaspersky Endpoint Security разрешает установку сетевого соединения. При переходе на домен с недоверенным сертификатом в браузере, Kaspersky Endpoint Security отображает HTML-страницу с предупреждением и информацией о причине, по которой этот домен не рекомендован для посещения. По ссылке из HTML-страницы с предупреждением пользователь может получить доступ к запрошенному веб-ресурсу. После перехода по этой ссылке Kaspersky Endpoint Security в течение часа не будет отображать предупреждения о недоверенном сертификате при переходе на другие веб-ресурсы в том же домене. **Блокировать соединение**. Если выбран этот вариант, то при переходе на домен с недоверенным сертификатом Kaspersky Endpoint Security блокирует сетевое соединение. При переходе на домен с недоверенным сертификатом в браузере, Kaspersky Endpoint Security отображает HTML-страницу с информацией о причине, по которой переход на этот домен заблокирован.
При возникновении ошибок проверки защищенных соединений	**Блокировать соединение**. Если выбран этот элемент, то при возникновении ошибки проверки защищенного соединения Kaspersky Endpoint Security блокирует это сетевое соединение. **Добавлять домен в исключения**. Если выбран этот элемент, то при возникновении ошибки проверки защищенного соединения Kaspersky Endpoint Security добавляет домен, при переходе на который возникла ошибка, в список доменов с ошибками проверки и не контролирует зашифрованный сетевой трафик при переходе на этот домен. Вы можете просмотреть список доменов с ошибками проверки защищенных соединений только в локальном интерфейсе программы. Чтобы сбросить содержание списка, нужно выбрать элемент **Блокировать соединение**.

Параметр	Описание
Блокировать соединение по протоколу SSL 2.0	Если флажок установлен, то Kaspersky Endpoint Security блокирует сетевые соединения, устанавливаемые по протоколу SSL 2.0. Если флажок снят, то Kaspersky Endpoint Security не блокирует сетевые соединения, устанавливаемые по протоколу SSL 2.0, и не контролирует сетевой трафик, передаваемый по этим соединениям.
Расшифровать защищенное соединение с сайтом, использующим EV-сертификат	EV-сертификаты (англ. Extended Validation Certificate) подтверждают подлинность веб-сайтов и повышают безопасность соединения. Браузеры сообщают о наличии на веб-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 Endpoint Security расшифровывает и контролирует защищенные соединения с EV-сертификатом. Если флажок снят, Kaspersky Endpoint Security не имеет доступа к содержанию HTTPS-трафика. Поэтому программа контролирует HTTPS-трафик только по адресу веб-сайта, например, `https://facebook.com`. Если вы впервые открываете веб-сайт с EV-сертификатом, защищенное соединение будет расшифровано независимо от того, установлен флажок или нет.

Проверка защищенных соединений в Firefox и Thunderbird

После установки Kaspersky Endpoint Security добавляет сертификат "Лаборатории Касперского" в системное хранилище доверенных сертификатов (хранилище сертификатов Windows). Firefox и Thunderbird по умолчанию используют собственное хранилище сертификатов Mozilla, а не хранилище сертификатов Windows. Если в вашей организации развернуто решение Kaspersky Security Center и к компьютеру применена политика, Kaspersky Endpoint Security автоматически включает использование хранилища сертификатов Windows в программах Firefox и Thunderbird для проверки трафика этих программ. Если к компьютеру не применена политика, вы можете выбрать хранилище сертификатов, которое будут использовать программы Mozilla. Если вы выбрали хранилище сертификатов Mozilla, добавьте сертификат "Лаборатории Касперского" в хранилище вручную. Это позволит избежать ошибок при работе с HTTPS-трафиком.

Перед добавлением сертификата в хранилище Mozilla экспортируйте сертификат "Лаборатории Касперского" из Панели управления Windows (свойства браузера). Подробнее о добавлении сертификата в хранилище см. на *сайте Службы технической поддержки Mozilla* https://support.mozilla.org/.

Вы можете выбрать хранилище сертификатов только в локальном интерфейсе программы.

► *Чтобы выбрать хранилище сертификатов для проверки защищенных соединений в Firefox и Thunderbird, выполните следующие действия:*

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Настройки сети**.
3. В блоке **Mozilla Firefox и Thunderbird** установите флажок **Проверять защищенный трафик в продуктах Mozilla**.
4. Выберите хранилище сертификатов:
   - **Использовать хранилище сертификатов Windows**. Это хранилище, в которое корневой сертификат "Лаборатории Касперского" добавляется при установке Kaspersky Endpoint Security.
   - **Использовать хранилище сертификатов Mozilla**. Программы Mozilla Firefox и Thunderbird используют собственное хранилище сертификатов. Если выбрано хранилище сертификатов Mozilla, корневой сертификат "Лаборатории Касперского" нужно добавить в это хранилище вручную через свойства браузера.
5. Сохраните внесенные изменения.

Исключение защищенных соединений из проверки

Большинство веб-ресурсов используют защищенное соединение. Специалисты "Лаборатории Касперского" рекомендуют включить проверку защищенных соединений (см. раздел "Настройка параметров проверки защищенных соединений" на стр. 140). Если проверка защищенных соединений мешает работе, вы можете добавить веб-сайт в исключения, – *доверенные адреса*. Если доверенная программа использует защищенное соединение, вы можете выключить проверку защищенных соединений для этой программы (см. раздел "Формирование списка доверенных программ" на стр. 201). Например, вы можете выключить проверку защищенных соединений для программ облачных хранилищ, так как эти программы используют двухфакторную аутентификацию с собственным сертификатом.

► *Чтобы исключить веб-адрес из проверки защищенных соединений, выполните следующие действия:*

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Настройки сети**.
3. В блоке **Проверка защищенных соединений** нажмите на кнопку **Доверенные адреса**.
4. Нажмите на кнопку **Добавить**.
5. Введите имя домена или IP-адрес, если вы хотите, чтобы программа Kaspersky Endpoint Security не проверяла защищенные соединения, устанавливаемые при переходе на эту веб-страницу.
6. Сохраните внесенные изменения.

По умолчанию Kaspersky Endpoint Security не проверяет защищенные соединения при возникновении ошибок и добавляет веб-сайт в специальный список – *домены с ошибками проверки*. Kaspersky Endpoint Security составляет список для каждого пользователя отдельно и не передает данные в Kaspersky Security Center. Вы можете включить блокирование соединения при возникновении ошибки (см. раздел "Настройка параметров проверки защищенных соединений" на стр. 140). Вы можете просмотреть список доменов с ошибками проверки защищенных соединений только в локальном интерфейсе программы.

► *Чтобы просмотреть список доменов с ошибками проверки, выполните следующие действия:*

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Настройки сети**.
3. В блоке **Проверка защищенных соединений** нажмите на кнопку **Домены с ошибками проверки**.

Откроется список доменов с ошибками проверки. Чтобы сбросить список вам нужно включить блокирование соединения при возникновении ошибки в политике, применить политику, вернуть параметр в исходное состояние и снова применить политику.

Специалисты "Лаборатории Касперского" составляют список доверенных веб-сайтов, которые Kaspersky Endpoint Security не проверяет независимо от параметров программы, – *глобальные исключения*.

► *Чтобы просмотреть глобальные исключения из проверки защищенного трафика, выполните следующие действия:*

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Настройки сети**.
3. В блоке **Проверка защищенных соединений** нажмите на ссылку **сайтах**.

Откроется список веб-сайтов, составленный специалистами "Лаборатории Касперского". Kaspersky Endpoint Security не проверяет защищенные соединения для сайтов из списка. Список может быть обновлен при обновлении баз и модулей Kaspersky Endpoint Security.

kaspersky

Контроль программ

Контроль программ управляет запуском программ на компьютерах пользователей. Это позволяет выполнить политику безопасности организации при использовании программ. Также Контроль программ снижает риск заражения компьютера, ограничивая доступ к программам.

Настройка Контроля программ состоит из следующих этапов:

1. Создание категорий программ.

   Администратор создает категории программ, которыми администратор хочет управлять. Категории программ предназначены для всех компьютеров сети организации независимо от групп администрирования. Для создания категории вы можете использовать следующие критерии: KL-категория (например, *Браузеры*), хеш файла, производитель программы и другие.

2. Создание правил Контроля программ (см. раздел "Добавление правила Контроля программ" на стр. 153).

   Администратор создает правила Контроля программ в политике для группы администрирования. Правило включает в себя категории программ и статус запуска программ из этих категорий: запрещен или разрешен.

3. Выбор режима работы Контроля программ (см. раздел "Выбор режима Контроля программ" на стр. 150).

   Администратор выбирает режим работы с программами, которые не входят ни в одно из правил (списки запрещенных и разрешенных программ).

При попытке пользователя запустить запрещенную программу, Kaspersky Endpoint Security заблокирует запуск программы и покажет уведомление (см. рис. ниже).

Для проверки настройки Контроля программ предусмотрен *тестовый режим*. В этом режиме Kaspersky Endpoint Security выполняет следующие действия:

- разрешает запуск программ, в том числе запрещенных;
- показывает уведомление о запуске запрещенной программы и добавляет информацию в отчет на компьютере пользователя;

- отправляет данные о запуске запрещенных программ в Kaspersky Security Center.

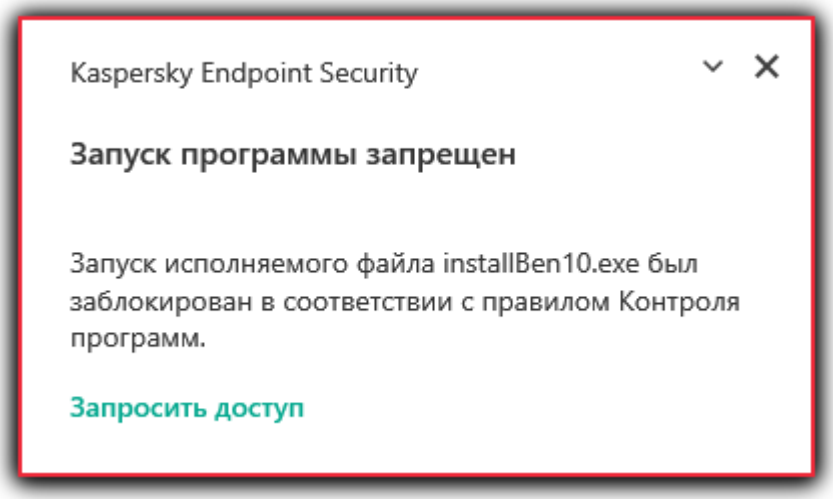


Рисунок 14. Уведомление Контроля программ

Режимы работы Контроля программ

Компонент Контроль программ может работать в двух режимах:

- **Список запрещенных**. Режим, при котором Контроль программ разрешает пользователям запуск любых программ, кроме тех, которые запрещены в правилах Контроля программ.

  Этот режим работы Контроля программ установлен по умолчанию.

- **Список разрешенных**. Режим, при котором Контроль программ запрещает пользователям запуск любых программ, кроме тех, которые разрешены и не запрещены в правилах Контроля программ.

  Если разрешающие правила Контроля программ сформированы максимально полно, компонент запрещает запуск всех новых программ, не проверенных администратором локальной сети организации, но обеспечивает работоспособность операционной системы и проверенных программ, которые нужны пользователям для выполнения должностных обязанностей.

  Вы можете ознакомиться с рекомендациями по настройке правил контроля программ в режиме списка разрешенных программ.

Настройка Контроля программ для работы в этих режимах возможна как в локальном интерфейсе Kaspersky Endpoint Security, так и с помощью Kaspersky Security Center.

Однако Kaspersky Security Center предоставляет инструменты, недоступные в локальном интерфейсе Kaspersky Endpoint Security и необходимые для следующих задач:

- Создание категорий программ.

  Правила Контроля программ, сформированные в Консоли администрирования Kaspersky Security Center, основываются на созданных вами категориях программ, а не на включающих и исключающих условиях, как в локальном интерфейсе Kaspersky Endpoint Security.

- Получение информации о программах, которые установлены на компьютерах локальной сети организации.

Поэтому настройку работы компонента Контроль программ рекомендуется выполнять с помощью Kaspersky Security Center.

Алгоритм работы Контроля программ

Kaspersky Endpoint Security использует алгоритм для принятия решения о запуске программы (см. рис. ниже).

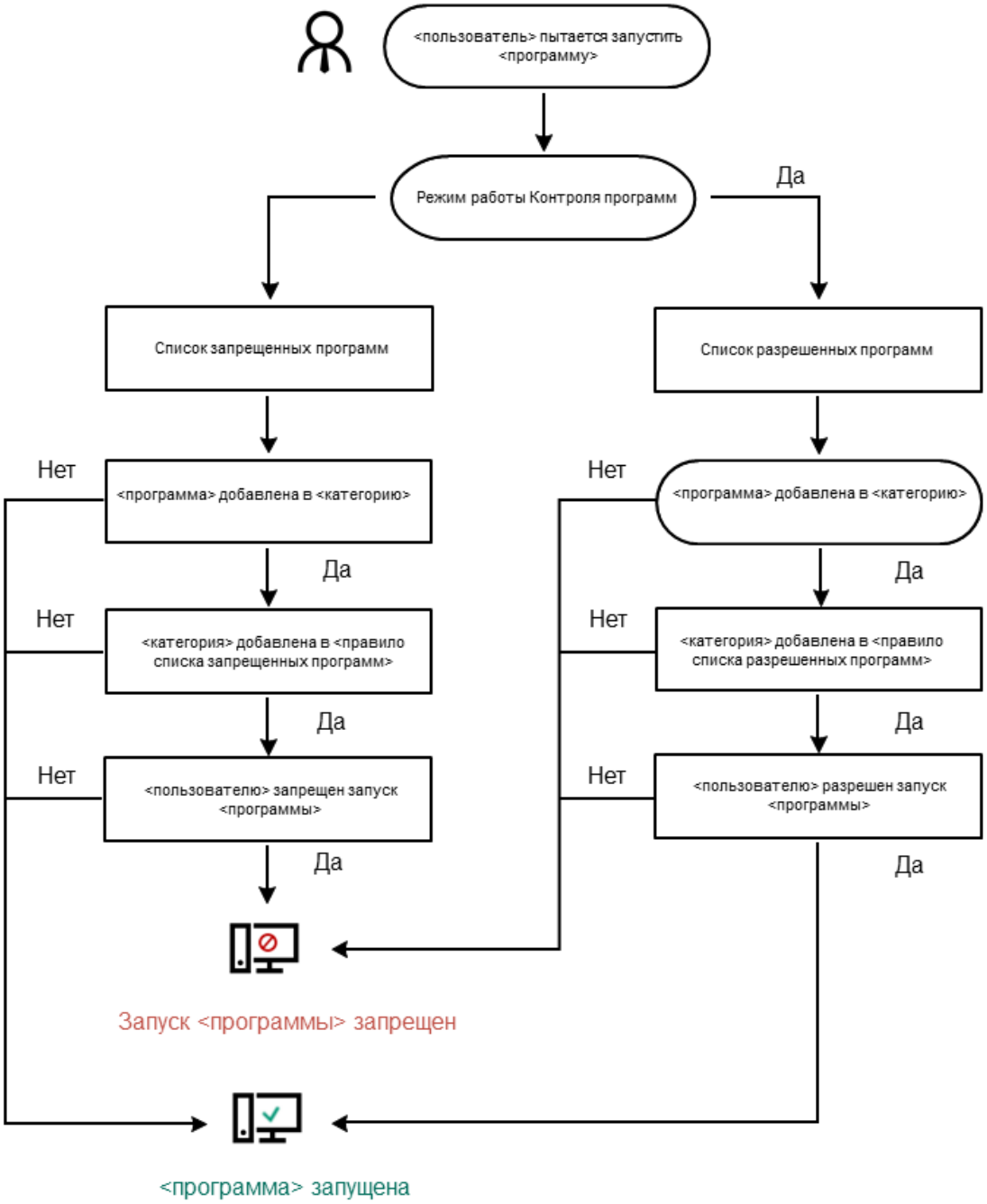


Рисунок 15. Алгоритм работы Контроля программ

kaspersky

В этом разделе

Ограничения функциональности Контроля программ

Работа компонента Контроль программ ограничена в следующих случаях:

- При обновлении версии программы импорт параметров компонента Контроль программ не поддерживается.
- При обновлении версии программы импорт параметров компонента Контроль программ поддерживается только при обновлении версии Kaspersky Endpoint Security 10 Service Pack 2 для Windows и выше до Kaspersky Endpoint Security 11.6.0 для Windows.

  При обновлении версий программы, отличных от Kaspersky Endpoint Security 10 Service Pack 2 для Windows, для восстановления работоспособности Контроля программ необходимо заново настроить параметры работы компонента.

- При отсутствии соединения с серверами KSN Kaspersky Endpoint Security получает информацию о репутации программ и их модулей только из локальных баз.

  Список программ, для которых Kaspersky Endpoint Security определяет KL-категорию **Программы, доверенные согласно репутации в KSN**, при наличии соединения с серверами KSN может отличаться от списка программ, для которых Kaspersky Endpoint Security определяет KL-категорию **Программы, доверенные согласно репутации в KSN**, при отсутствии соединения с KSN.

- В базе данных Kaspersky Security Center может храниться информация о 150 000 обработанных файлов. При достижении этого количества записей новые файлы не будут обработаны. Для возобновления работы инвентаризации требуется удалить с компьютера, на котором установлена программа Kaspersky Endpoint Security, файлы, учтенные в базе данных Kaspersky Security Center ранее в результате инвентаризации.
- Компонент не контролирует запуск скриптов, если скрипт передается интерпретатору не через командную строку.

Если запуск интерпретатора разрешен правилами Контроля программ, то компонент не блокирует скрипт, запущенный из этого интерпретатора.
Если запуск хотя бы одного из скриптов, указанных в командной строке интерпретатора, запрещен правилами Контроля программ, то компонент блокирует все скрипты, указанные в командной строке интерпретатора.

- Компонент не контролирует запуск скриптов из интерпретаторов, не поддерживаемых программой Kaspersky Endpoint Security.

  Kaspersky Endpoint Security поддерживает следующие интерпретаторы:

  - Java;
  - PowerShell.

  Поддерживаются следующие типы интерпретаторов:

  - %ComSpec%;
  - %SystemRoot%\\system32\\regedit.exe;
  - %SystemRoot%\\regedit.exe;
  - %SystemRoot%\\system32\\regedt32.exe;
  - %SystemRoot%\\system32\\cscript.exe;
  - %SystemRoot%\\system32\\wscript.exe;
  - %SystemRoot%\\system32\\msiexec.exe;
  - %SystemRoot%\\system32\\mshta.exe;
  - %SystemRoot%\\system32\\rundll32.exe;
  - %SystemRoot%\\system32\\wwahost.exe;
  - %SystemRoot%\\syswow64\\cmd.exe;
  - %SystemRoot%\\syswow64\\regedit.exe;
  - %SystemRoot%\\syswow64\\regedt32.exe;
  - %SystemRoot%\\syswow64\\cscript.exe;
  - %SystemRoot%\\syswow64\\wscript.exe;
  - %SystemRoot%\\syswow64\\msiexec.exe;
  - %SystemRoot%\\syswow64\\mshta.exe;
  - %SystemRoot%\\syswow64\\rundll32.exe;
  - %SystemRoot%\\syswow64\\wwahost.exe.

kaspersky

Включение и выключение Контроля программ

По умолчанию Контроль программ выключен.

► *Чтобы включить или выключить Контроль программ выполните следующие действия:*

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Защита** → **Контроль безопасности** → **Контроль программ**.
3. Используйте переключатель **Контроль программ**, чтобы включить или выключить компонент.
4. Сохраните внесенные изменения.

В результате, если Контроль программ включен, программа передает в Kaspersky Security Center информацию о запущенных исполняемых файлах. Вы можете просмотреть список запущенных исполняемых файлов в Kaspersky Security Center в папке **Исполняемые файлы**. Для получения информации обо всех исполняемых файлах, а не только о запущенных файлах, запустите задачу *Инвентаризация*.

Выбор режима Контроля программ

► *Чтобы выбрать режим Контроля программ, выполните следующие действия:*

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Защита** → **Контроль безопасности** → **Контроль программ**.
3. В блоке **Режим контроля запуска программ** выберите один из следующих вариантов:
   - **Список запрещенных**. Если выбран этот вариант, Контроль программ разрешает всем пользователям запуск любых программ, кроме случаев, удовлетворяющих условиям запрещающих правил Контроля программ.
   - **Список разрешенных**. Если выбран этот вариант, Контроль программ запрещает всем пользователям запуск любых программ, кроме случаев, удовлетворяющих условиям разрешающих правил Контроля программ.

     Для режима Список разрешенных программ изначально заданы правила **Программы ОС** и **Доверенные программы обновления**. Эти правила Контроля программ соответствуют KL-категориям. В KL-категорию "Программы ОС" входят программы, обеспечивающие нормальную работу операционной системы. В KL-категорию "Доверенные программы обновления" входят программы обновления наиболее известных производителей программного обеспечения. Вы не можете удалить эти правила. Параметры этих правил недоступны для изменения. По умолчанию правило **Программы ОС** включено, а правило **Доверенные программы обновления** выключено. Запуск программ, соответствующих условиям срабатывания этих правил, разрешен всем пользователям.

Все правила, сформированные при выбранном режиме, сохраняются после смены режима для возможности их повторного использования. Чтобы вернуться к использованию этих правил, достаточно выбрать нужный режим.

4. В блоке **Действие при запуске запрещенных программ** выберите, какое действие компонент должен выполнять при попытке пользователя запустить программу, запрещенную правилами Контроля программ.
5. Установите флажок **Контролировать загрузку DLL-модулей**, если вы хотите, чтобы программа Kaspersky Endpoint Security контролировала загрузку DLL-модулей при запуске пользователями программ.

   Информация о модуле и программе, загрузившей этот модуль, будет сохранена в отчет.

   Kaspersky Endpoint Security контролирует только DLL-модули и драйверы, загруженные с момента установки флажка. Перезагрузите компьютер после установки флажка, если вы хотите, чтобы программа Kaspersky Endpoint Security контролировала все DLL-модули и драйверы, включая те, которые загружаются до запуска Kaspersky Endpoint Security.

   При включении функции контроля загрузки DLL-модулей и драйверов убедитесь, что в параметрах Контроля программ включено правило по умолчанию **Программы ОС** или другое правило, которое содержит KL-категорию "Доверенные сертификаты" и обеспечивает загрузку доверенных DLL-модулей и драйверов до запуска Kaspersky Endpoint Security. Включение контроля загрузки DLL-модулей и драйверов при выключенном правиле **Программы ОС** может привести к нестабильности операционной системы.

   Рекомендуется включить защиту паролем (см. раздел "Включение Защиты паролем" на стр. 192) для настройки параметров программы, чтобы иметь возможность выключить запрещающие правила, блокирующие запуск критически важных DLL-модулей и драйверов, не изменяя при этом параметры политики Kaspersky Security Center.
6. Сохраните внесенные изменения.

Действия с правилами Контроля программ в интерфейсе программы

Kaspersky Endpoint Security контролирует запуск программ пользователями с помощью правил. В правиле Контроля программ содержатся условия срабатывания и действия компонента Контроль программ при срабатывании правила (разрешение или запрещение пользователям запускать программу).

Условия срабатывания правила

Условие срабатывания правила представляет собой соответствие "тип условия - критерий условия - значение условия". На основании условий срабатывания правила Kaspersky Endpoint Security применяет (или не применяет) правило к программе.

В правилах используются следующие типы условий:

- *Включающие условия*. Kaspersky Endpoint Security применяет правило к программе, если программа соответствует хотя бы одному включающему условию.

- *Исключающие условия*. Kaspersky Endpoint Security не применяет правило к программе, если программа соответствует хотя бы одному исключающему условию или не соответствует ни одному включающему условию.

Условия срабатывания правила формируются с помощью критериев. Для формирования условий в Kaspersky Endpoint Security используются следующие критерии:

- путь к папке с исполняемым файлом программы или путь к исполняемому файлу программы;
- метаданные: название исполняемого файла программы, версия исполняемого файла программы, название программы, версия программы, производитель программы;
- хеш исполняемого файла программы;
- сертификат: издатель, субъект, отпечаток;
- принадлежность программы к KL-категории;
- расположение исполняемого файла программы на съемном диске.

Для каждого критерия, используемого в условии, нужно указать его значение. Если параметры запускаемой программы соответствуют значениям критериев, указанных во включающем условии, правило срабатывает. В этом случае Контроль программ выполняет действие, прописанное в правиле. Если параметры программы соответствуют значениям критериев, указанных в исключающем условии, Контроль программ не контролирует запуск программы.

Решения компонента Контроль программ при срабатывании правила

При срабатывании правила Контроль программ в соответствии с правилом разрешает или запрещает пользователям (группам пользователей) запускать программы. Вы можете выбирать отдельных пользователей или группы пользователей, которым разрешен или запрещен запуск программ, для которых срабатывает правило.

Если в правиле не указан ни один пользователь, которому разрешен запуск программ, удовлетворяющих правилу, правило называется *запрещающим*.

Если в правиле не указан ни один пользователь, которому запрещен запуск программ, удовлетворяющих правилу, правило называется *разрешающим*.

Приоритет запрещающего правила выше приоритета разрешающего правила. Например, если для группы пользователей назначено разрешающее правило Контроля программы и для одного из пользователей этой группы назначено запрещающее правило Контроля программы, то этому пользователю будет запрещен запуск программы.

Статус работы правила

Правила Контроля программ могут иметь один из следующих статусов работы:

- **Вкл**. Статус означает, что правило используется во время работы компонента Контроль программ.
- **Выкл**. Статус означает, что правило не используется во время работы компонента Контроль программ.
- **Тест**. Статус означает, что Kaspersky Endpoint Security разрешает запуск программ, на которые распространяется действие правила, но заносит информацию о запуске этих программ в отчет.

kaspersky

В этом разделе

Добавление правила Контроля программ

► *Чтобы добавить правило Контроля программ, выполните следующие действия:*

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Защита** → **Контроль безопасности** → **Контроль программ**.
3. Нажмите на кнопку **Запрещенные программы** или **Разрешенные программы**.

   Откроется список правил Контроля программ.
4. Нажмите на кнопку **Добавить**.

   Откроется окно **Правило Контроля программ**.
5. На закладке **Общие настройки** задайте основные параметры правила:
   a. В поле **Название правила** введите название правила.
   b. В поле **Описание** введите описание правила.
   c. Задайте или измените список пользователей и / или групп пользователей, которым разрешено или запрещено запускать программы, удовлетворяющие условиям срабатывания правила. Для этого нажмите на кнопку **Добавить** в таблице **Субъекты и их права**.

      По умолчанию в список пользователей добавлено значение **Все**. Действие правила распространяется на всех пользователей.

      > Если в таблице не указан ни один пользователь, правило не может быть сохранено.

   d. В таблице **Субъекты и их права** определите право пользователей на запуск программ с помощью переключателя.
   e. Установите флажок **Запретить остальным пользователям**, если вы хотите, чтобы программа запрещала запуск программ, удовлетворяющих условиям срабатывания правила, всем пользователям, которые не указаны в графе **Субъект** и не входят в группы пользователей, указанные в графе **Субъект**.

      > Если флажок **Запретить остальным пользователям** снят, Kaspersky Endpoint Security не контролирует запуск программ пользователями, которые не указаны в таблице **Субъекты и их права** и не входят в группы пользователей, указанные в таблице **Субъекты и их права**.

f. Установите флажок **Доверенные программы обновления**, если вы хотите, чтобы программы, удовлетворяющие условиям срабатывания правила, Kaspersky Endpoint Security считал доверенными программами обновления с правом создавать другие исполняемые файлы, запуск которых в дальнейшем будет разрешен.

6. На закладке **Условия** сформируйте (см. раздел "Добавление условия срабатывания в правило Контроля программ" на стр. 154) или измените список включающих условий срабатывания правила.
7. На закладке **Исключения** сформируйте или измените список исключающих условий срабатывания правила.

   При миграции параметров Kaspersky Endpoint Security осуществляется также миграция списка исполняемых файлов, созданных доверенными программами обновления.
8. Сохраните внесенные изменения.

Добавление условия срабатывания в правило Контроля программ

► *Чтобы добавить новое условие срабатывания в правило Контроля программ, выполните следующие действия:*

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Защита → Контроль безопасности → Контроль программ**.
3. Нажмите на кнопку **Запрещенные программы** или **Разрешенные программы**.

   Откроется список правил Контроля программ.
4. Выберите правило, для которого вы хотите добавить условие срабатывания.

   Откроются свойства правила Контроля программ.
5. Перейдите на закладку **Условия** или **Исключения** и нажмите на кнопу **Добавить**.
6. Выберите условия срабатывания правила Контроля программ:

   - **Условия из свойств запускавшихся программ**. Вы можете выбрать программы, к которым будет применено правило Контроля программ, из списка запущенных программ. Kaspersky Endpoint Security также добавляет в этот список программы, которые когда-либо были запущены на компьютере. Вам нужно выбрать критерий, на основе которого вы хотите создать одно или несколько условий срабатывания правила: **Хеш файла**, **Сертификат**, **KL-категория**, **Метаданные** или **Путь к папке**.
   - **Условия "KL-категория"**. *KL-категория* – сформированный специалистами "Лаборатории Касперского" список программ, обладающих общими тематическими признаками. Например, KL-категория "Офисные программы" включает в себя программы из пакетов Microsoft Office, Adobe® Acrobat® и другие.
   - **Условие вручную**. Вы можете выбрать файл программы и выбрать одно из условий срабатывания правила: **Хеш файла**, **Сертификат**, **Метаданные** или **Путь к файлу или папке**.
   - **Условие по носителю файла (съемный диск)**. Правило Контроля программ применяется только к файлам, которые запускаются на съемном диске.
   - **Условия из свойств файлов указанной папки**. Привило Контроля программ применяется только к файлам, которые расположены в указанной папке. Вы также можете включить или исключить файлы из вложенных папок. Вам нужно выбрать критерий, на основе которого вы хотите создать одно или несколько условий срабатывания правила: **Хеш файла**, **Сертификат**, **KL-категория**, **Метаданные** или **Путь к папке**.

7. Сохраните внесенные изменения.

При добавлении условий учитывайте следующие особенности работы Контроля программ:

- Kaspersky Endpoint Security не поддерживает MD5-хеш файла и не контролирует запуск приложений на основе MD5-хеша. В качестве условия срабатывания правила используется SHA256-хеш.
- Не рекомендуется использовать в качестве условий срабатывания правил только критерии **Издатель** и **Субъект**. Использование этих критериев является ненадежным.
- Если вы используете символьную ссылку в поле **Путь к файлу или папке**, рекомендуется развернуть символьную ссылку для корректной работы правила Контроля программ. Для этого нажмите на кнопку **Развернуть символьную ссылку**.

Изменение статуса правила Контроля программ

► *Чтобы изменить статус правила Контроля программ, выполните следующие действия:*

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Защита** → **Контроль безопасности** → **Контроль программ**.
3. Нажмите на кнопку **Запрещенные программы** или **Разрешенные программы**.

   Откроется список правил Контроля программ.
4. В графе **Статус** откройте контекстное меню и выберите один из следующих пунктов:
   - **Включено**. Статус означает, что правило используется во время работы компонента Контроль программ.
   - **Выключено**. Статус означает, что правило не используется во время работы компонента Контроль программ.
   - **Тестирование**. Статус означает, что Kaspersky Endpoint Security всегда разрешает запуск программ, на которые распространяется действие этого правила, но заносит информацию о запуске этих программ в отчет.
5. Сохраните внесенные изменения.

Тестирование правил Контроля программ

Чтобы убедиться, что правила Контроля программ не блокируют программы, необходимые для работы, рекомендуется после создания правил включить тестирование правил Контроля программ и проанализировать их работу.

Для анализа работы правил Контроля программ требуется изучить события по результатам работы компонента Контроль программ, приходящие в Kaspersky Security Center. Если для всех программ, которые необходимы для работы пользователю компьютера, отсутствуют события о запрете запуска в тестовом режиме, то созданы верные правила. В противном случае рекомендуется уточнить параметры созданных вами правил, создать дополнительные или удалить существующие правила.

► *Чтобы включить тестирование правил Контроля программ или выбрать блокирующее действие Контроля программ, выполните следующие действия:*

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Защита** → **Контроль безопасности** → **Контроль программ**.

   Откроется список правил Контроля программ.
3. В графе **Статус** выберите пункт **Тестирование**.

   Статус означает, что Kaspersky Endpoint Security всегда разрешает запуск программ, на которые распространяется действие этого правила, но заносит информацию о запуске этих программ в отчет.
4. Сохраните внесенные изменения.

Kaspersky Endpoint Security не будет блокировать программы, запуск которых запрещен компонентом Контроль программ, но будет отправлять уведомления об их запуске на Сервер администрирования.

Мониторинг активности программ

Мониторинг активности программ – это инструмент, предназначенный для просмотра информации об активности программ на компьютере пользователя в режиме реального времени.

► *Чтобы запустить мониторинг активности программ,*

в главном окне программы нажмите на кнопку **Больше функций** → **Мониторинг активности программ**.

Откроется окно **Активность программ**. В этом окне информация об активности программ на компьютере пользователя представлена на трех закладках:

- На закладке **Все программы** отображается информация о всех программах, установленных на компьютере.
- На закладке **Работающие** отображается информация о потреблении ресурсов компьютера каждой из программ в режиме реального времени. На этой закладке вы можете, а также перейти к настройке разрешений для отдельной программы.
- На закладке **Запускается при старте** отображается список программ, которые запускаются при старте операционной системы.

Правила формирования масок имен файлов или папок

Маска имени файла или папки – это представление имени папки или имени и расширения файла с использованием общих символов.

Для формирования маски имени файла или папки вы можете использовать следующие общие символы:

- Символ `*`, который заменяет любой набор символов, в том числе пустой, кроме символов `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\*\*.txt` будет включать все пути к файлам с расширением txt, расположенным в папках на диске (C:), но не в подпапках.

- Символ `?`, который заменяет любой один символ, кроме символов `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\Folder\???.txt` будет включать пути ко всем расположенным в папке `Folder` файлам с расширением txt и именем, состоящим из трех символов.

Изменение шаблонов сообщений Контроля программ

Когда пользователь пытается запустить программу, запрещенную правилом Контроля программ, Kaspersky Endpoint Security выводит сообщение о блокировке запуска программы. Если блокировка запуска программы, по мнению пользователя, произошла ошибочно, по ссылке из текста сообщения о блокировке пользователь может отправить сообщение администратору локальной сети организации.

Для сообщения о блокировке запуска программы и сообщения администратору предусмотрены шаблоны. Вы можете изменять шаблоны сообщений.

► *Чтобы изменить шаблон сообщения, выполните следующие действия:*

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Защита** → **Контроль безопасности** → **Контроль программ**.
3. В блоке **Шаблоны** настройте шаблоны сообщений Контроля программы:
   - **Блокировка**. Шаблон сообщения, которое появляется при срабатывании правила Контроля программ, блокирующего запуск программы.
   - **Сообщение администратору**. Шаблон сообщения для отправки администратору локальной сети организации в случае, если блокировка программы, по мнению пользователя, произошла ошибочно.
4. Сохраните внесенные изменения.

См. также

Изменение шаблонов сообщений Веб-Контроля 178

Изменение шаблонов сообщений Адаптивного контроля аномалий 166

kaspersky

Адаптивный контроль аномалий

Этот компонент доступен только для решений Kaspersky Endpoint Security для бизнеса Расширенный и Kaspersky Total Security для бизнеса. Подробнее о решениях Kaspersky Endpoint Security для бизнеса см. на *сайте "Лаборатории Касперского"* https://www.kaspersky.ru/business-security/small-to-medium-business.
Этот компонент доступен, если программа Kaspersky Endpoint Security установлена на компьютере под управлением операционной системы Windows для рабочих станций. Этот компонент недоступен, если программа Kaspersky Endpoint Security установлена на компьютере под управлением операционной системы Windows для серверов.

Компонент Адаптивный контроль аномалий отслеживает и блокирует действия, нехарактерные для компьютеров сети организации. Для отслеживания нехарактерных действий Адаптивный контроль аномалий использует набор правил (например, правило *Запуск Windows PowerShell из офисной программы*). Правила созданы специалистами "Лаборатории Касперского" на основе типичных сценариев вредоносной активности. Вы можете выбрать поведение Адаптивного контроля аномалий для каждого из правил и, например, разрешить запуск PowerShell-скриптов для автоматизации решения корпоративных задач. Kaspersky Endpoint Security обновляет набор правил с базами программы. Обновление набора правил нужно подтверждать вручную (см. раздел "Применение обновлений для правил Адаптивного контроля аномалий" на стр. 165).

Настройка Адаптивного контроля аномалий

Настройка Адаптивного контроля аномалий состоит из следующих этапов:

1. Обучение Адаптивного контроля аномалий.

   После включения Адаптивного контроля аномалий правила работают в *обучающем режиме*. В ходе обучения Адаптивный контроль аномалий отслеживает срабатывание правил и отправляет события срабатывания в Kaspersky Security Center. Каждое правило имеет свой срок действия обучающего режима. Срок действия обучающего режима устанавливают специалисты "Лаборатории Касперского". Обычно срок действия обучающего режима составляет 2 недели.

   Если в ходе обучения правило ни разу не сработало, Адаптивный контроль аномалий будет считать действия, связанные с этим правилом, нехарактерным. Kaspersky Endpoint Security будет блокировать все действия, связанные с этим правилом.

   Если в ходе обучения правило сработало, Kaspersky Endpoint Security регистрирует события в отчете о срабатываниях правил (см. раздел "Просмотр отчетов Адаптивного контроля аномалий" на стр. 166) и в хранилище **Срабатывание правил в обучающем режиме**.

2. Анализ отчета о срабатывании правил.

   Администратор анализирует отчет о срабатываниях правил (см. раздел "Просмотр отчетов Адаптивного контроля аномалий" на стр. 166) или содержание хранилища **Срабатывание правил в обучающем режиме**. Далее администратор может выбрать поведение Адаптивного контроля аномалий при срабатывании правила: блокировать или разрешить. Также администратор может продолжить отслеживать срабатывание правила и продлить работу программы в обучающем режиме. Если администратор не предпринимает никаких мер, программа также продолжит работать в обучающем режиме. Отсчет срока действия обучающего режима начинается заново.

Настройка Адаптивного контроля аномалий происходит в режиме реального времени. Настройка Адаптивного контроля аномалий осуществляется по следующим каналам:

- Адаптивный контроль аномалий автоматически начинает блокировать действия, связанные с правилами, которые не сработали в течение обучающего режима.
- Kaspersky Endpoint Security добавляет новые правила или удаляет неактуальные.
- Администратор настраивает работу Адаптивного контроля аномалий после анализа отчета о срабатывании правил и содержимого хранилища **Срабатывание правил в обучающем режиме**. Рекомендуется проверять отчет о срабатывании правил и содержимое хранилища **Срабатывание правил в обучающем режиме**.

При попытке вредоносной программы выполнить действие, Kaspersky Endpoint Security заблокирует действие и покажет уведомление (см. рис. ниже).

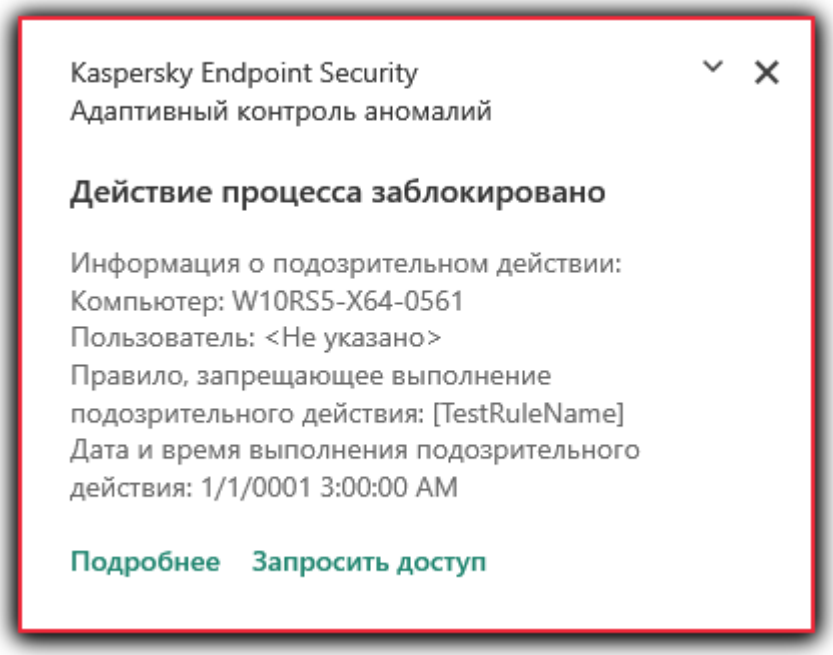


Рисунок 16. Уведомление Адаптивного контроля аномалий

Алгоритм работы Адаптивного контроля аномалий

Kaspersky Endpoint Security принимает решение о выполнении действия, связанного с правилом, по следующему алгоритму (см. рис. ниже).

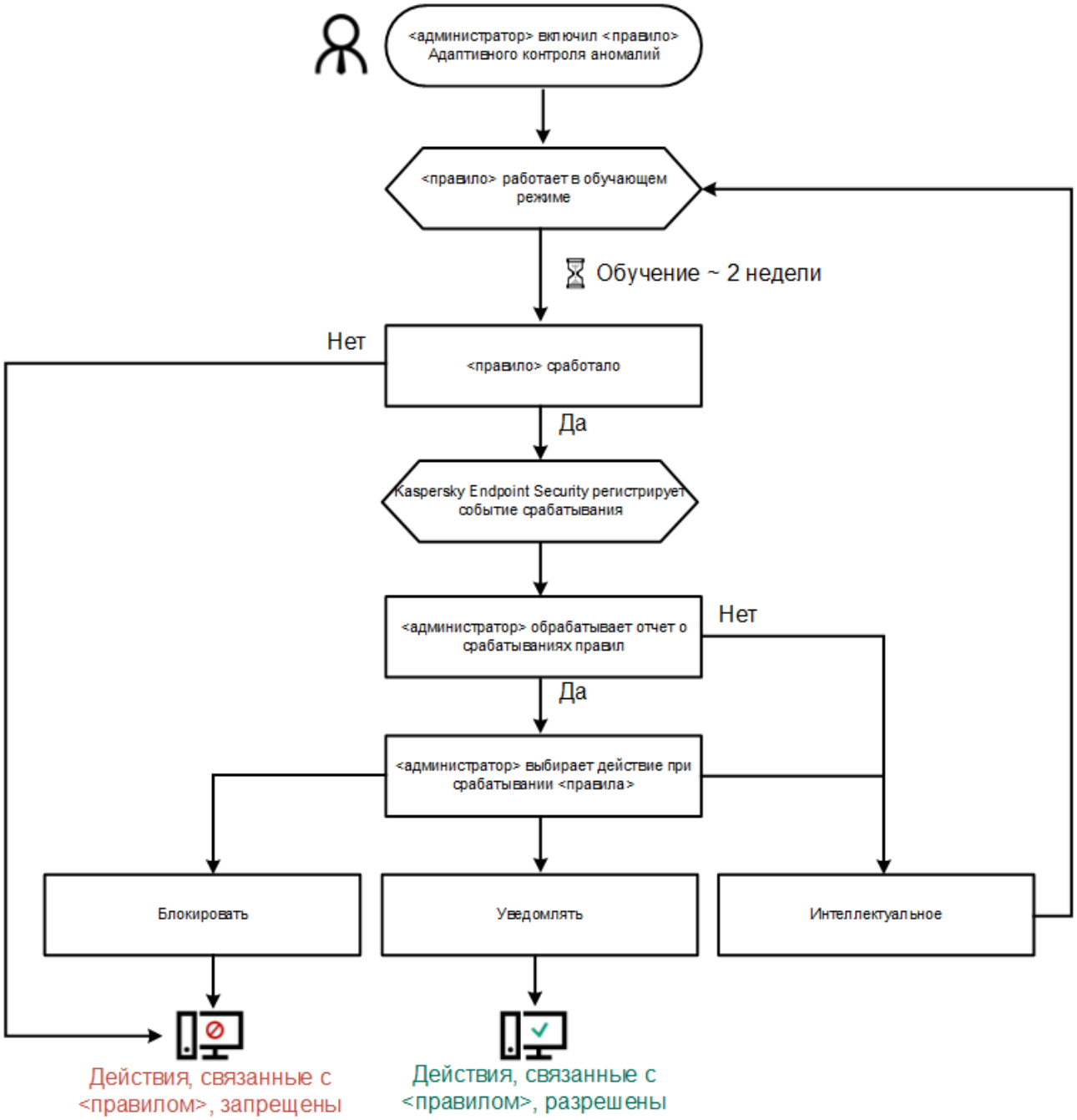


Рисунок 17. Алгоритм работы Адаптивного контроля аномалий

kaspersky

В этом разделе

Включение и выключение Адаптивного контроля аномалий

По умолчанию Адаптивный контроль аномалий включен.

► *Чтобы включить или выключить Адаптивный контроль аномалий, выполните следующие действия:*

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Защита** → **Контроль безопасности** → **Адаптивный контроль аномалий**.
3. Используйте переключатель **Адаптивный контроль аномалий**, чтобы включить или выключить компонент.
4. Сохраните внесенные изменения.

Включение и выключение правила Адаптивного контроля аномалий

► *Чтобы включить или выключить правило Адаптивного контроля аномалий, выполните следующие действия:*

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Защита** → **Контроль безопасности** → **Адаптивный контроль аномалий**.
3. В блоке **Правила** нажмите на кнопку **Изменить правила**.

   Откроется список правил Адаптивного контроля аномалий.
4. В таблице выберите набор правил (например, *Активность офисных программ*) и разверните набор.

5. Выберите правило (например, Запуск *Windows PowerShell из офисных программ*).
6. Используйте переключатель в графе **Статус**, чтобы включить или выключить правило Адаптивного контроля аномалий.
7. Сохраните внесенные изменения.

Изменение действия при срабатывании правила Адаптивного контроля аномалий

► *Чтобы изменить действие при срабатывании правила Адаптивного контроля аномалий, выполните следующие действия:*

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Защита** → **Контроль безопасности** → **Адаптивный контроль аномалий**.
3. В блоке **Правила** нажмите на кнопку **Изменить правила**.

   Откроется список правил Адаптивного контроля аномалий.
4. В таблице выберите правило.
5. Нажмите на кнопку **Изменить**.

   Откроется окно свойств правила Адаптивного контроля аномалий.
6. В блоке **Действие** выберите один из следующих пунктов:
   - **Интеллектуальное**. Если выбран этот вариант, то правило Адаптивного контроля аномалий работает в обучающем режиме в течение периода, определенного специалистами "Лаборатории Касперского". В этом режиме при срабатывании правила Адаптивного контроля аномалий Kaspersky Endpoint Security разрешает активность, подпадающую под это правило, и создает запись в хранилище **Срабатывание правил в обучающем режиме** Сервера администрирования Kaspersky Security Center. По истечении периода работы обучающего режима Kaspersky Endpoint Security блокирует активность, подпадающую под правило Адаптивного контроля аномалий, и создает в журнале запись, содержащую информацию об этой активности.
   - **Блокировать**. Если выбрано это действие, то при срабатывании правила Адаптивного контроля аномалий Kaspersky Endpoint Security блокирует активность, подпадающую под это правило, и создает в журнале запись, содержащую информацию об этой активности.
   - **Информировать**. Если выбрано это действие, то при срабатывании правила Адаптивного контроля аномалий Kaspersky Endpoint Security разрешает активность, подпадающую под это правило, и создает в журнале запись, содержащую информацию об этой активности.
7. Сохраните внесенные изменения.

kaspersky

Создание исключения для правила Адаптивного контроля аномалий

Для правил Адаптивного контроля аномалий невозможно создать более 1000 исключений. Не рекомендуется создавать более 200 исключений. Чтобы уменьшить количество используемых исключений, рекомендуется использовать маски в параметрах исключений.

Исключение для правила Адаптивного контроля аномалий включает в себя описание исходных и целевых объектов. *Исходный объект* – объект, который выполняет действия. *Целевой объект* – объект, над которым выполняются действия. Например, вы открыли файл `file.xlsx`. В результате в память компьютера была добавлена библиотека с расширением dll, которую использует браузер (исполняемый файл `browser.exe`). В данном примере `file.xlsx` – исходный объект, Excel – исходный процесс, `browser.exe` – целевой объект, Browser – целевой процесс.

► *Чтобы создать исключение для правила Адаптивного контроля аномалий, выполните следующие действия:*

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Защита** → **Контроль безопасности** → **Адаптивный контроль аномалий**.
3. В блоке **Правила** нажмите на кнопку **Изменить правила**.

   Откроется список правил Адаптивного контроля аномалий.
4. В таблице выберите правило.
5. Нажмите на кнопку **Изменить**.

   Откроется окно свойств правила Адаптивного контроля аномалий.
6. В блоке **Исключения** нажмите на кнопку **Добавить**.

   Откроется окно свойств исключения.
7. Выберите пользователей или группы пользователей, для которых вы хотите настроить исключение.
8. В поле **Описание** введите описание исключения.
9. Задайте параметры исходного объекта или исходного процесса, запущенных объектом:
   - **Исходный процесс**. Путь или маска пути к файлу или папке с файлами (например, `C:\Dir\File.exe` или `Dir\*.exe`**)**.
   - **Хеш исходного процесса**. Хеш файла.

- **Исходный объект**. Путь или маска пути к файлу или папке с файлами (например, `C:\Dir\File.exe` или `Dir\*.exe`). Например, путь к файлу `document.docm`, который запускает целевые процессы с помощью скрипта или макроса.

  Вы также можете указать другие объекты для исключения, например, веб-адрес, макрос, команду в командной строке, путь реестра и другие. Укажите объект по следующему шаблону: `object://<объект>`, где `<объект>` – название объекта, например, `object://web.site.example.com`, `object://VBA`, `object://ipconfig`, `object://HKEY_USERS`. Вы также можете использовать маски, например, `object://*C:\Windows\temp\*`.

- **Хеш исходного объекта**. Хеш файла.

Правило Адаптивного контроля аномалий не распространяется на действия, выполняемые объектом, или на процессы, запущенные объектом.

10. Задайте параметры целевого объекта или целевых процессов, запущенных над объектом.

    - **Целевой процесс**. Путь или маска пути к файлу или папке с файлами (например, `C:\Dir\File.exe` или `Dir\*.exe`**)**.
    - **Хеш целевого процесса**. Хеш файла.
    - **Целевой объект**. Команда запуска целевого процесса. Укажите команду по следующему шаблону `object://<команда>`, например, `object://cmdline:powershell -Command "$result = 'C:\windows\temp\result_local_users_pwdage.txt'"`. Также вы можете использовать маски, например, `object://*C:\windows\temp\*`.
    - **Хеш целевого объекта**. Хеш файла.

    Правило Адаптивного контроля аномалий не распространяется на действия над объектом или на процессы, запущенные над объектом.

11. Сохраните внесенные изменения.

Экспорт и импорт исключений для правил Адаптивного контроля аномалий

► *Чтобы экспортировать или импортировать список исключений для выбранных правил, выполните следующие действия:*

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Защита** → **Контроль безопасности** → **Адаптивный контроль аномалий**.
3. В блоке **Правила** нажмите на кнопку **Изменить правила**.

   Откроется список правил Адаптивного контроля аномалий.
4. Для экспорта списка исключений выполните следующие действия:
   a. Выберите правила, исключения для которых вы хотите экспортировать.
   b. Нажмите на кнопку **Экспорт**.
   c. В открывшемся окне введите имя файла формата XML, в который вы хотите экспортировать список исключений, а также выберите папку, в которой вы хотите сохранить этот файл.

d. Подтвердите, что вы хотите экспортировать только выбранные исключения, или экспортируйте весь список.

e. Нажмите на кнопку **Сохранить**.

5. Для импорта списка исключений, выполните следующие действия:

a. Нажмите на кнопку **Импорт**.

b. В открывшемся окне выберите XML-файл, из которого вы хотите импортировать список исключений.

c. Нажмите на кнопку **Открыть**.

Если на компьютере уже есть список исключений, Kaspersky Endpoint Security предложит удалить действующий список или добавить в него новые записи из XML-файла.

6. Сохраните внесенные изменения.

Применение обновлений для правил Адаптивного контроля аномалий

Новые правила Адаптивного контроля аномалий могут быть добавлены в таблицу правил и существующие правила Адаптивного контроля аномалий могут быть удалены из таблицы правил по результату обновления антивирусных баз. Kaspersky Endpoint Security выделяет удаляемые и добавляемые правила Адаптивного контроля аномалий в таблице, если для этих правил обновление не было применено.

До тех пор, пока обновление не применено, Kaspersky Endpoint Security отображает удаленные в результате обновления правила Адаптивного контроля аномалий в таблице правил и присваивает этим правилам статус *Выключено*. Изменение параметров этих правил невозможно.

► *Чтобы применить обновления для правил Адаптивного контроля аномалий, выполните следующие действия:*

1. В нижней части главного окна программы нажмите на кнопку .
2. В окне параметров программы выберите раздел **Защита** → **Контроль безопасности** → **Адаптивный контроль аномалий**.
3. В блоке **Правила** нажмите на кнопку **Изменить правила**.

Откроется список правил Адаптивного контроля аномалий.

4. В открывшемся окне нажмите на кнопку **Подтвердить обновления**.

Кнопка **Подтвердить обновления** доступна, если доступно обновление для правил Адаптивного контроля аномалий.

5. Сохраните внесенные изменения.

kaspersky

Изменение шаблонов сообщений Адаптивного контроля аномалий

Когда пользователь пытается выполнить действие, запрещенное правилами Адаптивного контроля аномалий, Kaspersky Endpoint Security выводит сообщение о блокировке потенциально опасных действий. Если блокировка, по мнению пользователя, произошла ошибочно, по ссылке из текста сообщения о блокировке пользователь может отправить сообщение администратору локальной сети организации.

Для сообщения о блокировке потенциально опасных действий и сообщения администратору предусмотрены шаблоны. Вы можете изменять шаблоны сообщений.

► *Чтобы изменить шаблон сообщения, выполните следующие действия:*

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Защита** → **Контроль безопасности** → **Адаптивный контроль аномалий**.
3. В блоке **Шаблоны** настройте шаблоны сообщений Адаптивного контроля аномалий:
   - **Блокировка**. Шаблон сообщения для пользователя, которое появляется при срабатывании правила Адаптивного контроля аномалий, блокирующего нехарактерное действие.
   - **Сообщение администратору**. Шаблон сообщения для отправки администратору локальной сети организации в случае, если блокировка действия, по мнению пользователя, произошла ошибочно.
4. Сохраните внесенные изменения.

См. также:

Изменение шаблонов сообщений Веб-Контроля 178

Изменение шаблонов сообщений Контроля программ 157

Просмотр отчетов Адаптивного контроля аномалий

► *Чтобы просмотреть отчеты Адаптивного контроля аномалий, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева Консоли администрирования откройте папку с названием группы администрирования, в состав которой входят нужные клиентские компьютеры.
3. В рабочей области выберите закладку **Политики**.
4. Выберите нужную политику и откройте свойства политики двойным щелчком мыши.
5. В разделе **Контроль безопасности** выберите подраздел **Адаптивный контроль аномалий**.

   В правой части окна отобразятся параметры компонента Адаптивный контроль аномалий.

6. Выполните одно из следующих действий:
    - Если вы хотите просмотреть отчет о параметрах правил Адаптивного контроля аномалий, нажмите на кнопку **Отчет о состоянии правил**.
    - Если вы хотите просмотреть отчет о срабатываниях правил Адаптивного контроля аномалий, нажмите на кнопку **Отчет о срабатываниях правил**.
7. Запустится процесс формирования отчета.

Отчет отобразится в новом окне.

kaspersky

Веб-Контроль

Этот компонент доступен, если программа Kaspersky Endpoint Security установлена на компьютере под управлением операционной системы Windows для рабочих станций. Этот компонент недоступен, если программа Kaspersky Endpoint Security установлена на компьютере под управлением операционной системы Windows для серверов.

Веб-Контроль управляет доступом пользователей к веб-ресурсам. Это позволяет уменьшить расход трафика и сократить нецелевое использование рабочего времени. При попытке пользователя открыть веб-сайт, доступ к которому ограничен Веб-Контролем, Kaspersky Endpoint Security заблокирует доступ или покажет предупреждение (см. рис. ниже).

Kaspersky Endpoint Security контролирует только HTTP- и HTTPS-трафик.

Для контроля HTTPS-трафика нужно включить проверку защищенных соединений (см. раздел "Настройка параметров проверки защищенных соединений" на стр. 140).

Способы управления доступом к веб-сайтам

Веб-Контроль позволяет настраивать доступ к веб-сайтам следующими способами:

- **Категория веб-сайта**. Категоризацию веб-сайтов обеспечивает облачная служба Kaspersky Security Network, эвристический анализ, а также база известных веб-сайтов (входит в состав баз программы). Вы можете ограничить доступ пользователей, например, к категории "Социальные сети" или другим категориям.
- **Тип данных**. Вы можете ограничить доступ пользователей к данным на веб-сайте и, например, скрыть графические изображения. Kaspersky Endpoint Security определяет тип данных по формату файла, а не по расширению.

  Kaspersky Endpoint Security не проверяет файлы внутри архивов. Например, если файлы изображений помещены в архив, Kaspersky Endpoint Security определит тип данных "Архивы", а не "Графические файлы".

- **Отдельный адрес**. Вы можете ввести веб-адрес или использовать маски (см. раздел "Правила формирования масок адресов веб-ресурсов" на стр. 179).

Вы можете использовать одновременно несколько способов регулирования доступа к веб-сайтам. Например, вы можете ограничить доступ к типу данных "Файлы офисных программ" только для категории веб-сайтов "Веб-почта".

Правила доступа к веб-сайтам

Веб-Контроль управляет доступом пользователей к веб-сайтам с помощью *правил доступа*. Вы можете настроить следующие дополнительные параметры правила доступа к веб-сайтам:

- Пользователи, на которых распространяется правило.

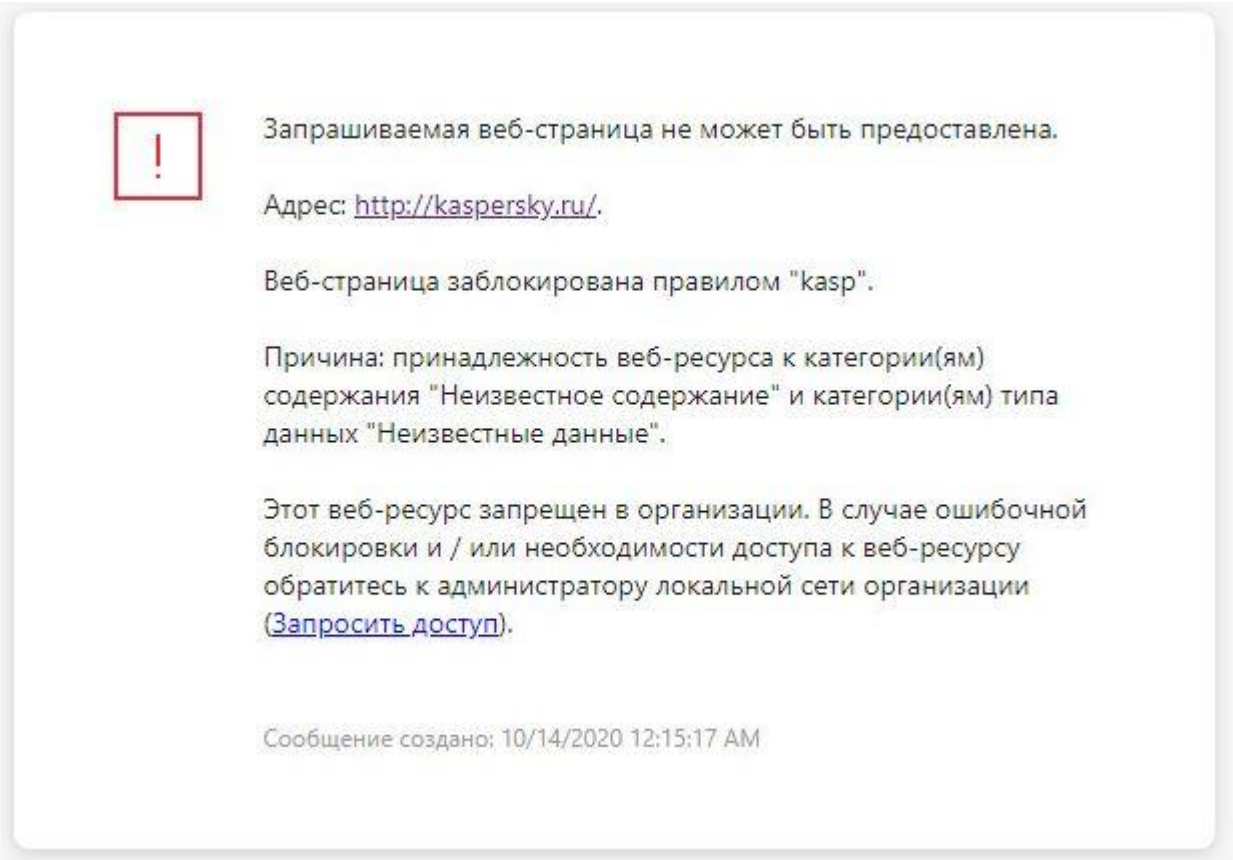
  Например, вы можете ограничить доступ в интернет через браузер для всех пользователей организации, кроме IT-отдела.

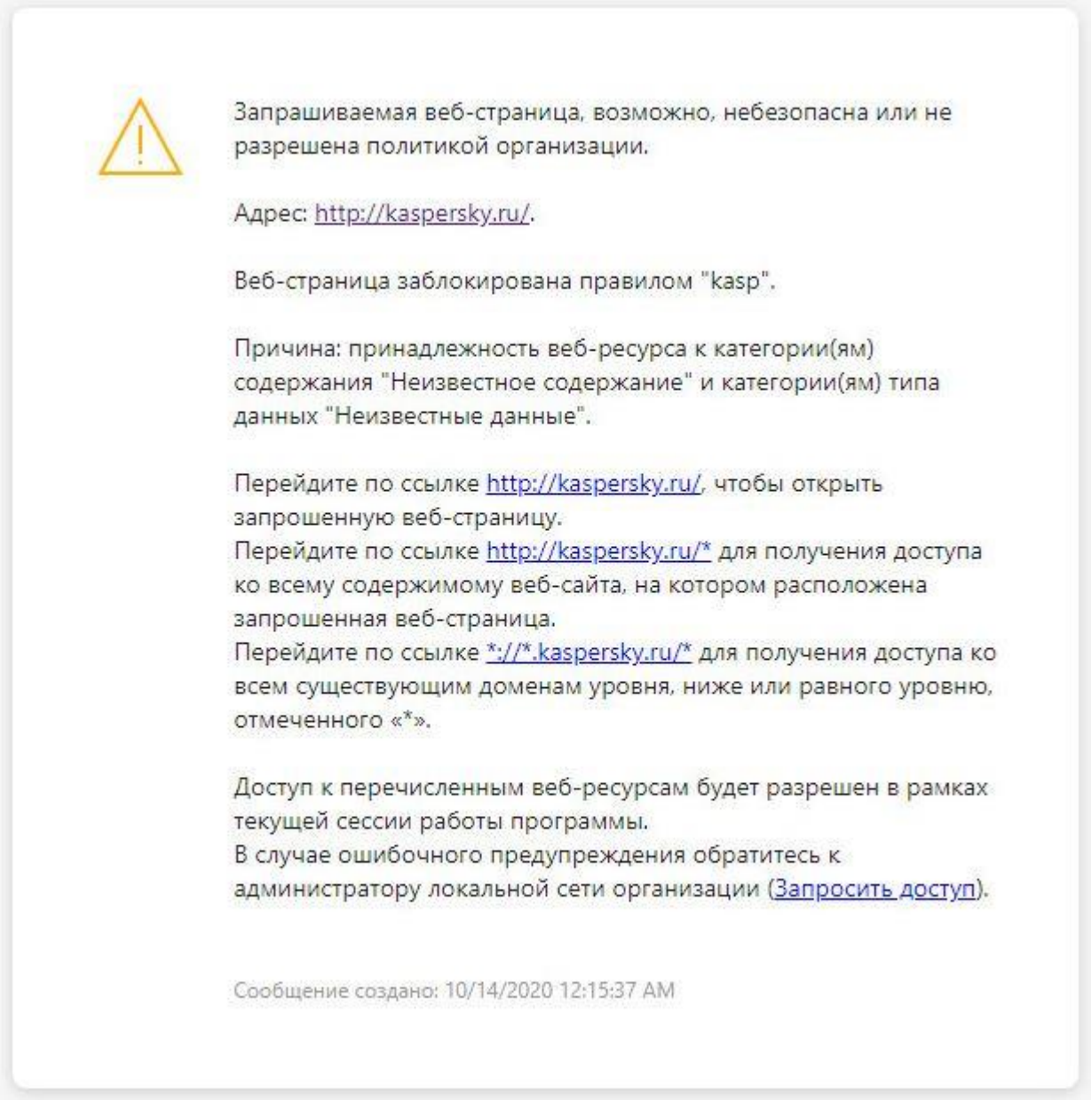
- Расписание работы правила.

  Например, вы можете ограничить доступ в интернет через браузер только в рабочее время.

Приоритеты правил доступа

Каждое правило имеет приоритет. Чем выше правило в списке, тем выше его приоритет. Если веб-сайт добавлен в несколько правил, Веб-Контроль регулирует доступ к веб-сайтам по правилу с высшим приоритетом. Например, Kaspersky Endpoint Security может определить корпоративный портал как социальную сеть. Чтобы ограничить доступ к социальным сетям и предоставить доступ к корпоративному веб-порталу, создайте два правила: запрещающее правило для категории веб-сайтов "Социальные сети" и разрешающее правило для корпоративного веб-портала. Правило доступа к корпоративному веб-порталу должно иметь приоритет выше, чем правило доступа к социальным сетям.





В этом разделе

kaspersky

Включение и выключение Веб-Контроля

По умолчанию Веб-Контроль включен.

► *Чтобы включить или выключить Веб-Контроль, выполните следующие действия:*

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Защита** → **Контроль безопасности** → **Веб-Контроль**.
3. Используйте переключатель **Веб-Контроль**, чтобы включить или выключить компонент.
4. Сохраните внесенные изменения.

Действия с правилами доступа к веб-ресурсам

Не рекомендуется создавать более 1000 правил доступа к веб-ресурсам, поскольку это может привести к нестабильности системы.

Правило доступа к веб-ресурсам представляет собой набор фильтров и действие, которое Kaspersky Endpoint Security выполняет при посещении пользователями описанных в правиле веб-ресурсов в указанное в расписании работы правила время. Фильтры позволяют точно задать круг веб-ресурсов, доступ к которым контролирует компонент Веб-Контроль.

Доступны следующие фильтры:

- **Фильтр по содержанию**. Веб-Контроль разделяет веб-ресурсы по категориям содержания и категориям типа данных. Вы можете контролировать доступ пользователей к размещенным на веб-ресурсах данным, относящихся к определенными этими категориями типам данных. При посещении пользователями веб-ресурсов, которые относятся к выбранной категории содержания и / или категории типа данных, Kaspersky Endpoint Security выполняет действие, указанное в правиле.
- **Фильтр по адресам веб-ресурсов**. Вы можете контролировать доступ пользователей ко всем адресам веб-ресурсов или к отдельным адресам веб-ресурсов и / или группам адресов веб-ресурсов.

  Если задан и фильтр по содержанию, и фильтр по адресам веб-ресурсов, и заданные адреса веб-ресурсов и / или группы адресов веб-ресурсов принадлежат к выбранным категориям содержания или категориям типа данных, Kaspersky Endpoint Security контролирует доступ не ко всем веб-ресурсам выбранных категорий содержания и / или категорий типа данных, а только к заданным адресам веб-ресурсов и / или группам адресов веб-ресурсов.
- **Фильтр по именам пользователей и групп пользователей**. Вы можете задавать пользователей и / или группы пользователей, для которых контролируется доступ к веб-ресурсам в соответствии с правилом.
- **Расписание работы правила**. Вы можете задавать расписание работы правила. Расписание работы правила определяет время, когда Kaspersky Endpoint Security контролирует доступ к веб-ресурсам, указанным в правиле.

После установки программы Kaspersky Endpoint Security список правил компонента Веб-Контроль не пуст.

kaspersky

Предустановлены два правила:

- Правило "Сценарии и таблицы стилей", которое разрешает всем пользователям в любое время доступ к веб-ресурсам, адреса которых содержат названия файлов с расширением css, js, vbs. Например: http://www.example.com/style.css, http://www.example.com/style.css?mode=normal.
- "Правило по умолчанию". Это правило в зависимости от выбранного действия разрешает или запрещает всем пользователям доступ ко всем веб-ресурсам, которые не попадают под действие других правил.

В этом разделе

Добавление правила доступа к веб-ресурсам

► *Чтобы добавить или изменить правило доступа к веб-ресурсам, выполните следующие действия:*

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Защита** → **Контроль безопасности** → **Веб-Контроль**.
3. В блоке **Настройки** нажмите на кнопку **Правила доступа к веб-ресурсам**.
4. В открывшемся окне нажмите на кнопку **Добавить**.

   Откроется окно **Правило доступа к веб-ресурсам**.
5. В поле **Название правила** введите название правила.
6. Установите статус правила доступа к веб-ресурсам **Активно**.

   Вы можете в любое время выключить правило доступа к веб-ресурсам (см. раздел "Включение и выключение правила доступа к веб-ресурсам" на стр. 174) с помощью переключателя.
7. В блоке **Действие** выберите нужный вариант:
   - **Разрешать**. Если выбрано это значение, то Kaspersky Endpoint Security разрешает доступ к веб-ресурсам, удовлетворяющим параметрам правила.
   - **Запрещать**. Если выбрано это значение, то Kaspersky Endpoint Security запрещает доступ к веб-ресурсам, удовлетворяющим параметрам правила.
   - **Предупреждать**. Если выбрано это значение, то при попытке доступа к веб-ресурсам, удовлетворяющим правилу, Kaspersky Endpoint Security выводит предупреждение о том, что веб-ресурс не рекомендован для посещения. По ссылкам из сообщения-предупреждения пользователь может получить доступ к запрошенному веб-ресурсу.

8. В блоке **Содержимое фильтра** выберите нужный фильтр по содержанию:

   - **По категориям содержания**. Вы можете контролировать доступ пользователей к веб-ресурсам по категориям (например, категория *Социальные сети*).
   - **По типам данных**. Вы можете контролировать доступ пользователей к веб-ресурсам по размещенным данным, относящихся к определенным типам данных (например, *Графические изображения*).

   Для настройки фильтра по содержанию выполните следующие действия:

   a. Нажмите на ссылку **Настроить**.

   b. Установите флажки напротив названий желаемых категорий содержания и / или типов данных.

      Установка флажка напротив названия категории содержания и / или типа данных означает, что Kaspersky Endpoint Security, в соответствии с правилом, контролирует доступ к веб-ресурсам, принадлежащим к выбранным категориям содержания и / или типам данных.

   c. Вернитесь в окно настройки правила доступа к веб-ресурсам.

9. В блоке **Адреса** выберите нужный фильтр по адресам веб-ресурсов:

   - **Ко всем адресам**. Веб-Контроль не фильтрует веб-ресурсы по адресам.
   - **К отдельным адресам**. Веб-Контроль фильтрует только адреса веб-ресурсов из списка. Для создания список адресов веб-ресурсов выполните следующие действия:

     a. Нажмите на кнопку **Добавить адрес** или **Добавить группу адресов**.

     b. В открывшемся окне сформируйте список адресов веб-ресурсов. Вы можете ввести веб-адрес или использовать маски (см. раздел «Правила формирования масок адресов веб-ресурсов» на стр. 179). Также вы можете экспортировать список адресов веб-ресурсов из TXT-файла (см. раздел «Экспорт и импорт списка адресов веб-ресурсов» на стр. 175).

     c. Вернитесь в окно настройки правила доступа к веб-ресурсам.

     Если Проверка защищенных соединений отключена (см. раздел "Проверка защищенных соединений" на стр. 140), для протокола HTTPS доступна фильтрация только по имени сервера.

10. В блоке **Пользователи** выберите нужный фильтр для пользователей:

    - **Ко всем пользователям**. Веб-Контроль не фильтрует веб-ресурсы для отдельных пользователей.
    - **К отдельным пользователям и / или группам**. Веб-Контроль фильтрует веб-ресурсы только для отдельных пользователей. Для создания списка пользователей, к которым вы хотите применить правило, выполните следующие действия:

      a. Нажмите на кнопку **Добавить**.

      b. В открывшемся окне выберите пользователей или группы пользователей, к которым вы хотите применить правило доступа к веб-ресурсам.

      c. Вернитесь в окно настройки правила доступа к веб-ресурсам.

11. Выберите из раскрывающегося списка **Расписание работы правила** название нужного расписания или сформируйте новое расписание на основе выбранного расписания работы правила. Для этого выполните следующие действия:
    a. Нажмите на кнопку **Изменить или добавить новое**.
    b. В открывшемся окне нажмите на кнопку **Добавить**.
    c. В открывшемся окне введите название расписания работы правила.
    d. Настройте расписание доступа к веб-ресурсам для пользователей.
    e. Вернитесь в окно настройки правила доступа к веб-ресурсам.
12. Сохраните внесенные изменения.

Назначение приоритета правилам доступа к веб-ресурсам

Вы можете назначить приоритет каждому правилу из списка правил, расположив их в определенном порядке.

► *Чтобы назначить правилам доступа к веб-ресурсам приоритет, выполните следующие действия:*

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Защита** → **Контроль безопасности** → **Веб-Контроль**.
3. В блоке **Настройки** нажмите на кнопку **Правила доступа к веб-ресурсам**.
4. В открывшемся окне выберите правило, приоритет которого вы хотите изменить.
5. С помощью кнопок **Вверх** и **Вниз** переместите правило на нужную позицию в списке правил доступа к веб-ресурсам.
6. Сохраните внесенные изменения.

Включение и выключение правила доступа к веб-ресурсам

► *Чтобы включить или выключить правило доступа к веб-ресурсам, выполните следующие действия:*

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Защита** → **Контроль безопасности** → **Веб-Контроль**.
3. В блоке **Настройки** нажмите на кнопку **Правила доступа к веб-ресурсам**.
4. В открывшемся окне выберите правило, которое вы хотите включить или выключить.
5. В графе **Состояние** выполните следующие действия:
    - Если вы хотите включить использование правила, выберите значение **Активно**.
    - Если вы хотите выключить использование правила, выберите значение **Не активно**.
6. Сохраните внесенные изменения.

Проверка работы правил доступа к веб-ресурсам

Чтобы оценить, насколько согласованы правила Веб-Контроля, вы можете проверить их работу. Для этого в рамках компонента Веб-Контроль предусмотрена функция "Диагностика правил".

► *Чтобы проверить работу правил доступа к веб-ресурсам, выполните следующие действия:*

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Защита** → **Контроль безопасности** → **Веб-Контроль**.
3. В блоке **Настройки** нажмите на ссылку **Диагностика правил**.

   Откроется окно **Диагностика правил**.
4. Установите флажок **Укажите адрес**, если вы хотите проверить работу правил, в соответствии с которыми Kaspersky Endpoint Security контролирует доступ к определенному веб-ресурсу. В поле ниже введите адрес веб-ресурса.
5. Задайте список пользователей и / или групп пользователей, если вы хотите проверить работу правил, в соответствии с которыми Kaspersky Endpoint Security контролирует доступ к веб-ресурсам для определенных пользователей и / или групп пользователей.
6. Установите флажок **Фильтровать содержание** и в раскрывающемся списке выберите нужный элемент (**По категориям содержания**, **По типам данных** или **По категориям содержания и типам данных**), если вы хотите проверить работу правил, в соответствии с которыми Kaspersky Endpoint Security контролирует доступ к веб-ресурсам определенных категорий содержания и / или категорий типа данных.
7. Установите флажок **Учитывать время попытки доступа**, если вы хотите проверить работу правил с учетом дня недели и времени совершения попытки доступа к веб-ресурсам, указанным в условиях диагностики правил. Далее укажите день недели и время.
8. Нажмите на кнопку **Проверить**.

В результате проверки выводится сообщение о действии Kaspersky Endpoint Security в соответствии с первым сработавшим правилом при попытке доступа к заданному веб-ресурсу (разрешение, запрет, предупреждение). Первым срабатывает правило, которое находится в списке правил Веб-Контроля выше других правил, удовлетворяющих условиям диагностики. Сообщение выводится справа от кнопки **Проверить**. В таблице ниже выводится список остальных сработавших правил с указанием действия, которое выполняет Kaspersky Endpoint Security. Правила выводятся в порядке убывания приоритета.

Экспорт и импорт списка адресов веб-ресурсов

Если в правиле доступа к веб-ресурсам вы сформировали список адресов веб-ресурсов, вы можете экспортировать его в файл формата TXT. В дальнейшем вы можете импортировать список из этого файла, чтобы при настройке правила не создавать список адресов веб-ресурсов вручную. Возможность экспорта и импорта списка адресов веб-ресурсов может понадобиться, например, если вы создаете правила со сходными параметрами.

► *Чтобы импортировать или экспортировать список адресов веб-ресурсов в файл, выполните следующие действия:*

1. В нижней части главного окна программы нажмите на кнопку .
2. В окне параметров программы выберите раздел **Защита** → **Контроль безопасности** → **Веб-Контроль**.
3. В блоке **Настройки** нажмите на кнопку **Правила доступа к веб-ресурсам**.
4. Выберите правило, список адресов веб-ресурсов которого вы хотите экспортировать или импортировать.
5. Для экспорта списка доверенных веб-ресурсов в блоке **Адреса** выполните следующие действия:
   a. Выберите адреса, которые вы хотите экспортировать.

      Если вы не выбрали ни одного адреса, Kaspersky Endpoint Security экспортирует все адреса.

   b. Нажмите на кнопку **Экспорт**.
   c. В открывшемся окне введите имя файла формата TXT, в который вы хотите экспортировать список адресов веб-ресурсов, а также выберите папку, в которой вы хотите сохранить этот файл.
   d. Нажмите на кнопку **Сохранить**.

      Kaspersky Endpoint Security экспортирует список адресов веб-ресурсов в TXT-файл.
6. Для импорта списка веб-ресурсов в блоке **Адреса** выполните следующие действия:
   a. Нажмите на кнопку **Импорт**.

      В открывшемся окне выберите TXT-файл, из которого вы хотите импортировать список веб-ресурсов.

   b. Нажмите на кнопку **Открыть**.

      Если на компьютере уже есть список адресов, Kaspersky Endpoint Security предложит удалить действующий список или добавить в него новые записи из TXT-файла.
7. Сохраните внесенные изменения.

Мониторинг активности пользователей в интернете

Kaspersky Endpoint Security позволяет записывать данные о посещении пользователями всех веб-сайтов, в том числе и разрешенных. Таким образом, вы можете получить полную историю просмотров в браузере. Kaspersky Endpoint Security отправляет события активности пользователя в Kaspersky Security Center, локальный журнал Kaspersky Endpoint Security (см. раздел "Работа с отчетами" на стр. 210), журнал событий Windows. Для получения событий в Kaspersky Security Center нужно настроить параметры событий в политике в Консоли администрирования или Web Console. Также вы можете настроить отправку событий Веб-Контроля по электронной почте и отображение уведомлений на экране компьютера пользователя.

Kaspersky Endpoint Security создает следующие события активности пользователя в интернете:

- блокировка веб-сайта (статус *Критические события*);
- посещение нерекомендованного веб-сайта (статус *Предупреждения*);
- посещение разрешенного веб-сайта (статус *Информационные сообщения*).

Перед включением мониторинга активности пользователей в интернете необходимо выполнить следующие действия:

- Внедрите в трафик скрипт взаимодействия с веб-страницами (см. инструкцию ниже). Скрипт позволяет регистрировать события работы Веб-Контроля.
- Для контроля HTTPS-трафика нужно включить проверку защищенных соединений (см. раздел "Настройка параметров проверки защищенных соединений" на стр. 140).

► *Чтобы внедрить в трафик скрипт взаимодействия с веб-страницами, выполните следующие действия:*

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Настройки сети**.
3. В блоке **Обработка трафика** установите флажок **Внедрять в трафик скрипт взаимодействия**.
4. Сохраните внесенные изменения.

В результате Kaspersky Endpoint Security внедрит в трафик скрипт взаимодействия с веб-страницами. Скрипт позволяет регистрировать события работы Веб-Контроля для журнала событий программы, журнала событий ОС, отчетов (см. раздел "Работа с отчетами" на стр. 210).

► *Чтобы настроить запись событий Веб-Контроля на компьютере пользователя, выполните следующие действия:*

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Интерфейс**.
3. В блоке **Уведомления** нажмите на кнопку **Правила уведомлений**.
4. В открывшемся окне выберите раздел **Веб-Контроль**.

   Откроется таблица событий Веб-Контроля и способов уведомлений.
5. Настройте для каждого события способ уведомления: **Сохранять в локальном журнале** и **Сохранять в журнале событий Windows**.

   Для записи событий посещения разрешенных веб-сайтов нужно дополнительно настроить Веб-Контроль (см. инструкцию ниже).

   Также в таблице событий вы можете включить уведомление на экране и уведомление по электронной почте. Для отправки уведомлений по почте нужно настроить параметры SMTP-сервера. Подробнее об отправке уведомлений по почте см. в *справке Kaspersky Security Center* https://help.kaspersky.com/KSC/12/ru-RU/.
6. Сохраните внесенные изменения.

В результате Kaspersky Endpoint Security начинает записывать события активности пользователя в интернете.

Веб-Контроль отправляет события активности пользователя в Kaspersky Security Center следующим образом:

- Если вы используете Kaspersky Security Center, Веб-Контроль отправляет события по всем объектам, из которых состоит веб-страница. Поэтому при блокировании одной веб-страницы может быть создано несколько событий. Например, при блокировании веб-страницы http://www.example.com Kaspersky Endpoint Security может отправить события по следующим объектам: http://www.example.com,

http://www.example.com/icon.ico, http://www.example.com/file.js и так далее.

- Если вы используете Kaspersky Security Center Cloud Console, Веб-Контроль группирует события и отправляет только протокол и домен веб-сайта. Например, если пользователь посетил нерекомендованные веб-страницы http://www.example.com/main, http://www.example.com/contact, http://www.example.com/gallery, то Kaspersky Endpoint Security отправит только одно событие с объектом http://www.example.com.

► *Чтобы включить запись событий посещения разрешенных веб-сайтов, выполните следующие действия:*

1. В нижней части главного окна программы нажмите на кнопку .
2. В окне параметров программы выберите раздел **Защита** → **Контроль безопасности** → **Веб-Контроль**.
3. В блоке **Дополнительно** нажмите на кнопку **Дополнительные настройки**.
4. В открывшемся окне установите флажок **Записывать данные о посещении разрешенных страниц в журнал**.
5. Сохраните внесенные изменения.

В результате вам будет доступна полная история просмотров в браузере.

Изменение шаблонов сообщений Веб-Контроля

В зависимости от действия, заданного в свойствах правил Веб-Контроля, при попытке пользователей получить доступ к веб-ресурсам Kaspersky Endpoint Security выводит сообщение (подменяет ответ HTTP-сервера HTML-страницей с сообщением) одного из следующих типов:

- Сообщение-предупреждение. Такое сообщение предупреждает пользователя о том, что посещение веб-ресурса не рекомендуется и / или не соответствует корпоративной политике безопасности. Kaspersky Endpoint Security выводит сообщение-предупреждение, если в параметрах правила, описывающего этот веб-ресурс, в раскрывающемся списке **Действие** выбран элемент **Предупреждать**.

  Если, по мнению пользователя, предупреждение ошибочно, по ссылке из предупреждения пользователь может отправить уже сформированное сообщение администратору локальной сети организации.

- Сообщение о блокировке веб-ресурса. Kaspersky Endpoint Security выводит сообщение о блокировке веб-ресурса, если в параметрах правила, которое описывает этот веб-ресурс, в раскрывающемся списке **Действие** выбран элемент **Запрещать**.

  Если блокировка доступа к веб-ресурсу, по мнению пользователя, была ошибочна, по ссылке из сообщения о блокировке веб-ресурса пользователь может отправить уже сформированное сообщение администратору локальной сети организации.

Для сообщения-предупреждения, сообщения о блокировке доступа к веб-ресурсу и сообщения для отправки администратору локальной сети организации предусмотрены шаблоны. Вы можете изменять их содержание.

► *Чтобы изменить шаблон сообщений Веб-Контроля, выполните следующие действия:*

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Защита** → **Контроль безопасности** → **Веб-Контроль**.
3. В блоке **Шаблоны** настройте шаблоны сообщений Веб-Контроля:
   - **Предупреждения**. Поле ввода содержит шаблон сообщения, которое появляется при срабатывании правила, предупреждающего о попытке доступа к нерекомендованному веб-ресурсу.
   - **Блокировка**. Поле ввода содержит шаблон сообщения, которое появляется при срабатывании правила, блокирующего доступ к веб-ресурсу.
   - **Сообщение администратору**. Поле ввода содержит шаблон сообщения для отправки администратору локальной сети организации в случае, если блокировка доступа к веб-ресурсу, по мнению пользователя, произошла ошибочно.
4. Сохраните внесенные изменения.

См. также

Изменение шаблонов сообщений Контроля программ 157
Изменение шаблонов сообщений Адаптивного контроля аномалий 166

Правила формирования масок адресов веб-ресурсов

Использование *маски адреса веб-ресурса* (далее также "маски адреса") может быть удобно в случаях, когда в процессе создания правила доступа к веб-ресурсам требуется ввести множество схожих адресов веб-ресурсов. Одна грамотно сформированная маска адреса может заменить множество адресов веб-ресурсов.

При формировании маски адреса следует использовать следующие правила:

1. Символ `*` заменяет любую последовательность из нуля или более символов.

   Например, при вводе маски адреса `*abc*` правило доступа к веб-ресурсам применяется ко всем адресам, содержащим последовательность `abc`. Пример: `http://www.example.com/page_0-9abcdef.html`.

2. Последовательность символов `*.` позволяет выбрать все домены адреса – *маска домена*. Маска домена `*.` трактуется как любое имя домена, имя поддомена или пустая строка.

   Пример: под действие маски `*.example.com` попадают следующие адреса:

   - `http://pictures.example.com` – маска домена `*.` применена для `pictures.`.
   - `http://user.pictures.example.com` – маска домена `*.` применена для `pictures.` и `user.`.
   - `http://example.com` – маска домена `*.` трактуется как пустая строка.

3. Последовательность символов `www.` в начале маски адреса трактуется как последовательность `*.`.

   Пример: маска адреса `www.example.com` трактуется как `*.example.com`. Под действие маски попадают адреса `www2.example.com` и `www.pictures.example.com`.

4. Если маска адреса начинается не с символа `*`, то содержание маски адреса эквивалентно тому же содержанию с префиксом `*.`.

5. Если маска адреса заканчивается символом, отличным от `/` или `*`, то содержание маски адреса эквивалентно тому же содержанию с постфиксом `/*`.

   Пример: под действие маски адреса `http://www.example.com` попадают адреса вида `http://www.example.com/abc`, где `a`, `b`, `c` – любые символы.

6. Если маска адреса заканчивается символом `/`, то содержание маски адреса эквивалентно тому же содержанию с постфиксом `/*`.

7. Последовательность символов `/*` в конце маски адреса трактуется как `/*` или пустая строка.

8. Проверка адресов веб-ресурсов по маске адреса осуществляется с учетом схемы (http или https):

   - Если сетевой протокол в маске адреса отсутствует, то под действие маски адреса попадает адрес с любым сетевым протоколом.

     Пример: под действие маски адреса `example.com` попадают адреса http://example.com и https://example.com.

   - Если сетевой протокол в маске адреса присутствует, то под действие маски адреса попадают только адреса с таким же сетевым протоколом, как у маски адреса.

     Пример: под действие маски адреса `http://*.example.com` попадает адрес `http://www.example.com` и не попадает адрес `https://www.example.com`.

9. Маска адреса, заключенная в двойные кавычки, трактуется без учета каких-либо дополнительных подстановок, за исключением символа `*`, если он изначально включен в состав маски адреса. Для масок адреса, заключенных в двойные кавычки, не выполняются правила 5 и 7 (см. примеры 14 – 18 в таблице ниже).

10. При сравнении с маской адреса веб-ресурса не учитываются имя пользователя и пароль, порт соединения и регистр символов.

Таблица 8. Примеры применения правил формирования масок адресов

№	Маска адреса	Проверяемый адрес веб-ресурса	Удовлетворяет ли проверяемый адрес маске адреса	Комментарий
1	*.example.com	http://www.123example.com	Нет	См. правило 1.
2	*.example.com	http://www.123.example.com	Да	См. правило 2.
3	*example.com	http://www.123example.com	Да	См. правило 1.
4	*example.com	http://www.123.example.com	Да	См. правило 1.
5	http://www.*.example.com	http://www.123example.com	Нет	См. правило 1.
6	www.example.com	http://www.example.com	Да	См. правила 3, 2, 1.

№	Маска адреса	Проверяемый адрес веб-ресурса	Удовлетворяет ли проверяемый адрес маске адреса	Комментарий
7	www.example.com	https://www.example.com	Да	См. правила 3, 2, 1.
8	http://www.*.example.com	http://123.example.com	Да	См. правила 3, 4, 1.
9	www.example.com	http://www.example.com/abc	Да	См. правила 3, 5, 1.
10	example.com	http://www.example.com	Да	См. правила 3, 1.
11	http://example.com/	http://example.com/abc	Да	См. правила 6.
12	http://example.com/*	http://example.com	Да	См. правило 7.
13	http://example.com	https://example.com	Нет	См. правило 8.
14	"example.com"	http://www.example.com	Нет	См. правило 9.
15	"http://www.example.com"	http://www.example.com/abc	Нет	См. правило 9.
16	"*.example.com"	http://www.example.com	Да	См. правила 1, 9.
17	"http://www.example.com/*"	http://www.example.com/abc	Да	См. правила 1, 9.
18	"www.example.com"	http://www.example.com; https://www.example.com	Да	См. правила 9, 8.
19	www.example.com/abc/123	http://www.example.com/abc	Нет	Маска адреса содержит больше информации, чем адрес веб-ресурса.

kaspersky

Контроль сетевых портов

Во время работы Kaspersky Endpoint Security компоненты Веб-Контроль (на стр. 168), Защита от почтовых угроз (на стр. 124), Защита от веб-угроз (на стр. 117) контролируют потоки данных, передаваемые по определенным протоколам и проходящие через определенные открытые TCP- и UDP-порты компьютера пользователя. Например, компонент Защита от почтовых угроз анализирует информацию, передаваемую по SMTP-протоколу, а компонент Защита от веб-угроз анализирует информацию, передаваемую по протоколам HTTP и FTP.

Kaspersky Endpoint Security подразделяет TCP- и UDP-порты компьютера пользователя на несколько групп в соответствии с вероятностью их взлома. Сетевые порты, отведенные для уязвимых служб, рекомендуется контролировать более тщательно, так как эти сетевые порты с большей вероятностью могут являться целью сетевой атаки. Если вы используете нестандартные службы, которым отведены нестандартные сетевые порты, эти сетевые порты также могут являться целью для атакующего компьютера. Вы можете задать список сетевых портов и список программ, запрашивающих сетевой доступ, на которые компоненты Защита от почтовых угроз и Защита от веб-угроз должны обращать особое внимание во время слежения за сетевым трафиком.

В этом разделе

Включение контроля всех сетевых портов

► *Чтобы включить контроль всех сетевых портов, выполните следующие действия:*

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Настройки сети**.
3. В блоке **Контролируемые порты** выберите вариант **Контролировать все сетевые порты**.
4. Сохраните внесенные изменения.

Формирование списка контролируемых сетевых портов

► *Чтобы сформировать список контролируемых сетевых портов, выполните следующие действия:*

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Настройки сети**.
3. В блоке **Контролируемые порты** выберите вариант **Контролировать только выбранные сетевые порты**.

4. Нажмите на кнопку **Выбрать**.

   Откроется список сетевых портов, которые обычно используются для передачи электронной почты и сетевого трафика. Этот список сетевых портов включен в поставку Kaspersky Endpoint Security.

5. Используйте переключатель в графе **Статус**, чтобы включить или выключить контроль сетевых портов.
6. Если сетевой порт отсутствует в списке сетевых портов, добавьте его следующим образом:
   a. Нажмите на кнопку **Добавить**.
   b. В открывшемся окне введите номер сетевого порта и короткое описание.
   c. Установите статус контроля сетевого порта **Активно** или **Неактивно**.
7. Сохраните внесенные изменения.

При работе протокола FTP в пассивном режиме соединение может устанавливаться через случайный сетевой порт, который не добавлен в список контролируемых сетевых портов. Чтобы защищать такие соединения, включите контроль всех сетевых портов (см. раздел "Включение контроля всех сетевых портов" на стр. 182) или настройте контроль сетевых портов для программ, с помощью которых устанавливается FTP-соединение (см. раздел "Формирование списка программ, для которых контролируются все сетевые порты" на стр. 183).

Формирование списка программ, для которых контролируются все сетевые порты

Вы можете сформировать список программ, для которых Kaspersky Endpoint Security контролирует все сетевые порты.

В список программ, для которых Kaspersky Endpoint Security контролирует все сетевые порты, рекомендуется включить программы, которые принимают или передают данные по протоколу FTP.

► *Чтобы сформировать список программ, для которых контролируются все сетевые порты, выполните следующие действия:*

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Настройки сети**.
3. В блоке **Контролируемые порты** выберите вариант **Контролировать только выбранные сетевые порты**.
4. Установите флажок **Контролировать все порты для программ из списка, рекомендованного "Лабораторией Касперского"**.

Если установлен этот флажок, Kaspersky Endpoint Security контролирует все порты для следующих программ:

- Adobe Reader.
- Apple Application Support.
- Google Chrome.
- Microsoft Edge.
- Mozilla Firefox.
- Internet Explorer.
- Java.
- mIRC.
- Opera.
- Pidgin.
- Safari.
- Агент Mail.ru.

5. Яндекс.Браузер.Установите флажок **Контролировать все порты для указанных программ**.
6. Нажмите на кнопку **Выбрать**.

   Откроется список программ, сетевые порты которых контролирует Kaspersky Endpoint Security.
7. Используйте переключатель в графе **Статус**, чтобы включить или выключить контроль сетевых портов.
8. Если программа отсутствует в списке программ, добавьте ее следующим образом:
   a. Нажмите на кнопку **Добавить**.
   b. В открывшемся окне укажите путь к исполняемому файлу программы и короткое описание.
   c. Установите статус контроля сетевых портов **Активно** или **Неактивно**.
9. Сохраните внесенные изменения.

kaspersky

Расширения защиты

В этом разделе

kaspersky

Managed Detection and Response

В Kaspersky Endpoint Security версии 11.6.0 добавлен компонент Managed Detection and Response. Компонент обеспечивает взаимодействие с решением Kaspersky Managed Detection and Response. *Kaspersky Managed Detection and Response (MDR)* обеспечивает непрерывный поиск, обнаружение и устранение угроз, направленных на вашу организацию. Подробную информацию о работе решения *см. в справке Kaspersky Managed Detection and Response* https://support.kaspersky.com/MDR/ru-RU/.

При взаимодействии с Kaspersky Managed Detection and Response программа позволяет выполнять следующие функции:

- Активация Managed Detection and Response с помощью конфигурационного файла BLOB.
- Выполнение команд от Kaspersky Managed Detection and Response.
- Отправка данных телеметрии для обнаружения угроз в Kaspersky Managed Detection and Response.

Интеграция с Kaspersky Managed Detection and Responce

Интеграция с Kaspersky Managed Detection and Response состоит из следующих этапов:

Настройка прокси-сервера Kaspersky Security Network

Прокси-сервер Kaspersky Security Network обеспечивает обмен данными между компьютерами и инфраструктурой облачных служб Kaspersky Security Network через Сервер администрирования, а не напрямую.

Загрузите конфигурационный файл Kaspersky Security Network в свойствах Сервера администрирования. Конфигурационный файл Kaspersky Security Network находится в ZIP-архиве конфигурационного файла MDR. Вы можете получить ZIP-архив в Консоли Kaspersky Managed Detection and Response. Подробнее о настройке прокси-сервера Kaspersky Security Network см. в *справке Kaspersky Security Center* https://support.kaspersky.com/KSC/12/ru-RU/89312.htm. Также вы можете загрузить конфигурационный файл Kaspersky Security Network на компьютер из командной строки (см. инструкцию ниже).

Как настроить прокси-сервер Kaspersky Security Network из командной строки

1. Запустите интерпретатор командной строки cmd от имени администратора.
2. Перейдите в папку, в которой расположен дистрибутив Kaspersky Endpoint Security.
3. Выполните команду:

   `avp.com KSN /private <имя файла>`

   где `<имя файла>` – имя конфигурационного файла с параметрами прокси-сервера KSN (формат файла PKCS7 или PEM).

Пример:

```
avp.com KSN /private C:\kpsn_config.pkcs7
```

В результате Kaspersky Endpoint Security будет использовать Локальный KSN для определения репутации файлов, программ и веб-сайтов. В параметрах политики в разделе **Kaspersky Security Network** будет указан статус работы *Сеть KSN: Локальный KSN*.

Для работы Managed Detection and Response необходимо включить расширенный режим KSN (см. раздел "Включение и выключение использования Kaspersky Security Network" на стр. 81).

Активация Managed Detection and Response

Загрузите конфигурационный файл BLOB в политике Kaspersky Endpoint Security (см. инструкцию ниже). BLOB-файл содержит идентификатор клиента и информацию о лицензии Kaspersky Managed Detection and Response. BLOB-файл находится в ZIP-архиве конфигурационного файла MDR. Вы можете получить ZIP-архив в Консоли Kaspersky Managed Detection and Response. Подробную информацию о BLOB-файле *см. в справке Kaspersky Managed Detection and Response* https://support.kaspersky.com/MDR/ru-RU/.

Как активировать Managed Detection and Response из командной строки:

1. Запустите интерпретатор командной строки cmd от имени администратора.
2. Перейдите в папку, в которой расположен дистрибутив Kaspersky Endpoint Security.
3. Выполните команду:
   - Если настройка параметров программы не защищена паролем (см. раздел "Защита паролем" на стр. 189):

     ```
     avp.com MDRLICENSE /ADD <имя файла>
     ```

     где `<имя файла>` – имя конфигурационного файла BLOB для активации Managed Detection and Response (формат файла P7).
   - Если настройка параметров программы защищена паролем (см. раздел "Защита паролем" на стр. 189):

     ```
     avp.com MDRLICENSE /ADD <имя файла> /login=<имя пользователя>
     /password=<пароль>
     ```

В результате Kaspersky Endpoint Security проверит BLOB-файл. Проверка BLOB-файла включает в себя проверку цифровой подписи и срока действия лицензии. Если BLOB-файл прошел проверку, Kaspersky Endpoint Security загрузит файл и отправит файл на компьютер при следующей синхронизации с Kaspersky Security Center. Проверьте статус работы компонента с помощью отчета *Отчет о статусе компонентов программы*. Также вы можете посмотреть статус работы компонента в локальном интерфейсе Kaspersky Endpoint Security в отчетах. В список компонентов Kaspersky Endpoint Security будет добавлен компонент **Managed Detection and Response**.

Компонент Managed Detection and Response в Kaspersky Endpoint Security и Kaspersky Endpoint Agent

Программа Kaspersky Endpoint Security версии 11 или выше поддерживает взаимодействие с решением MDR.

Если вы используете Kaspersky Endpoint Security 11 – 11.5.0, для интеграции с решением MDR нужно обновить базы до актуальной версии. Программа Kaspersky Endpoint Security этих версий только отправляет данные телеметрии для обнаружения угроз в Kaspersky Managed Detection and Response.

Если вы используете Kaspersky Endpoint Security 11.6.0 или выше, поддержка взаимодействия с решением MDR доступна сразу после установки.

Если для работы с решением MDR вы использовали Kaspersky Endpoint Agent, далее установили Kaspersky Endpoint Security 11.6.0 или обновили антивирусные базы, решение MDR прекращает работу с Kaspersky Endpoint Agent и продолжает работу с Kaspersky Endpoint Security. Переключение между Kaspersky Endpoint Agent и Kaspersky Endpoint Security имеет следующие особенности:

- переключение выполняется в тихом режиме;
- в Kaspersky Endpoint Agent доступна настройка параметров взаимодействия с решением MDR, но эти параметры не применяются на устройстве;
- при недоступности Kaspersky Endpoint Security (например, вы удалили программу), решение MDR может возобновить работу с Kaspersky Endpoint Agent, если перезапустить службу Kaspersky Endpoint Agent;
- компонент Managed Detection and Response в параметрах Kaspersky Endpoint Agent на устройстве остается в статусе *Запущен*, т.к. Kaspersky Endpoint Agent продолжает поддерживать связь с решением MDR (например, чтобы возобновить работу с решением при необходимости).

Kaspersky Endpoint Agent

Kaspersky Endpoint Agent обеспечивает взаимодействие программы с другими решениями "Лаборатории Касперского" для обнаружения сложных угроз (например, Kaspersky Sandbox). Решения "Лаборатории Касперского", которые поддерживает Kaspersky Endpoint Agent, зависят от версии Kaspersky Endpoint Agent.

Полную информацию о Kaspersky Endpoint Agent для Windows в составе программного решения, которое вы используете, а также полную информацию о самом решении смотрите в справке соответствующего решения:

- в *Справке Kaspersky Anti Targeted Attack Platform*;
- в *Справке Kaspersky Sandbox*;
- в *Справке Kaspersky Endpoint Detection and Response Optimum*;
- в *Справке Kaspersky Managed Detection and Response*.

Kaspersky Endpoint Agent входит в комплект поставки Kaspersky Endpoint Security. Вы можете установить Kaspersky Endpoint Agent при установке Kaspersky Endpoint Security. Для этого вам нужно выбрать компонент Endpoint Agent при установке программы (например, в инсталляционном пакете). После установки программы с компонентом Endpoint Agent в список установленных программ будут добавлены Kaspersky Endpoint Security и Kaspersky Endpoint Agent. После удаления Kaspersky Endpoint Security, программа Kaspersky Endpoint Agent также будет удалена автоматически.

kaspersky

Защита паролем

Для версии программы Kaspersky Endpoint Security для Windows 11.1.0 и выше порядок работы Защиты паролем изменился. В Kaspersky Endpoint Security для Windows 11.1.0 вы можете ограничить доступ к программе отдельным пользователям и не использовать одну учетную запись. При обновлении с предыдущих версий программы, если Защита паролем включена, Kaspersky Endpoint Security сохраняет ранее заданный пароль. Для первого изменения параметров Защиты паролем используйте имя пользователя KLAdmin и ранее заданный пароль.

Компьютер могут использовать несколько пользователей с разным уровнем компьютерной грамотности. Неограниченный доступ пользователей к Kaspersky Endpoint Security и его параметрам может привести к снижению уровня безопасности компьютера в целом. Защита паролем позволяет ограничить доступ пользователей к Kaspersky Endpoint Security в соответствии с предоставленными разрешениями (например, разрешение на завершение работы программы).

Если пользователь, который запустил сессию Windows, (*сессионный пользователь*) имеет разрешение на выполнение действия, Kaspersky Endpoint Security не запрашивает имя пользователя и пароль или временный пароль. Пользователь получает доступ к Kaspersky Endpoint Security в соответствии с предоставленными разрешениями.

Если у сессионного пользователя отсутствует разрешение на выполнение действия, пользователь может получить доступ к программе следующими способами:

- Ввод имени пользователя и пароля.

  Этот способ удобен для повседневной работы. Для выполнения действия, защищенного паролем, требуется ввести данные доменной учетной записи пользователя с необходимым разрешением. При этом компьютер должен быть в домене. Если компьютер не в домене, вы можете использовать учетную запись KLAdmin.

- Ввод временного пароля.

  Этот способ удобен, если пользователь находится вне корпоративной сети и необходимо предоставить ему временное разрешение на выполнение запрещенного действия (например, завершить работу программы). По истечении срока действия временного пароля или истечении сессии программа возвращает параметры Kaspersky Endpoint Security в прежнее состояние.

При попытке пользователя выполнить действие, защищенное паролем, Kaspersky Endpoint Security предложит пользователю ввести имя пользователя и пароль или временный пароль (см. рис. ниже).

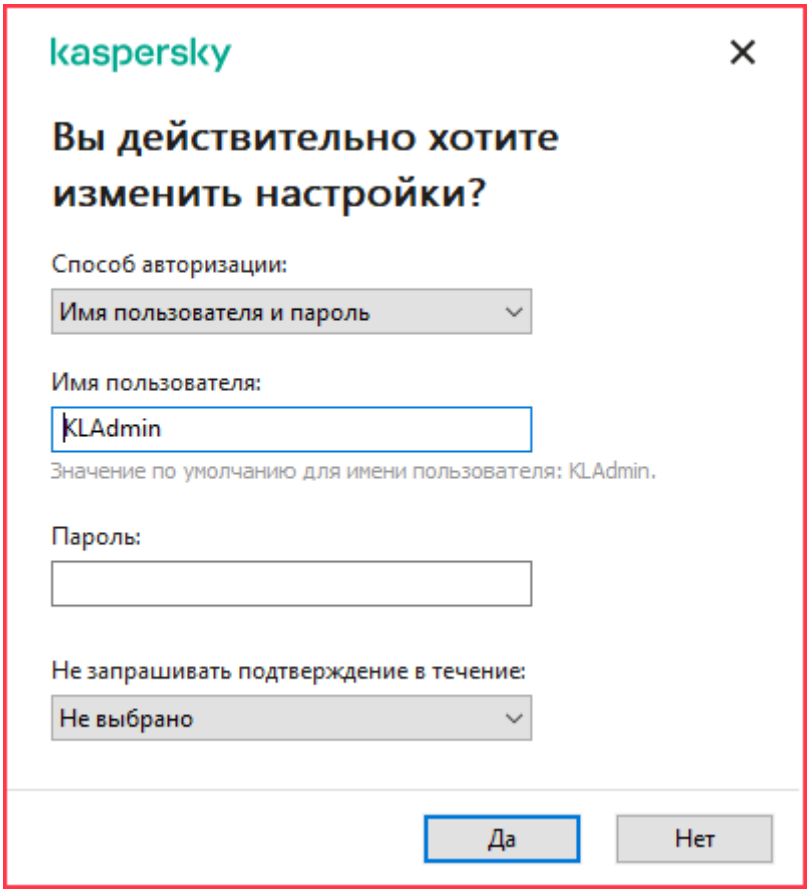


Рисунок 18. Запрос пароля для доступа к Kaspersky Endpoint Security

Имя пользователя и пароль

Для доступа к Kaspersky Endpoint Security необходимо ввести данные доменной учетной записи. Защита паролем поддерживает работу со следующими учетными записями:

- **KLAdmin**. Учетная запись администратора без ограничений доступа к Kaspersky Endpoint Security. Учетная запись KLAdmin имеет право на выполнение любого действия, защищенного паролем. Отменить разрешение для учетной записи KLAdmin невозможно. Kaspersky Endpoint Security требует задать пароль для учетной записи KLAdmin во время включения Защиты паролем.
- **Группа "Все"**. Стандартная группа Windows, которая включает в себя всех пользователей внутри корпоративной сети. Пользователи из группы "Все" могут получить доступ к программе в соответствии с предоставленными разрешениями.
- **Отдельные пользователи или группы**. Учетные записи пользователей, для которых вы можете настроить отдельные разрешения. Например, если для группы "Все" выполнение действия запрещено, то вы можете разрешить выполнение действия для отдельного пользователя или группы.
- **Сессионный пользователь**. Учетная запись пользователя, который запустил сессию Windows. Вы можете сменить сессионного пользователя во время ввода пароля (флажок **Запомнить пароль на текущую сессию**). В этом случае Kaspersky Endpoint Security назначает сессионным пользователем, учетные данные которого вы ввели, вместо пользователя, который запустил сессию Windows.

Временный пароль

Временный пароль позволяет предоставить временный доступ к Kaspersky Endpoint Security для отдельного компьютера вне корпоративной сети. Администратор создает временный пароль для отдельного компьютера в Kaspersky Security Center в свойствах компьютера пользователя. Администратор выбирает действия, на которые будет распространяться временный пароль, и срок действия временного пароля.

Алгоритм работы Защиты паролем

Kaspersky Endpoint Security принимает решение о выполнении действия, защищенного паролем, по следующему алгоритму (см. рис. ниже).

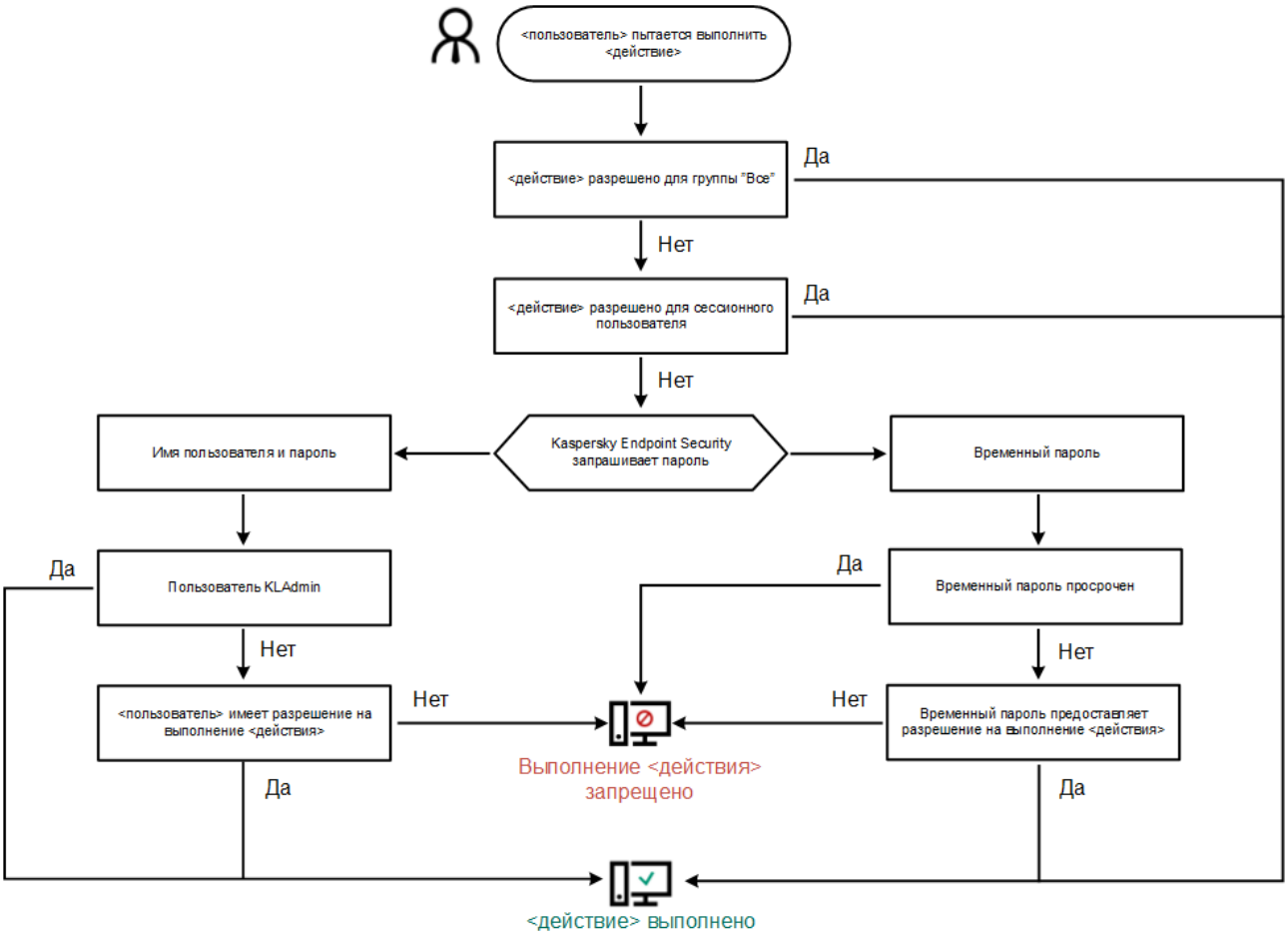


Рисунок 19. Алгоритм работы Защиты паролем

В этом разделе

kaspersky

Включение Защиты паролем

Защита паролем позволяет ограничить доступ пользователей к Kaspersky Endpoint Security в соответствии с предоставленными разрешениями (например, разрешение на завершение работы программы).

► *Чтобы включить Защиту паролем, выполните следующие действия:*

1. В нижней части главного окна программы нажмите на кнопку ⚙.

   В окне параметров программы выберите раздел **Интерфейс**.
2. Используйте переключатель **Защита паролем**, чтобы включить или выключить компонент.
3. Задайте пароль для учетной записи KLAdmin и подтвердите его.

   Учетная запись KLAdmin имеет право на выполнение любого действия, защищенного паролем.

   Если компьютер работает под управлением политики, администратор может сбросить пароль для учетной записи KLAdmin в свойствах политики. Если компьютер не подключен к Kaspersky Security Center и вы забыли пароль для учетной записи KLAdmin, восстановить пароль невозможно.
4. Настройте разрешения для всех пользователей внутри корпоративной сети:
   a. В таблице **Разрешения** откройте список разрешений для группы "Все" по кнопке **Изменить**.

      Группа "Все" – стандартная группа Windows, которая включает в себя всех пользователей внутри корпоративной сети.
   b. Установите флажки напротив тех действий, которые будут доступны пользователям без ввода пароля.

      Если флажок снят, пользователям запрещено выполнять это действие. Например, если флажок напротив разрешения **Завершение работы программы** снят, вы можете завершить работу программы только с помощью учетной записи KLAdmin, отдельной учетной записи с нужным разрешением (см. раздел "Предоставление разрешений для отдельных пользователей или групп" на стр. 193) или с помощью временного пароля (см. раздел "Использование временного пароля для предоставления разрешений" на стр. 194).

      Разрешения Защиты паролем имеют ряд особенностей (см. раздел "Особенности разрешений Защиты паролем" на стр. 195). Убедитесь, что для доступа к Kaspersky Endpoint Security выполнены все условия.
   c. Нажмите на кнопку **ОК**.
5. Сохраните внесенные изменения.

После включения Защиты паролем программа ограничит доступ пользователей к Kaspersky Endpoint Security в соответствии в разрешениями для группы "Все". Вы можете выполнить запрещенные для группы "Все" действия только с помощью учетной записи KLAdmin, отдельной учетной записи с нужными разрешениями (см. раздел "Предоставление разрешений для отдельных пользователей или групп" на стр. 193) или с помощью временного пароля (см. раздел "Использование временного пароля для предоставления разрешений" на стр. 194).

Вы можете выключить Защиту паролем только с помощью учетной записи KLAdmin. Выключить защиту паролем с помощью другой учетной записи или с помощью временного пароля невозможно.

Во время проверки пароля вы можете установить флажок **Запомнить пароль на текущую сессию**. В этом случае Kaspersky Endpoint Security не будет требовать ввода пароля при попытке пользователя выполнить другое разрешенное действие, защищенное паролем, в течение сессии.

Предоставление разрешений для отдельных пользователей или групп

Вы можете предоставить доступ к Kaspersky Endpoint Security для отдельных пользователей или групп. Например, если группе "Все" запрещено завершать работу программы, вы можете предоставить отдельному пользователю разрешение **Завершение работы программы**. В результате вы можете завершить работу программы только с помощью учетной записи этого пользователя или учетной записи KLAdmin.

Вы можете использовать данные учетной записи для доступа к программе, только если компьютер в домене. Если компьютер не в домене, вы можете использовать учетную запись KLAdmin или временный пароль (см. раздел "Использование временного пароля для предоставления разрешений" на стр. 194).

► *Чтобы предоставить разрешение для отдельных пользователей или групп, выполните следующие действия:*

1. В нижней части главного окна программы нажмите на кнопку ⚙.

   В окне параметров программы выберите раздел **Интерфейс**.
2. В таблице **Защита паролем** нажмите на кнопку **Добавить**.
3. В открывшемся окне нажмите на кнопку **Выбрать пользователя**.

   Откроется стандартное окно Windows для выбора пользователей или групп.
4. Выберите пользователя или группу в Active Directory и подтвердите свой выбор.
5. В списке **Разрешения** установите флажки напротив тех действий, которые будут доступны добавленному пользователю или группе без ввода пароля.

   Если флажок снят, пользователям запрещено выполнять это действие. Например, если флажок напротив разрешения **Завершение работы программы** снят, вы можете завершить работу программы только с помощью учетной записи KLAdmin, отдельной учетной записи с нужным разрешением (см. раздел "Предоставление разрешений для отдельных пользователей или групп" на стр. 193) или с помощью временного пароля (см. раздел "Использование временного пароля для предоставления разрешений" на стр. 194).

> Разрешения Защиты паролем имеют ряд особенностей (см. раздел "Особенности разрешений Защиты паролем" на стр. 195). Убедитесь, что для доступа к Kaspersky Endpoint Security выполнены все условия.

6. Сохраните внесенные изменения.

В результате, если для группы "Все" доступ к программе ограничен, пользователи получат доступ к Kaspersky Endpoint Security в соответствии с разрешениями для этих пользователей.

Использование временного пароля для предоставления разрешений

Временный пароль позволяет предоставить временный доступ к Kaspersky Endpoint Security для отдельного компьютера вне корпоративной сети. Это нужно, чтобы разрешить выполнение запрещенного действия без передачи пользователю учетных данных KLAdmin. Для использования временного пароля компьютер должен быть добавлен в Kaspersky Security Center.

► *Чтобы предоставить пользователю разрешение на выполнение запрещенного действия с помощью временного пароля, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева Консоли администрирования откройте папку с названием группы администрирования, в состав которой входят нужные клиентские компьютеры.
3. В рабочей области выберите закладку **Устройства**.
4. Откройте свойства компьютера двойным щелчком мыши.
5. В окне свойств компьютера выберите раздел **Программы**.
6. В списке установленных на компьютере программ "Лаборатории Касперского" выберите **Kaspersky Endpoint Security для Windows** и откройте свойства программы двойным щелчком мыши.
7. В окне параметров программы выберите раздел **Общие настройки** → **Интерфейс**.
8. В блоке **Защита паролем** нажмите на кнопку **Настройка**.

   Откроется окно **Защита паролем**.
9. В блоке **Временный пароль** нажмите на кнопку **Настройка**.

   Откроется окно **Создание временного пароля**.
10. В поле **Дата истечения** установите срок действия временного пароля.
11. В таблице **Область действия временного пароля** установите флажки напротив тех действий, которые будут доступны пользователю после ввода временного пароля.
12. Нажмите на кнопку **Создать**.

    Откроется окно с временным паролем (см. рис. ниже).

13. Скопируйте и передайте пользователю пароль.

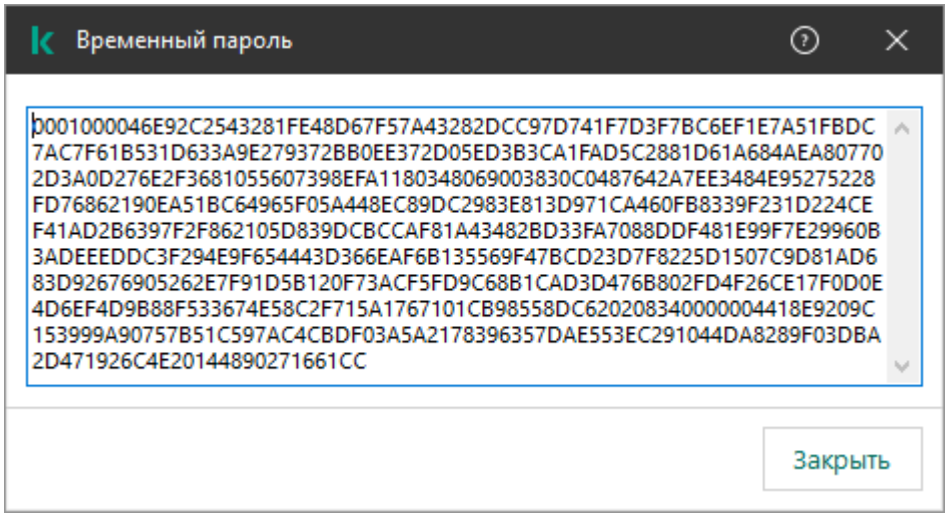


Рисунок 20. Временный пароль

Особенности разрешений Защиты паролем

Разрешения Защиты паролем имеют ряд особенностей и ограничений.

Настройка параметров программы

Если компьютер пользователя работает под управлением политики, убедитесь, что нужные параметры в политике доступны для изменения (атрибуты открыты).

Завершение работы программы

Особенностей и ограничений нет.

Выключение компонентов защиты

- Предоставить разрешение на выключение компонентов защиты для группы "Все" невозможно. Чтобы разрешить выключение компонентов защиты не только пользователю KLAdmin, но и другим пользователям, добавьте пользователя или группу (см. раздел "Предоставление разрешений для отдельных пользователей или групп" на стр. 193) с разрешением **Выключение компонентов защиты** в параметрах Защиты паролем.
- Если компьютер пользователя работает под управлением политики, убедитесь, что нужные параметры в политике доступны для изменения (атрибуты открыты).
- Для выключения компонентов защиты в параметрах программы пользователь должен иметь разрешение **Настройка параметров программы**.
- Для выключения компонентов защиты из контекстного меню (пункт **Приостановить защиту**) пользователь, кроме разрешения **Выключение компонентов защиты**, должен иметь разрешение **Выключение компонентов контроля**.

Выключение компонентов контроля

- Предоставить разрешение на выключение компонентов контроля для группы "Все" невозможно. Чтобы разрешить выключение компонентов защиты не только пользователю KLAdmin, но и другим пользователям, добавьте пользователя или группу (см. раздел "Предоставление разрешений для отдельных пользователей или групп" на стр. 193) с разрешением **Выключение компонентов контроля** в параметрах Защиты паролем.
- Если компьютер пользователя работает под управлением политики, убедитесь, что нужные параметры в политике доступны для изменения (атрибуты  открыты).
- Для выключения компонентов контроля в параметрах программы пользователь должен иметь разрешение **Настройка параметров программы**.
- Для выключения компонентов контроля из контекстного меню (пункт **Приостановить защиту**) пользователь, кроме разрешения **Выключение компонентов контроля**, должен обладать разрешением **Выключение компонентов защиты**.

Выключение политики Kaspersky Security Center

Предоставить разрешение на выключение политики Kaspersky Security Center для группы "Все" невозможно. Чтобы разрешить выключение политики не только пользователю KLAdmin, но и другим пользователям, добавьте пользователя или группу (см. раздел "Предоставление разрешений для отдельных пользователей или групп" на стр. 193) с разрешением **Выключение политики Kaspersky Security Center** в параметрах Защиты паролем.

Удаление ключа

Особенностей и ограничений нет.

Удаление / изменение / восстановление программы

Особенностей и ограничений нет.

Восстановление доступа к данным на зашифрованных устройствах

Вы можете восстановить доступ к данным на зашифрованных устройствах только с помощью учетной записи KLAdmin. Разрешить это действие другому пользователю невозможно.

Просмотр отчетов

Особенностей и ограничений нет.

Восстановление из резервного хранилища

Особенностей и ограничений нет.

kaspersky

Доверенная зона

Доверенная зона – это сформированный администратором системы список объектов и программ, которые Kaspersky Endpoint Security не контролирует в процессе работы.

Доверенную зону администратор системы формирует самостоятельно в зависимости от особенностей объектов, с которыми требуется работать, а также от программ, установленных на компьютере. Включение объектов и программ в доверенную зону может потребоваться, например, если Kaspersky Endpoint Security блокирует доступ к какому-либо объекту или программе, в то время как вы уверены, что этот объект или программа безвредны. Также администратор может разрешить пользователю формировать собственную локальную доверенную зону для отдельного компьютера. Таким образом, кроме общей доверенной зоны, сформированной в политике, пользователь может создавать собственные локальные списки исключений и доверенных программ.

В этом разделе

Создание исключения из проверки

Исключение из проверки – это совокупность условий, при выполнении которых Kaspersky Endpoint Security не проверяет объект на вирусы и другие программы, представляющие угрозу.

Исключения из проверки позволяют работать с легальными программами, которые могут быть использованы злоумышленниками для нанесения вреда компьютеру или данным пользователя. Такие программы сами по себе не имеют вредоносных функций, но эти программы могут быть использованы злоумышленниками. Подробную информацию о легальных программах, которые могут быть использованы злоумышленниками для нанесения вреда компьютеру или данным пользователя, вы можете получить на сайте Вирусной энциклопедии "Лаборатории Касперского" https://encyclopedia.kaspersky.ru/knowledge/classification/the-classification-tree/.

В результате работы Kaspersky Endpoint Security такие программы могут быть заблокированы. Чтобы избежать блокирования, для используемых программ вы можете настроить исключения из проверки. Для этого нужно добавить в доверенную зону название или маску названия по классификации Вирусной энциклопедии "Лаборатории Касперского". Например, вы часто используете в своей работе программу Radmin, предназначенную для удаленного управления компьютерами. Такая активность программы рассматривается Kaspersky Endpoint Security как подозрительная и может быть заблокирована. Чтобы исключить блокировку программы, нужно сформировать исключение из проверки, где указать название или маску названия по классификации Вирусной энциклопедии "Лаборатории Касперского".

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

Исключения из проверки могут использоваться в ходе работы следующих компонентов и задач программы, заданных администратором системы:

- Анализ поведения (на стр. 87).
- Защита от эксплойтов (на стр. 91).
- Предотвращение вторжений (на стр. 93).
- Защита от файловых угроз (на стр. 107).
- Защита от веб-угроз (на стр. 117).
- Защита от почтовых угроз (на стр. 124).
- Задачи проверки (на стр. 52).

Kaspersky Endpoint Security не проверяет объект, если при запуске одной из задач проверки в область проверки включен диск, на котором находится объект, или папка, в которой находится объект. Однако при запуске задачи выборочной проверки именно для этого объекта исключение из проверки не применяется.

Как создать исключение из проверки в интерфейсе программы:

1. В нижней части главного окна программы нажмите на кнопку .
2. В окне параметров программы выберите раздел **Угрозы и исключения**.
3. В блоке **Исключения** перейдите по ссылке **Настроить исключения**.
4. Нажмите на кнопку **Добавить**.
5. Если вы хотите исключить из проверки файл или папку, выберите файл или папку, нажав на кнопку **Обзор**.

   Также вы можете ввести путь вручную. Kaspersky Endpoint Security поддерживает символы * и ? для ввода маски:

   - Символ `*`, который заменяет любой набор символов, в том числе пустой, кроме символов `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\*\*.txt` будет включать все пути к файлам с расширением txt, расположенным в папках на диске (C:), но не в подпапках.
   - Два введенных подряд символа `*` заменяют любой набор символов, в том числе пустой, в имени файла или папки, включая символы `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\Folder\**\*.txt` будет включать все пути к файлам с расширением txt в папке `Folder` и вложенных папках. Маска должна включать хотя бы один уровень вложенности. Маска `C:\**\*.txt` не работает.
   - Символ `?`, который заменяет любой один символ, кроме символов `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `C:\Folder\???.txt` будет включать пути ко всем расположенным в папке `Folder` файлам с расширением txt и именем, состоящим из трех символов.

6. Если вы хотите исключить из проверки тип объектов, в поле **Объект** введите название типа объекта по классификации Энциклопедии "Касперского" https://encyclopedia.kaspersky.ru/knowledge/classification/the-classification-tree/ (например, `Email-Worm`, `Rootkit` или `RemoteAdmin`).

   Вы можете использовать маски с символами `?` (заменяет любой символ) и `*` (заменяет любые несколько символов). Например, если указана маска `Client*`, Kaspersky Endpoint Security исключает из проверки объекты типов `Client-IRC`, `Client-P2P` и `Client-SMTP`.

7. Если вы хотите исключить из проверки отдельный файл, в поле **Хеш файла** введите хеш файла.

   Если файл изменится, хеш файла тоже будет изменен. В результате измененный файл не будет добавлен в исключения.

8. В блоке **Компоненты защиты** выберите компоненты, на работу которых должно распространяться исключение из проверки.

9. Если необходимо, в поле **Комментарий** введите краткий комментарий к создаваемому исключению из проверки.

10. Установите статус для исключения **Активно**.

    Вы можете в любое время остановить работу исключения (см. раздел "Запуск и остановка работы исключения из проверки" на стр. 200) с помощью переключателя.

11. Сохраните внесенные изменения.

Примеры масок пути:

Пути к файлам, расположенным в любой из папок:

- Маска `*.exe` будет включать все пути к файлам с расширением exe.
- Маска `example*` будет включать все пути к файлам с именем EXAMPLE.

Пути к файлам, расположенным в указанной папке:

- маска `C:\dir\*.*` будет включать все пути к файлам в папке C:\dir\, но не в подпапках папки C:\dir\;
- маска `C:\dir\*` будет включать все пути к файлам в папке C:\dir\, но не в подпапках папки C:\dir\;
- маска `C:\dir\` будет включать все пути к файлам в папке C:\dir\, но не в подпапках папки C:\dir\;
- маска `C:\dir\*.exe` будет включать все пути к файлам с расширением exe в папке C:\dir\, но не в подпапках папки C:\dir\;
- маска `C:\dir\test` будет включать все пути к файлам с именем test в папке C:\dir\, но не в подпапках папки C:\dir\;
- маска `C:\dir\*\test` будет включать все пути к файлам с именем test в папке C:\dir\ и в подпапках папки C:\dir\.

Пути к файлам, расположенным во всех папках с указанным именем:

- маска `dir\*.*` будет включать все пути к файлам в папках с именем dir, но не в подпапках этих папок;
- маска `dir\*` будет включать все пути к файлам в папках с именем dir, но не в подпапках этих папок;
- маска `dir\` будет включать все пути к файлам в папках с именем dir, но не в подпапках этих папок;
- маска `dir\*.exe` будет включать все пути к файлам с расширением exe в папках с именем dir, но не в подпапках этих папок;
- маска `dir\test` будет включать все пути к файлам с именем test в папках с именем dir, но не в подпапках этих папок.

Запуск и остановка работы исключения из проверки

► *Чтобы запустить или остановить работу исключения из проверки, выполните следующие действия:*

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Угрозы и исключения**.
3. В блоке **Исключения** перейдите по ссылке **Настроить исключения**.
4. В списке исключений из проверки выберите нужное исключение.
5. Используйте переключатель рядом с объектом, чтобы включить или исключить объект из проверки.
6. Сохраните внесенные изменения.

kaspersky

Формирование списка доверенных программ

Список доверенных программ – это список программ, у которых Kaspersky Endpoint Security не контролирует файловую и сетевую активность (в том числе и вредоносную), а также обращения этих программ к системному реестру. По умолчанию Kaspersky Endpoint Security проверяет объекты, открываемые, запускаемые или сохраняемые любым программным процессом, а также контролирует активность всех программ и создаваемый ими сетевой трафик. Kaspersky Endpoint Security исключает из проверки программу, добавленную в список доверенных программ (см. раздел "Формирование списка доверенных программ" на стр. 201).

Например, если вы считаете объекты, используемые программой Microsoft Windows Блокнот, безопасными и не требующими проверки, то есть доверяете этой программе, вам следует добавить программу Microsoft Windows Блокнот в список доверенных программ, чтобы не проверять объекты, используемые этой программой.

Кроме того, некоторые действия, которые Kaspersky Endpoint Security классифицирует как подозрительные, могут быть безопасны в рамках функциональности ряда программ. Например, перехват текста, который вы вводите с клавиатуры, является штатным действием программ автоматического переключения раскладок клавиатуры (например, Punto Switcher). Чтобы учесть специфику таких программ и отключить контроль их активности, рекомендуется добавить их в список доверенных программ.

Исключение доверенных программ из проверки позволяет избежать проблемы совместимости Kaspersky Endpoint Security с другими программами (например, проблемы двойной проверки сетевого трафика стороннего компьютера Kaspersky Endpoint Security и другой антивирусной программой), а также увеличить производительность компьютера, что особенно важно при использовании серверных программ.

В то же время исполняемый файл и процесс доверенной программы по-прежнему проверяются на наличие в них вирусов и других программ, представляющих угрозу. Для полного исключения программы из проверки Kaspersky Endpoint Security следует пользоваться исключениями из проверки.

Как добавить программу в список доверенных в интерфейсе программы:

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Угрозы и исключения**.
3. В блоке **Исключения** перейдите по ссылке **Указать доверенные программы**.
4. В открывшемся окне нажмите на кнопку **Добавить**.
5. Выберите исполняемый файл доверенной программы.

   Также вы можете ввести путь вручную. Kaspersky Endpoint Security поддерживает переменные среды и символы * и ? для ввода маски.
6. В окне свойств доверенной программы настройте дополнительные параметры (см. таблицу ниже).
7. Вы можете в любое время исключить программу из доверенной зоны (см. раздел "Включение и выключение действия правил доверенной зоны на программу из списка доверенных программ" на стр. 203) с помощью переключателя.
8. Сохраните внесенные изменения.

Таблица 9. Параметры доверенной программы

Параметр	Описание
Не проверять открываемые файлы	Kaspersky Endpoint Security исключает из проверки все файлы, открываемые с помощью программы. Например, если вы используете программы резервного копирования файлов, функция позволит снизить потребление ресурсов компьютера Kaspersky Endpoint Security.
Не контролировать активность программы	Kaspersky Endpoint Security не контролирует файловую и сетевую активности программы в операционной системе. Контроль за активностью программы выполняют следующие компоненты: Анализ поведения (на стр. 87), Защита от эксплойтов (на стр. 91), Предотвращение вторжений (на стр. 93), Откат вредоносных действий (на стр. 105) и Сетевой экран.
Не наследовать ограничения родительского процесса (программы)	Kaspersky Endpoint Security не применяет ограничения к процессу, которые настроены для родительского процесса. Родительский процесс запускает программа, для которой настроены права программы (см. раздел "Работа с правами программ" на стр. 98) (Предотвращение вторжений) и сетевые правила программы (Сетевой экран).
Не контролировать активность дочерних программ	Kaspersky Endpoint Security не контролирует файловую и сетевую активности программ, которые запускает программа.
Разрешить взаимодействие с интерфейсом Kaspersky Endpoint Security	Самозащита Kaspersky Endpoint Security (на стр. 214) блокирует все попытки управления службами программы с удаленного компьютера. Если флажок установлен, то программе удаленного доступа к компьютеру разрешено управлять параметрами Kaspersky Endpoint Security через интерфейс Kaspersky Endpoint Security.
Не блокировать взаимодействие с компонентом AMSI-защита *(доступен только в консоли Kaspersky Security Center)*	Kaspersky Endpoint Security не контролирует запросы доверенной программы на проверку объектов компонентом AMSI-защита (см. раздел "AMSI-защита" на стр. 138).
Не проверять зашифрованный трафик / Не проверять весь трафик	Kaspersky Endpoint Security исключает из проверки сетевой трафик, инициируемый программой. Вы можете исключить из проверки весь трафик или только зашифрованный трафик. Также вы можете исключить из проверки отдельные IP-адреса или номера портов.
Комментарий	Если необходимо, вы можете ввести краткий комментарий к доверенной программе. Комментарий позволяет упростить поиск и сортировку доверенных программ.
Статус	Статус доверенной программы: • **Активно** – программа в доверенной зоне. • **Неактивно** – программа исключена из доверенной зоны.

kaspersky

Включение и выключение действия правил доверенной зоны на программу из списка доверенных программ

► *Чтобы включить или выключить действие правил доверенной зоны на программу из списка доверенных программ, выполните следующие действия:*

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Угрозы и исключения**.
3. В блоке **Исключения** перейдите по ссылке **Указать доверенные программы**.
4. В списке доверенных программ выберите нужную доверенную программу.
5. Используйте переключатель в графе **Статус**, чтобы включить или исключить доверенную программу из проверки.
6. Сохраните внесенные изменения.

Использование доверенного системного хранилища сертификатов

Использование системного хранилища сертификатов позволяет исключать из антивирусной проверки программы, подписанные доверенной цифровой подписью. Kaspersky Endpoint Security автоматически помещает такие программы в группу *Доверенные*.

► *Чтобы начать использовать доверенное системное хранилище сертификатов, выполните следующие действия:*

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Угрозы и исключения**.
3. В раскрывающемся списке **Доверенное системное хранилище сертификатов** выберите, какое системное хранилище Kaspersky Endpoint Security должен считать доверенным.
4. Сохраните внесенные изменения.

kaspersky

Работа с резервным хранилищем

Резервное хранилище – это хранилище резервных копий файлов, которые были изменены в процессе лечения или удалены. *Резервная копия* – копия файла, которая создается до лечения или удаления этого файла. Резервные копии файлов хранятся в специальном формате и не представляют опасности.

Резервные копии файлов хранятся в папке `C:\ProgramData\Kaspersky Lab\KES\QB`.

Полные права доступа к этой папке предоставлены пользователям группы "Администраторы". Ограниченные права доступа к этой папке предоставлены пользователю, под учетной записью которого выполнялась установка Kaspersky Endpoint Security.

В Kaspersky Endpoint Security отсутствует возможность настройки прав доступа пользователей к резервным копиям файлов.

Иногда при лечении файлов не удается сохранить их целостность. Если вылеченный файл содержал важную информацию, которая в результате лечения стала полностью или частично недоступна, вы можете попытаться восстановить файл из его резервной копии в папку исходного размещения файла.

Если Kaspersky Endpoint Security работает под управлением Kaspersky Security Center, то резервные копии файлов могут быть передана на Сервер администрирования Kaspersky Security Center. Подробнее о работе резервными копиями файлов в Kaspersky Security Center можно прочитать в Справочной системе Kaspersky Security Center.

В этом разделе

Настройка максимального срока хранения файлов в резервном хранилище

По умолчанию максимальный срок хранения копий файлов в резервном хранилище составляет 30 дней. По истечении максимального срока хранения Kaspersky Endpoint Security удаляет наиболее старые файлы из резервного хранилища.

► *Чтобы настроить максимальный срок хранения файлов в резервном хранилище, выполните следующие действия:*

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Отчеты и хранилище**.

3. В блоке **Резервное хранилище** установите флажок **Хранить объекты не более N дней**, если хотите ограничить срок хранения копий файлов в резервном хранилище. В поле справа от флажка **Хранить объекты не более N дней** укажите максимальный срок хранения копий файлов в резервном хранилище.
4. Сохраните внесенные изменения.

Настройка максимального размера резервного хранилища

Вы можете указать максимальный размер резервного хранилища. По умолчанию размер резервного хранилища не ограничен. После достижения максимального размера Kaspersky Endpoint Security автоматически удаляет наиболее старые файлы из резервного хранилища таким образом, чтобы не превышался его максимальный размер.

► *Чтобы настроить максимальный размер резервного хранилища, выполните следующие действия:*

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Отчеты и хранилище**.
3. В блоке **Резервное хранилище** установите флажок **Ограничить размер хранилища до N МБ**, если вы хотите ограничить размер резервного хранилища. Укажите максимальный размер резервного хранилища.
4. Сохраните внесенные изменения.

Восстановление файлов из резервного хранилища

Если в файле обнаружен вредоносный код, Kaspersky Endpoint Security блокирует файл, присваивает ему статус *Заражен*, помещает его копию в резервное хранилище и пытается провести лечение. Если файл удается вылечить, то статус резервной копии файла изменяется на *Вылечен*. Файл становится доступен в папке исходного размещения. Если файл не удается вылечить, то Kaspersky Endpoint Security удаляет его из папки исходного размещения. Вы можете восстановить файл из его резервной копии в папку исходного размещения.

Файлы со статусом *Будет вылечен при перезагрузке компьютера* восстановить невозможно. Перезагрузите компьютер и статус файла изменится на *Вылечен* или *Удален*. При этом вы можете восстановить файл из его резервной копии в папку исходного размещения.

В случае обнаружения вредоносного кода в файле, который является частью приложения Windows Store, Kaspersky Endpoint Security не помещает копию файла в резервное хранилище, а сразу удаляет его. При этом восстановить целостность приложения Windows Store вы можете средствами операционной системы Microsoft Windows 8 (подробную информацию о восстановлении приложения Windows Store читайте в *Справочной системе к Microsoft Windows 8*).

Набор резервных копий файлов представлен в виде таблицы. Для резервной копии файла отображается путь к папке исходного размещения этого файла. Путь к папке исходного размещения файла может содержать персональные данные.

Если в резервное хранилище помещено несколько расположенных в одной и той же папке файлов с одинаковыми именами и различным содержимым, то для восстановления доступен только тот файл, который был помещен в резервное хранилище последним.

► *Чтобы восстановить файлы из резервного хранилища, выполните следующие действия:*

1. В главном окне программы нажмите на кнопку **Больше функций** → **Хранилище**.

   Откроется окно **Резервное хранилище**.

2. В таблице в окне **Резервное хранилище** выберите один или несколько файлов резервного хранилища.

3. Нажмите на кнопку **Восстановить**.

Kaspersky Endpoint Security восстановит файлы из выбранных резервных копий в папки их исходного размещения.

Удаление резервных копий файлов из резервного хранилища

Kaspersky Endpoint Security удаляет резервные копии файлов с любым статусом из резервного хранилища автоматически по истечении времени, заданного в параметрах программы. Также вы можете самостоятельно удалить любую копию файла из резервного хранилища.

► *Чтобы удалить резервные копии файлов из резервного хранилища, выполните следующие действия:*

1. В главном окне программы нажмите на кнопку **Больше функций** → **Хранилище**.

   Откроется окно **Резервное хранилище**.

2. Выберите резервные копии файлов, которые вы хотите удалить из резервного хранилища, и нажмите на кнопку **Удалить**. Также вы можете удалить все файлы из резервного хранилища по кнопке **Удалить все**.

Kaspersky Endpoint Security удалит выбранные резервные копии файлов из резервного хранилища.

kaspersky

Служба уведомлений

В процессе работы Kaspersky Endpoint Security возникают различного рода события. Уведомления об этих событиях могут иметь информационный характер или нести важную информацию. Например, уведомление может информировать об успешно выполненном обновлении баз и модулей программы, а может фиксировать ошибку в работе некоторого компонента, которую вам требуется устранить.

Kaspersky Endpoint Security позволяет вносить информацию о событиях, возникающих в работе программы, в журнал событий Microsoft Windows и / или в журнал Kaspersky Endpoint Security.

Kaspersky Endpoint Security может доставлять уведомления следующими способами:

- с помощью всплывающих уведомлений в области уведомлений панели задач Microsoft Windows;
- по электронной почте.

Вы можете настроить способы доставки уведомлений. Способ доставки уведомлений устанавливается для каждого типа событий.

Работая с таблицей событий для настройки службы уведомлений, вы можете выполнять следующие действия:

- фильтровать события службы уведомлений по значениям граф или по условиям сложного фильтра;
- использовать функцию поиска событий службы уведомлений;
- сортировать события службы уведомлений;
- изменять порядок и набор граф, отображаемых в списке событий службы уведомлений.

В этом разделе

Настройка параметров журналов событий

► *Чтобы настроить параметры журналов событий, выполните следующие действия:*

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Интерфейс**.
3. В блоке **Уведомления** нажмите на кнопку **Настроить уведомления**.

   В левой части окна представлены компоненты и задачи Kaspersky Endpoint Security. В правой части окна отображается список событий, сформированный для выбранного компонента или выбранной задачи.

События могут содержать следующие данные пользователя:

- пути к файлам, проверяемым с помощью Kaspersky Endpoint Security;
- пути к ключам реестра, изменяемым в ходе работы Kaspersky Endpoint Security;
- имя пользователя Microsoft Windows;
- адреса веб-страниц, открываемых пользователем.

4. В левой части окна выберите компонент или задачу, для которой вы хотите настроить параметры журналов событий.
5. В графах **Сохранять в локальном отчете** и **Сохранять в журнале событий Windows** установите флажки напротив нужных событий.

   События, напротив которых установлен флажок в графе **Сохранять в локальном отчете**, отображаются в **Журналах приложений и служб** в разделе **Журнал событий Kaspersky**. События, напротив которых установлен флажок в графе **Сохранять в журнале событий Windows**, отображаются в **Журналах Windows** в разделе **Приложение**. Чтобы открыть журналы событий, выберите **Пуск** → **Панель управления** → **Администрирование** → **Просмотр событий**.
6. Сохраните внесенные изменения.

Настройка отображения и доставки уведомлений

► *Чтобы настроить отображение и доставку уведомлений, выполните следующие действия:*

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Интерфейс**.
3. В блоке **Уведомления** нажмите на кнопку **Настроить уведомления**.

   В левой части окна представлены компоненты и задачи Kaspersky Endpoint Security. В правой части окна отображается список событий, сформированный для выбранного компонента или выбранной задачи.

   События могут содержать следующие данные пользователя:

   - пути к файлам, проверяемым с помощью Kaspersky Endpoint Security;
   - пути к ключам реестра, изменяемым в ходе работы Kaspersky Endpoint Security;
   - имя пользователя Microsoft Windows;
   - адреса веб-страниц, открываемых пользователем.
4. В левой части окна выберите компонент или задачу, для которой вы хотите настроить доставку уведомлений.
5. В графе **Уведомлять на экране** установите флажки напротив нужных событий.

   Информация о выбранных событиях отображается на экране в виде всплывающих уведомлений в области уведомлений панели задач Microsoft Windows.
6. В графе **Уведомлять по почте** установите флажки напротив нужных событий.

   Информация о выбранных событиях доставляется по электронной почте, если заданы параметры доставки почтовых уведомлений.
7. Нажмите на кнопку **OK**.

8. Если вы включили уведомления по почте, настройте параметры доставки электронных сообщений:
   a. Нажмите на кнопку **Настройка почтовых уведомлений**.
   b. Установите флажок **Уведомлять о событиях**, чтобы включить доставку информации о событиях в работе Kaspersky Endpoint Security, отмеченных в графе **Уведомлять по почте**.
   c. Укажите параметры доставки почтовых уведомлений.
   d. Нажмите на кнопку **OK**.
9. Сохраните внесенные изменения.

Настройка отображения предупреждений о состоянии программы в области уведомлений

► *Чтобы настроить отображение предупреждений о состоянии программы в области уведомлений, выполните следующие действия:*

1. В нижней части главного окна программы нажмите на кнопку .
2. В окне параметров программы выберите раздел **Интерфейс**.
3. В блоке **Отображать состояние программы в области уведомлений** установите флажки напротив тех категорий событий, уведомления о которых вы хотите видеть в области уведомлений Microsoft Windows.
4. Сохраните внесенные изменения.

При возникновении событий, относящихся к выбранным категориям, значок программы (см. раздел "Значок программы в области уведомлений" на стр. 43) в области уведомлений будет меняться на или в зависимости от важности предупреждения.

kaspersky

Работа с отчетами

Информация о работе каждого компонента Kaspersky Endpoint Security, о событиях шифрования данных, о выполнении каждой задачи проверки, задачи обновления и задачи проверки целостности, а также о работе программы в целом сохраняется в отчетах.

Отчеты хранятся в папке `C:\ProgramData\Kaspersky Lab\KES\Report`.

Отчеты могут содержать следующие данные пользователя:

- пути к файлам, проверяемым с помощью Kaspersky Endpoint Security;
- пути к ключам реестра, изменяемым в ходе работы Kaspersky Endpoint Security;
- имя пользователя Microsoft Windows;
- адреса веб-страниц, открываемых пользователем.

Данные в отчете представлены в виде таблицы. Каждая строка таблицы содержит информацию об отдельном событии, атрибуты события находятся в графах таблицы. Некоторые графы являются составными и содержат вложенные графы с дополнительными атрибутами. Чтобы просмотреть дополнительные атрибуты, нажмите на кнопку  рядом с названием графы. События, зарегистрированные в работе разных компонентов или при выполнении разных задач, имеют разный набор атрибутов.

Доступны следующие отчеты:

- Отчет **Системный аудит**. Содержит информацию о событиях, возникающих в процессе взаимодействия пользователя с программой, а также в ходе работы программы в целом и не относящихся к каким-либо отдельным компонентам или задачам Kaspersky Endpoint Security.
- Отчеты о работе компонентов Kaspersky Endpoint Security.
- Отчеты о выполнении задач Kaspersky Endpoint Security.
- Отчет **Шифрование данных**. Содержит информацию о событиях, возникающих при шифровании и расшифровке данных.

В отчетах применяются следующие уровни важности событий:

 **Информационные сообщения**. События справочного характера, как правило, не несущие важной информации.

 **Предупреждения**. События, на которые нужно обратить внимание, поскольку они отражают важные ситуации в работе Kaspersky Endpoint Security.

 **Критические события**. События критической важности, указывающие на проблемы в работе Kaspersky Endpoint Security или на уязвимости в защите компьютера пользователя.

Для удобства работы с отчетами вы можете изменять представление данных на экране следующими способами:

- фильтровать список событий по различным критериям;
- использовать функцию поиска определенного события;
- просматривать выбранное событие в отдельном блоке;
- сортировать список событий по каждой графе отчета;
- отображать и скрывать сгруппированные с помощью фильтра события по кнопке  ;
- изменять порядок и набор граф, отображаемых в отчете.

При необходимости вы можете сохранить сформированный отчет в текстовый файл. Также вы можете удалять информацию из отчетов (см. раздел "Удаление информации из отчетов" на стр. 213) по компонентам и задачам Kaspersky Endpoint Security, объединенным в группы.

Если Kaspersky Endpoint Security работает под управлением Kaspersky Security Center, то информация о событиях может быть передана на Сервер администрирования Kaspersky Security Center (подробнее см. в *справке Kaspersky Security Center* https://help.kaspersky.com/KSC/12/ru-RU/).

В этом разделе

Просмотр отчетов

Если для пользователя доступен просмотр отчетов, то для этого пользователя доступен просмотр всех событий, отраженных в отчетах.

► *Чтобы просмотреть отчеты, выполните следующие действия:*

1. В главном окне программы нажмите на кнопку **Больше функций** → **Отчеты**.
2. В левой части окна **Отчеты** в списке компонентов и задач выберите компонент или задачу.

   В правой части окна отобразится отчет, содержащий список событий по результатам работы выбранного компонента или выбранной задачи Kaspersky Endpoint Security. Вы можете отсортировать события в отчете по значениям в ячейках одной из граф. По умолчанию события в отчете отсортированы по возрастанию значений в ячейках графы **Дата события**.
3. Если требуется просмотреть подробную информацию о событии, выберите в отчете нужное событие.

   В нижней части окна отобразится блок со сводной информацией о событии.

Настройка максимального срока хранения отчетов

По умолчанию максимальный срок хранения отчетов о событиях, фиксируемых Kaspersky Endpoint Security, составляет 30 дней. По истечении этого времени Kaspersky Endpoint Security автоматически удаляет наиболее старые записи из файла отчета.

► *Чтобы настроить максимальный срок хранения отчетов, выполните следующие действия:*

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Отчеты и хранилище**.
3. В блоке **Отчеты** установите флажок **Хранить отчеты не более N дней**, если хотите ограничить срок хранения отчетов. Укажите максимальный срок хранения отчетов.
4. Сохраните внесенные изменения.

Настройка максимального размера файла отчета

Вы можете указать максимальный размер файла, содержащего отчет. По умолчанию максимальный размер файла отчета составляет 1024 МБ. После достижения максимального размера файла отчета Kaspersky Endpoint Security автоматически удаляет наиболее старые записи из файла отчета таким образом, чтобы не превышался максимальный размер файла отчета.

► *Чтобы настроить максимальный размер файла отчета, выполните следующие действия:*

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Отчеты и хранилище**.
3. В блоке **Отчеты** установите флажок **Ограничить размер файла отчетов до N МБ**, если хотите ограничить размер файла отчета. Укажите максимальный размер файла отчета.
4. Сохраните внесенные изменения.

Сохранение отчета в файл

Пользователь сам несет ответственность за обеспечение безопасности информации из сохраненного в файл отчета и, в частности, за контроль и ограничение доступа к этой информации.

Сформированный отчет вы можете сохранить в файл текстового формата TXT или CSV.

Kaspersky Endpoint Security сохраняет событие в отчет в том виде, в каком событие отображается на экране, то есть с тем же составом и с той же последовательностью атрибутов события.

► *Чтобы сохранить отчет в файл, выполните следующие действия:*

1. В главном окне программы нажмите на кнопку **Больше функций** → **Отчеты**.
2. В открывшемся окне выберите компонент или задачу.

   В правой части окна отобразится отчет, содержащий список событий о работе выбранного компонента или задачи Kaspersky Endpoint Security.

3. Если требуется, измените представление данных в отчете с помощью следующих способов:
   - фильтрация событий;
   - поиск событий;
   - изменение расположения граф;
   - сортировка событий.
4. Нажмите на кнопку **Сохранить отчет**, расположенную в верхней правой части окна.
5. В открывшемся окне укажите папку, в которую вы хотите сохранить файл отчета.
6. В поле **Имя файла** введите название файла отчета.
7. В поле **Тип файла** выберите нужный формат файла отчета: TXT или CSV.
8. Сохраните внесенные изменения.

Удаление информации из отчетов

► *Чтобы удалить информацию из отчетов, выполните следующие действия*:

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Отчеты и хранилище**.
3. В блоке **Отчеты** нажмите на кнопку **Очистить**.
4. Если включена Защита паролем (см. раздел "Включение Защиты паролем" на стр. 192), Kaspersky Endpoint Security может запросить учетные данные пользователя. Программа запрашивает учетные данные, если у пользователя нет необходимого расширения.

Kaspersky Endpoint Security удалит все отчеты для всех компонентов и задач программы.

kaspersky

Самозащита Kaspersky Endpoint Security

Kaspersky Endpoint Security обеспечивает безопасность компьютера от вредоносных программ, включая и вредоносные программы, которые пытаются заблокировать работу Kaspersky Endpoint Security или удалить программу с компьютера.

Kaspersky Endpoint Security обеспечивает стабильность системы безопасности компьютера за счет следующих технологий:

- Механизм самозащиты. Предотвращает изменение и удаление файлов программы на жестком диске, процессов в памяти, записей в системном реестре.
- AM-PPL (Antimalware Protected Process Light). Защищает процессы Kaspersky Endpoint Security от вредоносных действий. Подробнее о технологии AM-PPL см. на сайте Microsoft (https://docs.microsoft.com/ru-ru/windows/win32/services/protecting-anti-malware-services-/).

  Технология AM-PPL доступна для операционных систем Windows 10 версии 1703 (RS2) и выше, Windows Server 2019.

- Механизм защиты от внешнего управления. Позволяет блокировать попытки управления службами программы и ее настройками с удаленного компьютера.

Под управлением 64-разрядных операционных систем доступно только управление механизмом самозащиты Kaspersky Endpoint Security от изменения или удаления файлов программы на жестком диске, а также от изменения или удаления записей в системном реестре.

В этом разделе

Включение и выключение механизма самозащиты

По умолчанию механизм самозащиты Kaspersky Endpoint Security включен.

► *Чтобы включить или выключить механизм самозащиты, выполните следующие действия:*

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Общие**.

3. Используйте флажок **Включить самозащиту**, чтобы включить или выключить механизм самозащиты.
4. Сохраните внесенные изменения.

Включение и выключение поддержки AM-PPL

Kaspersky Endpoint Security поддерживает технологию Antimalware Protected Process Light (далее "AM-PPL") от Microsoft. AM-PPL защищает процессы Kaspersky Endpoint Security от вредоносных действий (например, завершение работы программы). AM-PPL разрешает запуск только доверенных процессов. Процессы Kaspersky Endpoint Security подписаны в соответствии с требованиями безопасности Windows, поэтому являются доверенными. Подробнее о технологии AM-PPL см. на сайте Microsoft (https://docs.microsoft.com/ru-ru/windows/win32/services/protecting-anti-malware-services-/). По умолчанию технология AM-PPL включена.

Kaspersky Endpoint Security также имеет встроенные механизмы защиты процессов программы. Поддержка AM-PPL позволяет делегировать функции защиты процессов операционной системе. Таким образом, вы увеличиваете быстродействие программы и уменьшаете потребление ресурсов компьютера.

Сервис AM-PPL доступен для операционных систем Windows 10 версии 1703 (RS2) и выше, Windows Server 2019.

► *Чтобы включить или выключить поддержку технологии AM-PPL, выполните следующие действия:*

1. Выключите механизм самозащиты программы (см. раздел "Включение и выключение механизма самозащиты" на стр. 214).

   Механизм самозащиты предотвращает изменение и удаление процессов программы в памяти компьютера, в том числе изменение статуса AM-PPL.
2. Запустите интерпретатор командной строки cmd от имени администратора.
3. Перейдите в папку, в которой расположен исполняемый файл Kaspersky Endpoint Security.
4. В командной строке введите:
   - `klpsm.exe enable` – включение поддержки технологии AM-PPL (см. рис. ниже).
   - `klpsm.exe disable` – выключение поддержки технологии AM-PPL.
5. Перезапустите Kaspersky Endpoint Security.

6. Возобновите работу механизма самозащиты программы (см. раздел "Включение и выключение механизма самозащиты" на стр. 214).

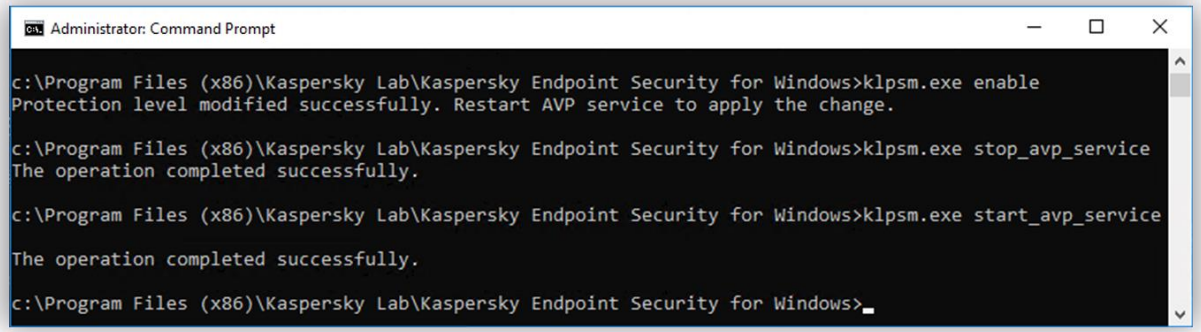


Рисунок 21. Включение поддержки технологии AM-PPL

Включение и выключение защиты от внешнего управления

Kaspersky Endpoint Security использует следующие механизмы защиты от внешнего управления:

- Защита от изменения настроек Kaspersky Endpoint Security с помощью программ удаленного администрирования (например, программы TeamViewer или RemotelyAnywhere).
- Защита от внешнего управления службами Kaspersky Endpoint Security (например, служба `AVP`).

► *Чтобы включить или выключить защиту от внешнего управления, выполните следующие действия:*

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Общие**.
3. Используйте флажок **Разрешить управление настройками Kaspersky Endpoint Security через программы удаленного управления**, чтобы включить или выключить защиту от изменения настроек Kaspersky Endpoint Security. Если вы используете программы удаленного администрирования, вам нужно разрешить управление настройками Kaspersky Endpoint Security и добавить программы в список доверенных (см. раздел "Обеспечение работы программ удаленного администрирования" на стр. 217). Недоверенным программам удаленного администрирования изменение настроек Kaspersky Endpoint Security запрещено, даже если установлен флажок **Разрешить управление настройками Kaspersky Endpoint Security через программы удаленного управления**. Этот флажок недоступен, если снят флажок **Включить самозащиту**.
4. Используйте флажок **Включить возможность внешнего управления системными службами**, чтобы включить или выключить защиту служб Kaspersky Endpoint Security от внешнего управления.

   Для завершения работы программы из командной строки необходимо, чтобы защита от внешнего управления службами Kaspersky Endpoint Security была выключена.

5. Сохраните внесенные изменения.

В результате, если механизмы защиты от внешнего управления включены, Kaspersky Endpoint Security блокирует наведение курсора на окно программы. При попытке удаленного пользователя остановить работу службы программы отображается системное окно с ошибкой.

kaspersky

Обеспечение работы программ удаленного администрирования

Нередко возникают ситуации, когда при использовании механизма защиты от внешнего управления возникает необходимость применить программы удаленного администрирования.

► *Чтобы обеспечить работу программ удаленного администрирования, выполните следующие действия:*

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Угрозы и исключения**.
3. В блоке **Исключения** перейдите по ссылке **Указать доверенные программы**.
4. В открывшемся окне нажмите на кнопку **Добавить**.
5. Выберите исполняемый файл программы удаленного администрирования.

   Также вы можете ввести путь вручную. Kaspersky Endpoint Security поддерживает переменные среды и символы `*` и `?` для ввода маски.
6. Установите флажок **Не контролировать активность программы**.
7. Сохраните внесенные изменения.

kaspersky

Производительность Kaspersky Endpoint Security и совместимость с другими программами

Производительность Kaspersky Endpoint Security

Под производительностью Kaspersky Endpoint Security подразумевается количество обнаруживаемых типов объектов, которые могут нанести вред компьютеру, а также потребление энергии и ресурсов компьютера.

Выбор типов обнаруживаемых объектов

Kaspersky Endpoint Security позволяет гибко настраивать защиту компьютера и выбирать типы объектов (см. раздел "Выбор типов обнаруживаемых объектов" на стр. 219), которые программа обнаруживает в ходе работы. Kaspersky Endpoint Security всегда проверяет операционную систему на наличие вирусов, червей и троянских программ. Вы не можете выключить проверку этих типов объектов. Такие программы могут нанести значительный вред компьютеру пользователя. Чтобы обеспечить большую безопасность компьютера, вы можете расширить список обнаруживаемых типов объектов, включив контроль действий легальных программ, которые могут быть использованы злоумышленником для нанесения вреда компьютеру или данным пользователя.

Использование режима энергосбережения

Во время работы на портативных компьютерах потребление программами энергоресурсов имеет особое значение. Зачастую задачи, которые Kaspersky Endpoint Security выполняет по расписанию, требуют значительного количества ресурсов. При питании компьютера от аккумулятора для экономии его заряда вы можете использовать режим энергосбережения.

Режим энергосбережения позволяет автоматически откладывать выполнение задач, для которых установлен запуск по расписанию:

- задача обновления;
- задача полной проверки;
- задача проверки важных областей;
- задача выборочной проверки;
- задача проверки целостности.

Независимо от того, включен режим энергосбережения или нет, Kaspersky Endpoint Security приостанавливает выполнение задач шифрования при переходе портативного компьютера в режим работы от аккумулятора. При выходе портативного компьютера из режима работы от аккумулятора в режим работы от сети программа возобновляет выполнение задач шифрования.

Передача ресурсов компьютера другим программам

Потребление ресурсов компьютера Kaspersky Endpoint Security может сказываться на производительности других программ. Чтобы решить проблему совместной работы при увеличении нагрузки на процессор и дисковые подсистемы, Kaspersky Endpoint Security может приостанавливать выполнение задач по расписанию и уступать ресурсы другим программам.

Однако существует ряд программ, которые запускаются в момент высвобождения ресурсов процессора и работают в фоновом режиме. Чтобы проверка не зависела от работы таких программ, не следует уступать им ресурсы операционной системы.

По мере необходимости вы можете запускать эти задачи вручную.

Применение технологии лечения активного заражения

Современные вредоносные программы могут внедряться на самые нижние уровни операционной системы, что делает их удаление практически невозможным. Обнаружив вредоносную активность в операционной системе, Kaspersky Endpoint Security выполняет расширенную процедуру лечения, применяя специальную технологию лечения активного заражения. *Технология лечения активного заражения* направлена на лечение операционной системы от вредоносных программ, которые уже запустили свои процессы в оперативной памяти и мешают Kaspersky Endpoint Security удалить их с помощью других методов. В результате угроза нейтрализуется. В процессе процедуры лечения активного заражения не рекомендуется запускать новые процессы или редактировать реестр операционной системы. Технология лечения активного заражения требует значительных ресурсов операционной системы, что может замедлить работу других программ.

После окончания процедуры лечения активного заражения на компьютере под управлением операционной системы Microsoft Windows для рабочих станций Kaspersky Endpoint Security запрашивает у пользователя разрешение на перезагрузку компьютера. После перезагрузки компьютера Kaspersky Endpoint Security удаляет файлы вредоносного программного обеспечения и запускает облегченную полную проверку компьютера.

Запрос перезагрузки на компьютере под управлением операционной системы Microsoft Windows для серверов невозможен из-за особенностей программы Kaspersky Endpoint Security. Незапланированная перезагрузка файлового сервера может повлечь за собой проблемы, связанные с временным отказом доступа к данным файлового сервера или потерей несохраненных данных. Перезагрузку файлового сервера рекомендуется выполнять строго по расписанию. Поэтому по умолчанию технология лечения активного заражения для файловых серверов выключена (см. раздел "Включение и выключение технологии лечения активного заражения" на стр. 220).

В случае обнаружения активного заражения на файловом сервере, на Kaspersky Security Center передается событие о необходимости лечения активного заражения. Для лечения активного заражения на сервере требуется включить технологию лечения активного заражения для серверов и запустить групповую задачу *Поиск вирусов* в удобное для пользователей сервера время.

В этом разделе

Выбор типов обнаруживаемых объектов

► *Чтобы выбрать типы обнаруживаемых объектов, выполните следующие действия:*

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Угрозы и исключения**.

3. В блоке **Типы обнаруживаемых объектов** установите флажки для типов объектов, которые должен обнаруживать Kaspersky Endpoint Security:
   - **Вирусы, черви**
   - **Троянские программы**
   - **Вредоносные утилиты**
   - **Рекламные программы**
   - **Программы автодозвона**
   - **Другие программы, которые могут быть использованы злоумышленниками для нанесения вреда компьютеру или данным пользователя**
   - **Упакованные объекты, способ упаковки которых может использоваться для защиты вредоносного кода**
   - **Множественно упакованные файлы**
4. Сохраните внесенные изменения.

Включение и выключение технологии лечения активного заражения

► *Чтобы включить или выключить технологию лечения активного заражения для рабочих станций, выполните следующие действия:*

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Общие**.
3. В блоке Режим защиты используйте флажок **Применять технологию лечения активного заражения**, чтобы включить или выключить технологию лечения активного заражения.
4. Сохраните внесенные изменения.

При запуске задачи лечения активного заражения через Kaspersky Security Center пользователю не будут доступны большинство функций операционной системы. После завершения задачи рабочая станция будет перезагружена.

► *Чтобы включить технологию лечения активного заражения для серверов, выполните одно из следующих действий:*

- Включите технологию лечения активного заражения в свойствах активной политики Kaspersky Security Center. Для этого выполните следующие действия:
  a. Откройте раздел **Параметры программы** окна свойств политики.
  b. Установите флажок **Применять технологию лечения активного заражения**.
  c. Нажмите на кнопку **ОК** в окне свойств политики, чтобы сохранить внесенные изменения.
- В свойствах групповой задачи Kaspersky Security Center "Поиск вирусов" установите флажок **Выполнять лечение активного заражения немедленно**.

► *Чтобы выключить технологию лечения активного заражения для серверов, выполните одно из следующих действий:*

- Выключите технологию лечения активного заражения в свойствах политики Kaspersky Security Center. Для этого выполните следующие действия:
  a. Откройте раздел **Параметры программы** окна свойств политики.
  b. Снимите флажок **Применять технологию лечения активного заражения**.
  c. Нажмите на кнопку **ОК** в окне свойств политики, чтобы сохранить внесенные изменения.
- В свойствах групповой задачи Kaspersky Security Center "Поиск вирусов" снимите флажок **Выполнять лечение активного заражения немедленно**.

Включение и выключение режима энергосбережения

► *Чтобы включить или выключить режим энергосбережения, выполните следующие действия:*

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Угрозы и исключения**.
3. В блоке **Производительность** используйте флажок **Откладывать задачи по расписанию при работе от аккумулятора**, чтобы включить или выключить режим энергосбережения.

   Если включен режим энергосбережения, при работе от аккумулятора не запускаются следующие задачи, даже если для них задан запуск по расписанию:

   - задача обновления;
   - задача полной проверки;
   - задача проверки важных областей;
   - задача выборочной проверки;
   - задача проверки целостности.
4. Сохраните внесенные изменения.

Включение и выключение режима передачи ресурсов другим программам

► *Чтобы включить или выключить режим передачи ресурсов другим программам, выполните следующие действия:*

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Общие**.
3. В блоке **Производительность** используйте флажок **Уступать ресурсы другим программам**, чтобы включить или выключить режим передачи ресурсов другим программам.

При включенном режиме передачи ресурсов другим программам Kaspersky Endpoint Security откладывает выполнение задач, если для них задан запуск по расписанию и их выполнение замедляет работу других программ:

- задача обновления;
- задача полной проверки;
- задача проверки важных областей;
- задача выборочной проверки;
- задача проверки целостности.

По умолчанию режим передачи ресурсов другим программам включен.

4. Сохраните внесенные изменения.

kaspersky

Создание и использование конфигурационного файла

Конфигурационный файл с параметрами работы Kaspersky Endpoint Security позволяет решить следующие задачи:

- Выполнить локальную установку Kaspersky Endpoint Security через командную строку с заранее заданными параметрами.

  Для этого требуется сохранить конфигурационный файл в той же папке, где находится дистрибутив.
- Выполнить удаленную установку Kaspersky Endpoint Security через Kaspersky Security Center с заранее заданными параметрами.
- Перенести параметры работы Kaspersky Endpoint Security с одного компьютера на другой.

► *Чтобы создать конфигурационный файл, выполните следующие действия:*

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Управление настройками**.
3. Нажмите на кнопку **Экспортировать**.
4. В открывшемся окне укажите путь, по которому вы хотите сохранить конфигурационный файл, и введите его имя.

   Чтобы использовать конфигурационный файл для локальной или удаленной установки Kaspersky Endpoint Security, необходимо назвать его install.cfg.
5. Нажмите на кнопку **Сохранить**.

► *Чтобы импортировать параметры работы Kaspersky Endpoint Security из конфигурационного файла, выполните следующие действия:*

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Управление настройками**.
3. Нажмите на кнопку **Импортировать**.
4. В открывшемся окне укажите путь к конфигурационному файлу.
5. Нажмите на кнопку **Открыть**.

Все значения параметров Kaspersky Endpoint Security будут установлены в соответствии с выбранным конфигурационным файлом.

Восстановление параметров программы по умолчанию

Вы в любое время можете восстановить настройки Kaspersky Endpoint Security, рекомендуемые "Лабораторией Касперского". В результате восстановления настроек для всех компонентов защиты будет установлен уровень безопасности **Рекомендуемый**.

► *Чтобы восстановить параметры программы по умолчанию, выполните следующие действия:*

1. В нижней части главного окна программы нажмите на кнопку .
2. В окне параметров программы выберите раздел **Управление настройками**.
3. Нажмите на кнопку **Восстановление**.
4. Нажмите на кнопку **Сохранить**.

kaspersky

Работа с программой из командной строки

Этот раздел содержит описание работы с Kaspersky Endpoint Security из командной строки.

В этом разделе

Команды

► *Чтобы управлять Kaspersky Endpoint Security из командной строки, выполните следующие действия:*

1. Запустите интерпретатор командной строки cmd от имени администратора.
2. Перейдите в папку, в которой расположен исполняемый файл Kaspersky Endpoint Security.
3. Используйте следующий шаблон для выполнения команды:

```
avp.com <команда> [параметры]
```

В результате Kaspersky Endpoint Security выполнит команду (см. рис. ниже).

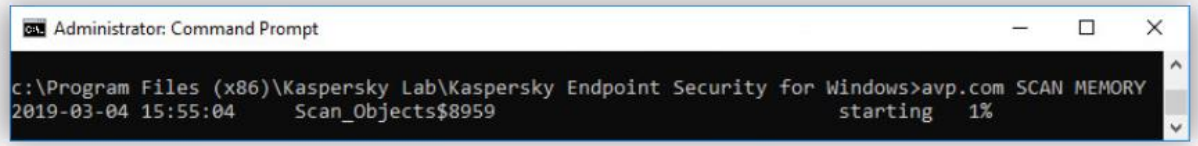


Рисунок 22. Управление программой из командной строки

kaspersky

В этом разделе

SCAN. Антивирусная проверка

Запустить задачу антивирусной проверки.

Синтаксис команды

```
SCAN [<область проверки>] [<действие при обнаружении угрозы>] [<типы файлов>]
[<исключения из проверки>] [/R[A]:<файл отчета>] [<технологии проверки>]
[/C:<файл с параметрами антивирусной проверки>]
```

kaspersky

Область проверки

`<файлы для проверки>`	Список файлов и папок через пробел. Длинные пути должны быть заключены в кавычки. Короткие пути (формат MS-DOS) заключать в кавычки не требуется. Например: • `"C:\Program Files (x86)\Example Folder"` – длинный путь. • `C:\PROGRA~2\EXAMPL~1` – короткий путь.
`/ALL`	Запустить задачу *Полная проверка*. Kaspersky Endpoint Security проверяет следующие объекты: • память ядра; • объекты, загрузка которых осуществляется при запуске операционной системы; • загрузочные секторы; • резервное хранилище операционной системы; • все жесткие и съемные диски.
`/MEMORY`	Проверить память ядра.
`/STARTUP`	Проверить объекты, загрузка которых осуществляется при запуске операционной системы.
`/MAIL`	Проверить почтовый ящик Outlook.
`/REMDRIVES`	Проверить съемные диски.
`/FIXDRIVES`	Проверить жесткие диски.
`/NETDRIVES`	Проверить сетевые диски.
`/QUARANTINE`	Проверить файлы в резервном хранилище Kaspersky Endpoint Security.
`/@:<список файлов.lst>`	Проверить файлы и папки, перечисленные в списке. Каждый файл из списка нужно вводить с новой строки. Длинные пути должны быть заключены в кавычки. Короткие пути (формат MS-DOS) заключать в кавычки не требуется. Например: • `"C:\Program Files (x86)\Example Folder"` – длинный путь. • `C:\PROGRA~2\EXAMPL~1` – короткий путь.

Действие при обнаружении угрозы

/i0	Информировать. Если выбран этот вариант действия, то при обнаружении зараженных файлов Kaspersky Endpoint Security добавляет информацию об этих файлах в список активных угроз.
/i1	Лечить; блокировать, если лечение невозможно. Если выбран этот вариант действия, то Kaspersky Endpoint Security автоматически пытается вылечить все обнаруженные зараженные файлы. Если лечение невозможно, то Kaspersky Endpoint Security добавляет информацию об обнаруженных зараженных файлах в список активных угроз.
/i2	Лечить; удалять, если лечение невозможно. Если выбран этот вариант действия, то Kaspersky Endpoint Security автоматически пытается вылечить все обнаруженные зараженные файлы. Если лечение невозможно, то Kaspersky Endpoint Security их удаляет. Этот вариант действия выбран по умолчанию.
/i3	Лечить обнаруженные зараженные файлы. Если лечение невозможно, удалять зараженные файлы. Также удалять составные файлы (например, архивы), если вылечить или удалить зараженный файл невозможно.
/i4	Удалять зараженные файлы. Также удалять составные файлы (например, архивы), если удалить зараженный файл невозможно.
/i8	Запрашивать действие у пользователя сразу после обнаружения угрозы.
/i9	Запрашивать действие у пользователя после выполнения проверки.

Типы файлов

`/fe`	Файлы, проверяемые по расширению. Если выбран этот параметр, Kaspersky Endpoint Security проверяет только потенциально заражаемые файлы. Формат файла определяется на основании его расширения.
`/fi`	Файлы, проверяемые по формату. Если выбран этот параметр, Kaspersky Endpoint Security проверяет только потенциально заражаемые файлы. Перед началом поиска вредоносного кода в файле выполняется анализ его внутреннего заголовка на предмет формата файла (например, TXT, DOC, EXE). В процессе проверки учитывается также расширение файла.
`/fa`	Все файлы. Если выбран этот параметр, Kaspersky Endpoint Security проверяет все файлы без исключения (любых форматов и расширений). Параметр выбран по умолчанию.

Исключения из проверки

`-e:a`	Исключение из проверки архивов форматов RAR, ARJ, ZIP, CAB, LHA, JAR, ICE.
`-e:b`	Исключение из проверки почтовых баз, входящих и исходящих сообщений электронной почты.
`-e:<маска файла>`	Исключение из проверки файлов по маске. Например: • Маска `*.exe` будет включать все пути к файлам с расширением exe. • Маска `example*` будет включать все пути к файлам с именем EXAMPLE.
`-e:<секунды>`	Исключение из проверки файлов, длительность проверки которых превышает установленное значение в секундах.
`-es:<мегабайты>`	Исключение из проверки файлов, размер которых превышает установленное значение в мегабайтах.

Режим сохранения событий в файл отчета

`/R:<файл отчета>`	Сохранять только критические события в файл отчета.
`/RA:<файл отчета>`	Сохранять все события в файл отчета.

Технологии проверки

`/iChecker=on|off`	Технология, позволяющая увеличить скорость проверки за счет исключения из нее некоторых файлов. Файлы исключаются из проверки по специальному алгоритму, учитывающему дату выпуска баз Kaspersky Endpoint Security, 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).
`/iSwift=on|off`	Технология, позволяющая увеличить скорость проверки за счет исключения из нее некоторых файлов. Файлы исключаются из проверки по специальному алгоритму, учитывающему дату выпуска баз Kaspersky Endpoint Security, дату предыдущей проверки файла, а также изменение параметров проверки. Технология iSwift является развитием технологии iChecker для файловой системы NTFS.

Дополнительные параметры

`/C:<файл с параметрами антивирусной проверки>`	Файл с параметрами задачи антивирусной проверки. Файл должен быть создан вручную и сохранен в формате TXT. Файл может иметь следующее содержание: `[<область проверки>] [<действие при обнаружении угрозы>] [<типы файлов>] [<исключения из проверки>] [/R[A]:<файл отчета>] [<технологии проверки>]`.

Пример:

```
avp.com SCAN /R:log.txt /MEMORY /STARTUP /MAIL "C:\Documents and Settings\All Users\My Documents" "C:\Program Files"
```

kaspersky

См. также

UPDATE. Обновление баз и модулей программы

Запустить задачу *Обновление*.

Синтаксис команды

```
UPDATE [local] ["<источник обновления>"] [/R[A]:<файл отчета>] [/C:<файл с параметрами обновления>]
```

Параметры задачи обновления

`local`

Запуск задачи *Обновление*, созданной автоматически после установки программы. Вы можете изменить параметры задачи *Обновление* в локальном интерфейсе программы или в консоли Kaspersky Security Center. Если этот параметр не установлен, Kaspersky Endpoint Security запускает задачу *Обновление* с параметрами по умолчанию или с параметрами, заданными в команде. Таким образом, вы можете настроить параметры задачи Обновление, следующим образом:

- `UPDATE` – запуск задачи *Обновление* с параметрами по умолчанию: источник обновления – серверы обновлений "Лаборатории Касперского", учетная запись – System, и другие.
- `UPDATE local` – запуск задачи *Обновление*, созданной автоматически после установки (предустановленная задача).
- `UPDATE <параметры обновления>` – запуск задача *Обновление* с параметрами, заданными вручную (см. ниже).

Источник обновления

`"<источник обновления>"`	Адрес HTTP-, FTP-сервера или папки общего доступа с пакетом обновлений. Вы можете указать только один источник обновления. Если источник обновлений не указан, Kaspersky Endpoint Security использует источник по умолчанию – серверы обновлений "Лаборатории Касперского".

Режим сохранения событий в файл отчета

`/R:<файл отчета>`	Сохранять только критические события в файл отчета.
`/RA:<файл отчета>`	Сохранять все события в файл отчета.

Дополнительные параметры

`/C:<файл с параметрами обновления>`	Файл с параметрами задачи *Обновление*. Файл должен быть создан вручную и сохранен в формате TXT. Файл может иметь следующее содержание: `["<источник обновления>"] [/R[A]:<файл отчета>]`.

Пример:

```
avp.com UPDATE local
avp.com UPDATE "ftp://my_server/kav updates" /RA:avbases_upd.txt
```

См. также

Запуск и остановка задачи обновления 70

ROLLBACK. Откат последнего обновления

Откатить последние обновления антивирусных баз. Это позволяет вернуться к использованию предыдущей версии баз и модулей программы при необходимости, например, в том случае, если новая версия баз содержит некорректную сигнатуру, из-за которой Kaspersky Endpoint Security блокирует безопасную программу.

Синтаксис команды

```
ROLLBACK [/R[A]:<файл отчета>]
```

Режим сохранения событий в файл отчета

`/R:<файл отчета>`	Сохранять только критические события в файл отчета.
`/RA:<файл отчета>`	Сохранять все события в файл отчета.

Пример:

```
avp.com ROLLBACK /RA:rollback.txt
```

TRACES. Трассировка

Включить / выключить трассировку. Файлы трассировки (см. раздел "О составе и хранении файлов трассировки" на стр. 261) хранятся на вашем компьютере в течение всего времени использования программы и безвозвратно удаляются при удалении программы. Файлы трассировки, кроме файлов трассировки Агента аутентификации, хранятся в папке %ProgramData%\Kaspersky Lab\KES\Traces. По умолчанию трассировка выключена.

Синтаксис команды

```
TRACES on|off [<уровень трассировки>] [<дополнительные параметры>]
```

Уровень трассировки

`<уровень трассировки>`	Уровень детализации трассировки. Возможные значения: • `100` (критический). Только сообщения о неустранимых ошибках. • `200` (высокий). Сообщения о всех ошибках, включая неустранимые. • `300` (диагностический). Сообщения о всех ошибках, а также предупреждения. • `400` (важный). Сообщения о всех ошибках, предупреждения, а также дополнительная информация. • `500` (обычный). Сообщения о всех ошибках, предупреждениях, а также подробная информация о работе программы в нормальном режиме (значение по умолчанию). • `600` (низкий). Все сообщения.

Дополнительные параметры	
`all`	Выполнить команду с параметрами `dbg`, `file` и `mem`.
`dbg`	Использовать функцию OutputDebugString и сохранять файл трассировки. Функция OutputDebugString отправляет символьную строку отладчику программы для вывода на экран. Подробнее см. на *сайте MSDN* (*https://msdn.microsoft.com/ru-RU/library/windows/desktop/aa363362(v=vs.85).aspx*).
`file`	Сохранить один файл трассировки (без ограничений по размеру).
`rot`	Сохранить результаты трассировки в ограниченное число файлов ограниченного размера и перезаписать старые файлы при достижении максимального размера.
`mem`	Записывать результаты трассировки в файлы дампов.

Примеры:

- `avp.com TRACES on 500`
- `avp.com TRACES on 500 dbg`
- `avp.com TRACES off`
- `avp.com TRACES on 500 dbg mem`
- `avp.com TRACES off file`

См. также

Трассировка работы программы 264
Трассировка производительности программы 265
О составе и хранении файлов трассировки 261
Запись дампов 266
Защита файлов дампов и трассировок 266

START. Запуск профиля

Запустить выполнение профиля (например, запустить обновление баз или включить компонент защиты).

Синтаксис команды

```
START <профиль> [/R[A]:<файл отчета>]
```

Профиль

`<профиль>`

Название профиля. *Профиль* – компонент, задача или функция Kaspersky Endpoint Security. Список доступных профилей (см. раздел "Профили программы" на стр. 256) вы можете узнать по команде `HELP START`.

Режим сохранения событий в файл отчета

`/R:<файл отчета>`

Сохранять только критические события в файл отчета.

`/RA:<файл отчета>`

Сохранять все события в файл отчета.

Пример:

```
avp.com START Scan_Objects
```

STOP. Остановка профиля

Остановить выполняемый профиль (например, остановить проверку съемных дисков или выключить компонент защиты).

Для выполнения команды должна быть включена Защита паролем (см. раздел "Включение Защиты паролем" на стр. 192). Пользователь должен иметь разрешения **Выключение компонентов защиты**, **Выключение компонентов контроля**.

Синтаксис команды

```
STOP <профиль> /login=<имя пользователя> /password=<пароль>
```

Профиль

`<профиль>`

Название профиля. *Профиль* – компонент, задача или функция Kaspersky Endpoint Security. Список доступных профилей (см. раздел "Профили программы" на стр. 256) вы можете узнать по команде `HELP STOP`.

Авторизация
`/login=<имя пользователя>`
`/password=<пароль>`
	Учетные данные пользователя с необходимыми разрешениями Защиты паролем (см. раздел "Предоставление разрешений для отдельных пользователей или групп" на стр. 193).

STATUS. Статус профиля

Показать информацию о состоянии профилей программы (см. раздел "Профили программы" на стр. 256) (например, `running` или `completed`). Список доступных профилей вы можете узнать по команде `HELP STATUS`.

Также Kaspersky Endpoint Security показывает информацию о состоянии служебных профилей. Информация о состоянии служебных профилей может понадобиться при обращении в Службу технической поддержки "Лаборатории Касперского".

Синтаксис команды

```
STATUS [<профиль>]
```

STATISTICS. Статистика выполнения профиля

Показать статистическую информацию о профиле программы (см. раздел "Профили программы" на стр. 256) (например, время проверки или количество обнаруженных угроз). Список доступных профилей вы можете узнать по команде `HELP STATISTICS`.

Синтаксис команды

```
STATISTICS <профиль>
```

RESTORE. Восстановление файлов

Восстановить файл из резервного хранилища в папку его исходного размещения. Если по указанному пути уже существует файл с таким же именем, к имени файла добавляется суффикс "-copy". Восстанавливаемый файл копируется с исходным именем.

Для выполнения команды должна быть включена Защита паролем (см. раздел "Включение Защиты паролем" на стр. 192). Пользователь должен иметь разрешение **Восстановление из резервного хранилища**.

Резервное хранилище – это хранилище резервных копий файлов, которые были изменены в процессе лечения или удалены. *Резервная копия* – копия файла, которая создается до лечения или удаления этого файла. Резервные копии файлов хранятся в специальном формате и не представляют опасности.

Резервные копии файлов хранятся в папке `C:\ProgramData\Kaspersky Lab\KES\QB`.

Полные права доступа к этой папке предоставлены пользователям группы "Администраторы". Ограниченные права доступа к этой папке предоставлены пользователю, под учетной записью которого выполнялась установка Kaspersky Endpoint Security.

В Kaspersky Endpoint Security отсутствует возможность настройки прав доступа пользователей к резервным копиям файлов.

Синтаксис команды

```
RESTORE [/REPLACE] <имя файла> /login=<имя пользователя> /password=<пароль>
```

Дополнительные параметры

`/REPLACE`	Переписать существующий файл.
`<имя файла>`	Имя восстанавливаемого файла.

Авторизация

`/login=<имя пользователя>` `/password=<пароль>`	Учетные данные пользователя с необходимыми разрешениями Защиты паролем (см. раздел "Предоставление разрешений для отдельных пользователей или групп" на стр. 193).

Пример:

```
avp.com RESTORE /REPLACE true_file.txt /login=KLAdmin /password=!Password1
```

EXPORT. Экспорт параметров программы

Экспортировать параметры Kaspersky Endpoint Security в файл. Файл будет размещен в папке C:\Windows\SysWOW64.

Синтаксис команды

```
EXPORT <профиль> <имя файла>
```

Профиль

`<профиль>`

Название профиля. *Профиль* – компонент, задача или функция Kaspersky Endpoint Security. Список доступных профилей (см. раздел "Профили программы" на стр. 256) вы можете узнать по команде `HELP EXPORT`.

Файл для экспорта

`<имя файла>`

Имя файла, в который должны быть экспортированы параметры профиля. Вы можете экспортировать параметры профиля в конфигурационный файл в формате DAT или CFG, в текстовый файл в формате TXT или в документ в формате XML.

Примеры:

- `avp.com EXPORT ids ids_config.dat`
- `avp.com EXPORT fm fm_config.txt`

См. также

Создание и использование конфигурационного файла 223

IMPORT. Импорт параметров программы

Импортировать параметры Kaspersky Endpoint Security из файла, который был создан с помощью команды `EXPORT`.

Для выполнения команды должна быть включена Защита паролем (см. раздел "Включение Защиты паролем" на стр. 192). Пользователь должен иметь разрешение **Настройка параметров программы**.

Синтаксис команды

```
IMPORT <имя файла> /login=<имя пользователя> /password=<пароль>
```

Файл для импорта

`<имя файла>`

Имя файла, из которого должны быть импортированы параметры программы. Вы можете импортировать параметры Kaspersky Endpoint Security из конфигурационного файла в формате DAT или CFG, текстового файла в формате TXT или документа в формате XML.

Авторизация

`/login=<имя пользователя>`
`/password=<пароль>`

Учетные данные пользователя с необходимыми разрешениями Защиты паролем (см. раздел "Предоставление разрешений для отдельных пользователей или групп" на стр. 193).

Пример:

```
avp.com IMPORT config.dat /login=KLAdmin /password=!Password1
```

См. также

Создание и использование конфигурационного файла 223

ADDKEY. Применение файла ключа

Применить файл ключа для активации Kaspersky Endpoint Security. Если программа уже активирована, ключ будет добавлен в качестве резервного.

Синтаксис команды

```
ADDKEY <имя файла> [/login=<имя пользователя> /password=<пароль>]
```

Файл ключа

`<имя файла>`

Имя файла ключа.

Авторизация

`/login=<имя пользователя>`
`/password=<пароль>`

Данные учетной записи пользователя. Данные учетные записи нужно вводить, только если включена Защита паролем (на стр. 189).

Пример:

```
avp.com ADDKEY file.key
```

LICENSE. Лицензирование

Выполнить операции с лицензионными ключами программы Kaspersky Endpoint Security.

Для выполнения команды удаления лицензионного ключа должна быть включена Защита паролем (см. раздел "Включение Защиты паролем" на стр. 192). Пользователь должен иметь разрешение **Удаление ключа**.

Синтаксис команды

```
LICENSE <операция> [/login=<имя пользователя> /password=<пароль>]
```

Операция	
`/ADD <имя файла>`	Применить файл ключа для активации Kaspersky Endpoint Security. Если программа уже активирована, ключ будет добавлен в качестве резервного.
`/ADD <код активации>`	Активировать Kaspersky Endpoint Security с помощью кода активации. Если программа уже активирована, ключ будет добавлен в качестве резервного.
`/REFRESH <имя файла>`	Продлить срок действия лицензии с помощью файла ключа. В результате будет добавлен резервный ключ, который станет активным по истечении срока действия лицензии. Добавить активный ключ с помощью этой команды невозможно.
`/REFRESH <код активации>`	Продлить срок действия лицензии с помощью кода активации. В результате будет добавлен резервный ключ, который станет активным по истечении срока действия лицензии. Добавить активный ключ с помощью этой команды невозможно.
`/DEL /login=<имя пользователя> /password=<пароль>`	Удалить лицензионный ключ. Также будет удален резервный ключ.

Авторизация

`/login=<имя пользователя>`
`/password=<пароль>`

Учетные данные пользователя с необходимыми разрешениями Защиты паролем (см. раздел "Предоставление разрешений для отдельных пользователей или групп" на стр. 193).

Пример:

- `avp.com LICENSE /ADD file.key`
- `avp.com LICENSE /ADD AAAAA-BBBBB-CCCCC-DDDDD`
- `avp.com LICENSE /DEL /login=KLAdmin /password=!Password1`

RENEW. Покупка лицензии

Перейти на веб-сайт "Лаборатории Касперского" для покупки лицензии или продления ее срока действия.

PBATESTRESET. Сбросить результаты проверки перед шифрованием диска

Сбросить результаты проверки поддержки полнодискового шифрования (FDE) по технологиям Шифрование диска Kaspersky и BitLocker.

Перед запуском полнодискового шифрования программа выполняет ряд проверок на возможность шифрования компьютера. Если полнодисковое шифрование невозможно, Kaspersky Endpoint Security сохраняет информацию о несовместимости. При следующей попытке шифрования программа не выполняет проверки и предупреждает о том, что шифрование невозможно. Если аппаратная конфигурация компьютера изменилась, то для проверки системного жесткого диска на совместимость с технологией Шифрования диска Kaspersky или BitLocker требуется сбросить информацию о несовместимости, полученную программой при предыдущей проверке.

EXIT. Завершение работы программы

Завершить работу Kaspersky Endpoint Security. Программа будет выгружена из оперативной памяти компьютера.

Для выполнения команды должна быть включена Защита паролем (см. раздел "Включение Защиты паролем" на стр. 192). Пользователь должен иметь разрешение **Завершение работы программы**.

Синтаксис команды

`EXIT /login=<имя пользователя> /password=<пароль>`

kaspersky

EXITPOLICY. Выключение политики

Выключает политику Kaspersky Security Center на компьютере. Все параметры Kaspersky Endpoint Security доступны для настройки, в том числе параметры, отмеченные в политике закрытым замком ().

Для выполнения команды должна быть включена Защита паролем (см. раздел "Включение Защиты паролем" на стр. 192). Пользователь должен иметь разрешение **Выключение политики Kaspersky Security Center**.

Синтаксис команды

```
EXITPOLICY /login=<имя пользователя> /password=<пароль>
```

STARTPOLICY. Включение политики

Включить политику Kaspersky Security Center на компьютере. Параметры программы будут настроены в соответствии с политикой.

DISABLE. Выключение защиты

Выключить Защиту от файловых угроз на компьютере с истекшей лицензией на Kaspersky Endpoint Security. Выполнить команду на компьютере с неактивированной программой или с действующей лицензией невозможно.

SPYWARE. Обнаружение шпионского ПО

Включить / выключить обнаружение шпионского ПО. По умолчанию обнаружение шпионского ПО включено.

Синтаксис команды

```
SPYWARE on|off
```

MDRLICENSE. Активация MDR

Выполнить операции с конфигурационным файлом BLOB для активации Managed Detection and Response. BLOB-файл содержит идентификатор клиента и информацию о лицензии Kaspersky Managed Detection and Response. BLOB-файл находится в ZIP-архиве конфигурационного файла MDR. Вы можете получить ZIP-архив в Консоли Kaspersky Managed Detection and Response. Подробную информацию о BLOB-файле *см. в справке Kaspersky Managed Detection and Response* https://support.kaspersky.com/MDR/ru-RU/.

Для выполнения операций с BLOB-файлом требуются права администратора. Также параметры Managed Detection and Response в политике должны быть доступны для изменения ().

Синтаксис команды

```
MDRLICENSE <операция> [/login=<имя пользователя> /password=<пароль>]
```

Операция

`/ADD <имя файла>`	Применить конфигурационный файл BLOB для интеграции с Kaspersky Managed Detection and Response (формат файла P7). Вы можете применить только один BLOB-файл. Если BLOB-файл уже добавлен на компьютер, файл будет заменен.
`/DEL`	Удалить конфигурационный файл BLOB.

Авторизация

`/login=<имя пользователя> /password=<пароль>`	Учетные данные пользователя с необходимыми разрешениями Защиты паролем (см. раздел "Предоставление разрешений для отдельных пользователей или групп" на стр. 193).

Пример:

- `avp.com MDRLICENSE /ADD file.key`
- `avp.com MDRLICENSE /DEL /login=KLAdmin /password=!Password1`

KSN. Переключение Глобальный / Локальный KSN

Выбор решения Kaspersky Security Network для определения репутации файлов или сайтов. Kaspersky Endpoint Security поддерживает следующие инфраструктурные решения KSN:

- *Глобальный KSN* – это решение, которое используют большинство программ "Лаборатории Касперского". Участники KSN получают информацию от Kaspersky Security Network, а также отправляют в "Лабораторию Касперского" данные об объектах, обнаруженных на компьютере пользователя, для дополнительной проверки аналитиками "Лаборатории Касперского" и пополнения репутационных и статистических баз Kaspersky Security Network.
- *Локальный KSN* – это решение, позволяющее пользователям компьютеров, на которые установлена программа Kaspersky Endpoint Security или другие программы "Лаборатории Касперского", получать доступ к репутационным базам Kaspersky Security Network, а также другим статистическим данным, не отправляя данные в KSN со своих компьютеров. Локальный KSN разработан для корпоративных клиентов, не имеющих возможности участвовать в Kaspersky Security Network, например, по следующим причинам:
  - отсутствие подключения локальных рабочих мест к сети Интернет;
  - законодательный запрет или ограничение корпоративной безопасности на отправку любых данных за пределы страны или за пределы локальной сети организации.

Синтаксис команды

```
KSN /global | /private <имя файла>
```

Конфигурационный файл Локального KSN

`<имя файла>`

Имя
PEM

Пример:

```
avp.com KSN /global
avp.com KSN /private C:\ksn_config.pkcs7
```

См. также

Сообщения об ошибках

При работе с программой возможно появление следующих сообщений об ошибках:

Таблица 10. Сообщения об ошибках и коды возврата

Сообщение об ошибке в командной строке	Код возврата в Shell
`Error %d getting thread's context`	
`Error %d loading QueryInformationThread function`	
`Error %d opening thread`	
`Error %d querying thread information`	
`Error %d suspending thread`	
`Error in UpdateKSNConfig`	
`Error in thread safety code: could not acquire a lock`	
`Error: %S (err 0x%x)`	
`Error: %S: %s (err 0x%x)`	

Сообщение об ошибке в командной строке	Код возврата в Shell
Error: '%S' has not been completed due to execution timeout	_Shell::_E_TIMEOUT
Error: '%S' is disabled	
Error: Cannot change state for '%S' (%S), task already in state?	SHELL_RET_FAILED
Error: Cannot change state for '%S' (%S), task disabled?	SHELL_RET_FAILED
Error: Cannot create message receiver	
Error: Cannot create task, err=%08X	SHELL_RET_FAILED
Error: Cannot find task '%S'	SHELL_RET_FAILED /SHELL_RET_PARAMETER_INVALID
Error: Cannot get product settings	
Error: Cannot get tasks list	SHELL_RET_FAILED
Error: Cannot initialize task parameters block	SHELL_RET_PARAMETER_INVALID
Error: Cannot open configuration file '%S'	
Error: Cannot open list file '%S'	
Error: Cannot set report handler	
Error: Cannot start task '%S', error=%08X	SHELL_RET_NO_LICENCE
Error: Cannot start task '%S', no licence	_Shell::_S_NO_LICENSE
Error: Cannot start task '%S', parameters invalid	SHELL_RET_PARAMETER_INVALID
Error: Cannot verify task parameters block	
Error: Change state failed for task '%S' (%S), error=%08X	SHELL_RET_FAILED
Error: Command unavailable due to password protection disabled	
Error: Configuration file not specified (/C)	
Error: Credential is not obtained, access denied	
Error: Duplicate taskid '%S'	
Error: Failed to flush cached data	

Сообщение об ошибке в командной строке	Код возврата в Shell
Error: File list not specified	
Error: File list not specified (/@)	
Error: Internal error %08X	SHELL_RET_FAILED
Error: Invalid command '%S'	
Error: Invalid parameter '%S'	
Error: Local task control is denied by policy	
Error: NOT IMLEMENTED	SHELL_RET_FAILED
Error: Not enough memory	
Error: Nothing to scan	
Error: Parameter '%S' must contain exclusion specification	
Error: Parameter '%S' must specify size in megabytes	
Error: Parameter not supported by task '%S'	
Error: Password or login is invalid, access denied	
Error: Profile name must be specified	SHELL_RET_PARAMETER_INVALID
Error: Task '%S' not found	SHELL_RET_TASK_FAILED
Error: Unknown parameter '%S'	
Error: Usage parameter /APP=<on|off>	
Error: Usage parameter /iChecker=<on|off>	
Error: Usage parameter /iSwift=<on|off>	
Error: cannot open report file %S, error=%d %s	
Error: control of this task is not allowed	
Error: failed to register message handlers	
Error: failed to set INetSwift state	
Error: failed to unregister message handlers	

Сообщение об ошибке в командной строке	Код возврата в Shell
Error: Local task control is denied by policy	
Scan_Quarantine failed: %	SHELL_RET_FAILED
Scan_Quarantine completed successfully	SHELL_RET_OK
Failed to get AVP_SERVICE_PRODUCT. Error	SHELL_RET_FAILED
Disable command cannot be elevated. Error	SHELL_RET_FAILED
Failed to disable product from command line. Error	SHELL_RET_FAILED
Failed to get AVP_SERVICE_PRODUCT. Error	
Failed to get TaskManager service. Error	
Failed to get service locator. Error	
Invalid parameters	SHELL_RET_PARAMETER_INVALID
Failed while activating Global KSN	SHELL_RET_FAILED
Failed to execute command set silent detect. Error	_Shell::_E_FAIL
Failed to execute command silent detect check. Error	_Shell::_E_FAIL
Path not exist	
Cannot write to file, no permission	
Cannot add key file	SHELL_RET_TASK_FAILED
INetSwift state set to	SHELL_RET_OK
Internal error	SHELL_RET_FAILED
Fail to terminate command on user's request	_Shell::_E_BREAK_FAIL
Command is terminated on user's request	_Shell::_E_BREAK_OK

kaspersky

Коды возврата

Любая команда, выполняемая администратором в командной строке, может возвращать код возврата. Коды возврата бывают general или специфичные для отдельных задач.

Доступны следующие коды возврата:

- General коды возврата:
  - `0` - задача выполнена успешно;
  - `1` - некорректное значение параметра;
  - `2` - неизвестная ошибка;
  - `3` - ошибка во время выполнения задачи;
  - `4` - выполнение задачи прервано.
- Коды возврата задач антивирусной проверки:
  - `101` - все опасные объекты обработаны;
  - `102` - обнаружены опасные объекты.
- Коды возврата других задач:
  - `-14` - истекло время ожидания.
  - `239` - ошибка во время приостановки задачи.
  - `240` - задача отменена пользователем.
  - `-15` - файл заблокирован другим процессом и недоступен для обработки программой.
  - `-10` - указан неверный путь к объекту.
  - `-8` - ключ недействителен.
  - `-7` - ключ находится в черном списке.
  - `-13` - ключ предназначен для другого продукта.
  - `[1-127]` - дни до истечения срока действия лицензии.

    Если до истечения срока действия лицензии осталось более 127 дней, код возврата 127. Если до истечения срока действия лицензии осталось менее 127 дней, код возврата соответствует реальному количеству дней. Если лицензия уже истекла, код возврата 1.
  - `8000045` - недостаточно прав.
  - `102` - есть необработанные угрозы.

Таблица 11. Символьные и числовые значения кодов возврата

Символьные значения	Числовые значения	Доступно для команд
_Shell::_E_TIMEOUT	-14	START UPDATE ROLLBACK SCAN
_Shell::_E_BREAK_FAIL	239	UPDATE ROLLBACK SCAN
_Shell::_E_BREAK_OK	240	UPDATE ROLLBACK SCAN
_Shell::_E_FAIL	-3	MESSAGES LICENSE: /Check /Add (ActivateByCode) /Add (ActivateByKeyEx) /AddTicket /DeleteKey /Refresh
_Shell::_E_FILE_BLOCKED	-15	UPDATE ROLLBACK SCAN
_Shell::_E_INVALID_PATH	-10	LICENSE: /Add (ActivateByKeyEx) /AddTicket
_Shell::_E_INVALID_SYNTAX	-2	UPDATE ROLLBACK MESSAGES SCAN
_Shell::_E_KEY_CORRUPTED	-8	LICENSE: /Add (ActivateByKeyEx) /AddTicket

Символьные значения	Числовые значения	Доступно для команд
_Shell::_E_KEY_IN_BLST	-7	LICENSE: /Check /Add (ActivateByCode) /Add (ActivateByKeyEx) /AddTicket
_Shell::_E_KEY_NOT_MATCH	-13	LICENSE: /Add (ActivateByKeyEx) /AddTicket
_Shell::_S_ALL_DETECTION	2	UPDATE ROLLBACK SCAN
_Shell::_S_NO_LICENSE	0	LICENSE: /Check /Add (ActivateByCode) /Add (ActivateByKeyEx) /AddTicket /DeleteKey
_Shell::_S_OK	0	UPDATE ROLLBACK SCAN LICENSE: /Add (ActivateByKeyEx) /AddTicket /Refresh
_Shell::_S_PARTIAL_DETECTION	3	UPDATE ROLLBACK SCAN
[1-127]	[1-127]	LICENSE: /Check /Add (ActivateByCode) /Add (ActivateByKeyEx) /AddTicket
errACCESS_DENIED	8000045	STOP EXITPOLICY

Символьные значения	Числовые значения	Доступно для команд
SHELL_RET_FAILED	2	START STOP STATUS STATISTICS MODE HELP EXPORT IMPORT EXIT ADDKEY INETSWIFT EXITPOLICY STARTPOLICY UPDATE ROLLBACK RENEW DISABLE TRACE\TRACES SPYWARE MESSAGES RESTORE PBATESTRESET PATCHCOMPATIBILITYRESET SCAN
-SHELL_RET_FAILED	-2	LICENSE: /Add (ActivateByKeyEx) /AddTicket
SHELL_RET_NO_LICENCE	2	START UPDATE ROLLBACK SCAN

Символьные значения	Числовые значения	Доступно для команд
SHELL_RET_OK	0	START STOP STATUS STATISTICS HELP EXPORT IMPORT EXIT ADDKEY INETSWIFT EXITPOLICY STARTPOLICY UPDATE ROLLBACK RENEW DISABLE TRACE\TRACES SLC SPYWARE LETSDUMP MESSAGES RESTORE PBATESTRESET PATCHCOMPATIBILITYRESET SCAN LICENSE: /Add (ActivateByCode)

Символьные значения	Числовые значения	Доступно для команд
SHELL_RET_PARAMETER_INVALID	1	START STOP STATUS STATISTICS EXPORT IMPORT ADDKEY INETSWIFT UPDATE ROLLBACK RENEW DISABLE TRACE\TRACES SPYWARE RESTORE PATCHCOMPATIBILITYRESET SCAN
-SHELL_RET_PARAMETER_INVALID	-1	LICENSE: /Add (ActivateByKeyEx) /AddTicket
SHELL_RET_SCAN_ALL_THREATED	101	UPDATE ROLLBACK SCAN
SHELL_RET_SCAN_NO_THREATS	0	UPDATE ROLLBACK SCAN
SHELL_RET_SCAN_SUSPICIOUS_UNTREATED	0	UPDATE ROLLBACK SCAN
SHELL_RET_SCAN_THREATS	102	UPDATE ROLLBACK SCAN

Символьные значения	Числовые значения	Доступно для команд
SHELL_RET_TASK_FAILED	3	STOP EXPORT IMPORT ADDKEY UPDATE ROLLBACK RESTORE SCAN
-SHELL_RET_TASK_FAILED	-3	LICENSE: /Add (ActivateByKey) /Add (ActivateByKeyEx) /AddTicket
SHELL_RET_TASK_STOPPED	4	UPDATE ROLLBACK SCAN

Использование профилей задач

Профиль задачи (далее также "профиль") – это набор параметров в текстовом или бинарном виде для создания задачи Kaspersky Endpoint Security.

Профили определяются в реестре операционной системы Windows в ветке HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\protected\KES10SP2\profiles или HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\KasperskyLab\protected\KES10SP2\profiles.

Профили имеют иерархическую структуру. Изменения, внесенные в родительский профиль, отражаются и на профилях, входящих в его состав. Например, при удалении родительского профиля все профили, входящие в его состав, также будут удалены.

Профиль может содержать следующие параметры:

- flags – внутренний механизм, описывающий доступные операции с задачей;
- enabled – параметр, разрешающий или запрещающий запуск задачи;
- installed – внутренний механизм, определяющий, установлены ли модули для данного профиля;
- level – внутренний механизм, используемый для разделения параметров по уровням;
- type – текстовое описание типа задачи;

- `remote` – параметр, позволяющий запустить задачу в отдельном процессе;
- `admflags` - параметры управления задачей с помощью Kaspersky Security Center;
- `pid` – идентификатор бинарного модуля, который содержит реализацию задачи;
- `iid` – идентификатор интерфейса задачи, определяющий класс, который содержит исполняемый код для работы задачи;
- `persistent` – параметр, определяющий количество задач одного типа, которые можно создать в программе Kaspersky Endpoint Security;
- `idSettings` – идентификатор структуры параметров;
- `idStatistics` – идентификатор структуры статистики выполнения задачи;
- `schedule` – параметры расписания задачи;
- `runas` – параметры прав запуска задачи (используется только при значении параметра `persistent = 0`);
- `smode` – параметр, используемый для отложенного выполнения задачи;
- `settings` – дополнительные параметры задачи;
- `def` – параметры задачи, установленные по умолчанию.

Kaspersky Endpoint Security выполняет задачи на основе заданных параметров профиля. При создании задачи программа считывает все профили из реестра и для каждого профиля выполняет следующие действия:

1. Создает пустую структуру параметров с типом `idSettings`.
2. Десериализует значения параметра `settings` в подготовленную структуру.

   Если значения параметра `settings` не заданы, то программа использует значения параметра `def` и десериализует их в структуру. При отсутствии значений параметра `def` используются системные значения, заданные по умолчанию для пустой структуры параметров.

3. Создает пустую структуру с типом `idStatistics`, если этот параметр был указан в профиле для создаваемой задачи.
4. Находит бинарный модуль по идентификатору `pid`.
5. Создает экземпляр задачи по идентификатору `iid` из бинарного модуля.
6. Передает структуру параметров и статистики полученному экземпляру задачи.
7. Если указаны значения параметров `installed = 1` и `persistent = 1`, то программа запускает задачу.
8. Если указано значение параметра `persistent = 0`, то программа проверяет параметры `schedule` и `smode` и планирует запуск задачи в соответствии с заданными значениями.

Консоль администрирования Kaspersky Security Center позволяет создавать несколько групповых задач одного типа с различными параметрами. Для каждой такой задачи в реестре создается профиль с названием вида `<profile name>$<unique id>`, где `unique id` - уникальный идентификатор для задачи.

kaspersky

Профили программы

Профиль – компонент, задача или функция Kaspersky Endpoint Security. Профили предназначены для управления программой из командной строки. Вы можете использовать профили для выполнения команд `START`, `STOP`, `STATUS`, `STATISTICS`, `EXPORT` и `IMPORT`. С помощью профилей вы можете настроить параметры программы (например, `STOP DeviceControl`) или запустить задачу (например, `START Scan_My_Computer`).

Доступны следующие профили:

- `AdaptiveAnomaliesControl` – Адаптивный контроль аномалий.
- `AMSI` – AMSI-защита.
- `BehaviorDetection` – Анализ поведения.
- `DeviceControl` – Контроль устройств.
- `EntAppControl` – Контроль программ.
- `File_Monitoring` или `FM` – Защита от файловых угроз.
- `Firewall` или `FW` – Сетевой экран.
- `HIPS` – Предотвращение вторжений.
- `IDS` – Защита от сетевых угроз.
- `IntegrityCheck` – Проверка целостности.
- `Mail_Monitoring` или `EM` – Защита от почтовых угроз.
- `Rollback` – Откат обновления.
- `Scan_ContextScan` – Проверка из контекстного меню.
- `Scan_IdleScan` – Фоновая проверка.
- `Scan_Memory` – Проверка памяти ядра.
- `Scan_My_Computer` – Полная проверка.
- `Scan_Objects` – Выборочная проверка.
- `Scan_Qscan` – Проверка объектов, загрузка которых осуществляется при запуске операционной системы.
- `Scan_Removable_Drive` – Проверка съемных дисков.
- `Scan_Startup` или `STARTUP` – Проверка важных областей.
- `Updater` – Обновление.
- `Web_Monitoring` или `WM` – Защита от веб-угроз.
- `WebControl` – Веб-Контроль.

Также Kaspersky Endpoint Security поддерживает работу служебных профилей. Служебные профили могут понадобиться при обращении в Службу технической поддержки "Лаборатории Касперского".

kaspersky

Действия после сбоя или неустранимой ошибки в работе программы

Программа автоматически восстанавливает свою работу после сбоев, участие пользователя не требуется. В случае, когда программа не может восстановить свою работу, вам требуется переустановить программу или ее компонент. Вы также можете обратиться за помощью в Службу технической поддержки (см. раздел "Способы получения технической поддержки" на стр. 258).

kaspersky

Способы получения технической поддержки

Если вы не нашли решения вашей проблемы в документации или других источниках информации о программе, рекомендуется обратиться в Службу технической поддержки. Сотрудники Службы технической поддержки ответят на ваши вопросы об установке и использовании программы.

Kaspersky предоставляет поддержку этой программы в течение ее жизненного цикла (см. страницу жизненного цикла программ (https://support.kaspersky.com/corporate/lifecycle)). Прежде чем обратиться в Службу технической поддержки, ознакомьтесь с правилами предоставления технической поддержки (https://support.kaspersky.ru/support/rules#ru_ru).

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

- позвонить в Службу технической поддержки по телефону (https://support.kaspersky.ru/b2b) ;
- отправить запрос в Службу технической поддержки "Лаборатории Касперского" с портала Kaspersky CompanyAccount (https://companyaccount.kaspersky.com).

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" (https://support.kaspersky.ru/b2b).

Перед обращением в Службу технической поддержки ознакомьтесь с правилами предоставления технической поддержки (https://support.kaspersky.ru/support/rules#ru_ru).

Техническая поддержка через Kaspersky CompanyAccount

Kaspersky CompanyAccount (https://companyaccount.kaspersky.com) – это портал для организаций, использующих программы "Лаборатории Касперского". Портал Kaspersky CompanyAccount предназначен для взаимодействия пользователей со специалистами "Лаборатории Касперского" с помощью электронных запросов. На портале Kaspersky CompanyAccount можно отслеживать статус обработки электронных запросов специалистами "Лаборатории Касперского" и хранить историю электронных запросов.

Вы можете зарегистрировать всех сотрудников вашей организации в рамках одной учетной записи Kaspersky CompanyAccount. Одна учетная запись позволяет вам централизованно управлять электронными запросами от зарегистрированных сотрудников в "Лабораторию Касперского", а также управлять правами этих сотрудников в Kaspersky CompanyAccount.

Портал Kaspersky CompanyAccount доступен на следующих языках:

- английском;
- испанском;
- итальянском;
- немецком;
- польском;
- португальском;
- русском;
- французском;
- японском.

Вы можете узнать больше о Kaspersky CompanyAccount на веб-сайте Службы технической поддержки (https://support.kaspersky.ru/faq/companyaccount_help).

kaspersky

Обращение в Службу технической поддержки

Если вы не нашли решения вашей проблемы в документации или других источниках информации о программе, рекомендуется обратиться в Службу технической поддержки. Сотрудники Службы технической поддержки ответят на ваши вопросы об установке и использовании программы.

Kaspersky предоставляет поддержку этой программы в течение ее жизненного цикла (см. страницу жизненного цикла программ (https://support.kaspersky.com/corporate/lifecycle)). Прежде чем обратиться в Службу технической поддержки, ознакомьтесь с правилами предоставления технической поддержки (https://support.kaspersky.ru/support/rules#ru_ru).

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

- позвонить в Службу технической поддержки по телефону (https://support.kaspersky.ru/b2b) ;
- отправить запрос в Службу технической поддержки "Лаборатории Касперского" с портала Kaspersky CompanyAccount (https://companyaccount.kaspersky.com).

После того как вы проинформируете специалистов Службы технической поддержки "Лаборатории Касперского" о возникшей проблеме, они могут попросить вас создать *файл трассировки*. Файл трассировки позволяет отследить процесс пошагового выполнения команд программы и обнаружить, на каком этапе работы программы возникает ошибка.

Кроме того, специалистам Службы технической поддержки может понадобиться дополнительная информация об операционной системе, запущенных процессах на компьютере, подробные отчеты работы компонентов программы.

Во время работ по диагностике специалисты Службы технической поддержки могут попросить вас изменить параметры программы:

- Активировать функциональность получения расширенной диагностической информации.
- Выполнить более тонкую настройку работы отдельных компонентов программы, недоступную через стандартные средства пользовательского интерфейса.
- Изменить параметры хранения полученной диагностической информации.
- Настроить перехват и сохранение в файл сетевого трафика.

Вся необходимая для выполнения перечисленных действий информация (описание последовательности шагов, изменяемые параметры, конфигурационные файлы, скрипты, дополнительные возможности командной строки, отладочные модули, специализированные утилиты и так далее), а также состав полученных в отладочных целях данных будут сообщены вам специалистами Службы технической поддержки. Полученная расширенная диагностическая информация сохраняется на компьютере пользователя. Автоматическая пересылка полученных данных в "Лабораторию Касперского" не выполняется.

kaspersky

Перечисленные выше действия должны выполняться только под руководством специалистов Службы технической поддержки по полученным от них инструкциям. Самостоятельное изменение параметров работы программы способами, не описанными в Руководстве администратора или в рекомендациях специалистов Службы технической поддержки, может привести к замедлению и сбоям в работе операционной системы, снижению уровня защиты компьютера, а также к нарушению доступности и целостности обрабатываемой информации.

В этом разделе

О составе и хранении файлов трассировки

Вы сами несете ответственность за обеспечение безопасности полученной информации и, в частности, за контроль и ограничение доступа к полученной информации, хранимой на компьютере, до ее передачи в "Лабораторию Касперского".

Файлы трассировки хранятся на вашем компьютере в течение всего времени использования программы и безвозвратно удаляются при удалении программы.

Файлы трассировки, кроме файлов трассировки Агента аутентификации, хранятся в папке %ProgramData%\Kaspersky Lab\KES\Traces.

Файлы трассировки называются следующим образом: `KES<служебный номер версии_dateXX.XX_timeXX.XX_pidXXX.><тип файла трассировки>.log`.

Вы можете просмотреть данные, записанные в файлы трассировки.

Все файлы трассировки содержат следующие общие данные:

- Время события.
- Номер потока выполнения.

  Эту информацию не содержит файл трассировки Агента аутентификации.

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

Kaspersky Endpoint Security сохраняет пароли пользователя в файл трассировки только в зашифрованном виде.

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

В файлы трассировки `SRV.log`, `GUI.log` и `ALL.log`, помимо общих данных, может записываться следующая информация:

- Персональные данные, в том числе фамилия, имя и отчество, если эти данные являются частью пути к файлам на локальном компьютере.
- Данные об установленном на компьютере аппаратном обеспечении (например, данные о прошивке BIOS / UEFI). Эти данные записываются в файлы трассировки при выполнении полнодискового шифрования по технологии Шифрование диска Kaspersky.
- Имя пользователя и пароль, если они передавались в открытом виде. Эти данные могут записываться в файлы трассировки при проверке интернет-трафика.
- Имя пользователя и пароль, если они содержатся в заголовках протокола HTTP.
- Имя учетной записи для входа в Microsoft Windows, если имя учетной записи является частью имени файла.
- Адрес вашей электронной почты или веб-адрес с именем учетной записи и паролем, если они содержатся в имени обнаруженного объекта.
- Веб-сайты, которые вы посещаете, а также ссылки с этих веб-сайтов. Эти данные записываются в файлы трассировки, когда программа проверяет веб-сайты.
- Адрес прокси-сервера, имя компьютера, порт, IP-адрес, имя пользователя, используемое при авторизации на прокси-сервере. Эти данные записываются в файлы трассировки, если программа использует прокси-сервер.
- Внешние IP-адреса, с которыми было установлено соединение с вашего компьютера.
- Тема сообщения, идентификатор, имя отправителя и адрес веб-страницы отправителя сообщения в социальной сети. Эти данные записываются в файлы трассировки, если включен компонент Веб-Контроль.
- Данные о сетевом трафике. Эти данные записываются в файлы трассировки, если включены компоненты мониторинга трафика (например, Веб-Контроль).
- Данные, полученные с серверов "Лаборатории Касперского" (например, версия антивирусных баз).
- Статусы компонентов Kaspersky Endpoint Security и сведения об их работе.
- Данные о действиях пользователя в программе.
- События операционной системы.

Содержание файлов трассировки HST.log, BL.log, Dumpwriter.log, WD.log, AVPCon.dll.log

Файл трассировки `HST.log`, помимо общих данных, содержит информацию о выполнении задачи обновления баз и программных модулей.

Файл трассировки `BL.log`, помимо общих данных, содержит информацию о событиях, возникающих во время работы программы, а также данные, необходимые для устранения неполадок в работе программы. Этот файл создается, если программа запускается с параметром avp.exe –bl.

Файл трассировки `Dumpwriter.log`, помимо общих данных, содержит служебную информацию, необходимую для устранения неполадок, возникающих при записи файла дампа программы.

Файл трассировки `WD.log`, помимо общих данных, содержит информацию о событиях, возникающих в процессе работы службы avpsus, в том числе события обновления программных модулей.

Файл трассировки `AVPCon.dll.log`, помимо общих данных, содержит информацию о событиях, возникающих при работе модуля связи с Kaspersky Security Center.

Содержание файлов трассировки производительности

Файлы трассировки производительности называются следующим образом: `KES<номер версии_dateXX.XX_timeXX.XX_pidXXX.>PERF.HAND.etl`.

Файлы трассировки производительности, помимо общих данных, содержат информацию о нагрузке на процессор, о времени загрузки операционной системы и программ, о запущенных процессах.

Содержание файла трассировки компонента AMSI-защита

Файл трассировки AMSI.log, помимо общих данных, содержит информацию о результатах проверок, запрошенных сторонними приложениями.

Содержание файла трассировки компонента Защита от почтовых угроз

Файл трассировки `mcou.OUTLOOK.EXE.log`, помимо общих данных, может содержать части сообщений электронной почты, в том числе адреса электронной почты.

Содержание файла трассировки компонента Проверка из контекстного меню

Файл трассировки `shellex.dll.log`, помимо общих данных, содержит информацию о выполнении задачи проверки и данные, необходимые для устранения неполадок в работе программы.

Содержание файлов трассировки веб-плагина программы

Файлы трассировки веб-плагина программы хранятся на компьютере, на котором развернута Kaspersky Security Center 12 Web Console, в папке Program Files\Kaspersky Lab\Kaspersky Security Center Web Console 12\logs.

Файлы трассировки веб-плагина программы называются следующим образом: `logs-kes_windows-<тип файла трассировки>.DESKTOP-<дата обновления файла>.log`. Web Console начинает записывать данные после установки и удаляет файлы трассировки после удаления Web Console.

Файлы трассировки веб-плагина программы, помимо общих данных, содержат следующую информацию:

- Пароль пользователя KLAdmin для разблокировки интерфейса Kaspersky Endpoint Security (Защита паролем).
- Временный пароль для разблокировки интерфейса Kaspersky Endpoint Security (Защита паролем).
- Имя пользователя и пароль для почтового SMTP-сервера (Уведомления по электронной почте).
- Имя пользователя и пароль для прокси-сервера сети интернет (Прокси-сервер).
- Имя пользователя и пароль для задачи *Изменение состава компонентов программы*.
- Учетные данные и пути, указанные в свойствах политики и в задачах Kaspersky Endpoint Security.

Содержание файла трассировки Агента аутентификации

Файл трассировки Агента аутентификации хранится в папке System Volume Information и называется следующим образом: `KLFDE.{EB2A5993-DFC8-41a1-B050-F0824113A33A}.PBELOG.bin`.

Файл трассировки Агента аутентификации, помимо общих данных, содержит информацию о работе Агента аутентификации и действиях, которые выполняет пользователь в Агенте аутентификации.

Трассировка работы программы

Трассировка программы – это подробная запись действий, выполняемых программой, и сообщений о событиях, происходящих во время работы программы.

Выполняйте трассировку программы под руководством Службы технической поддержки "Лаборатории Касперского".

► *Чтобы создать файл трассировки программы, выполните следующие действия:*

1. В главном окне программы нажмите на кнопку .

   Откроется окно **Поддержка**.
2. В окне **Поддержка** нажмите на кнопку **Мониторинг проблем**.
3. Используйте переключатель **Включить трассировку программы**, чтобы включить или выключить трассировку работы программы.
4. В раскрывающемся списке **Трассировка** выберите режим трассировки работы программы:
   - **С ротацией**. Сохранить результаты трассировки в ограниченное число файлов ограниченного размера и перезаписать старые файлы при достижении максимального размера. Если выбран этот режим, вы можете указать максимальное количество файлов для ротации и максимальный размер каждого файла.
   - **Записывать в один файл**. Сохранить один файл трассировки (без ограничений по размеру).
5. В раскрывающемся списке **Уровень** выберите уровень трассировки.

   Требуемый уровень трассировки рекомендуется уточнить у специалиста Службы технической поддержки. Если указания Службы технической поддержки отсутствуют, рекомендуется устанавливать уровень трассировки **Обычный (500)**.
6. Перезапустите Kaspersky Endpoint Security.
7. Чтобы остановить процесс трассировки, вернитесь в окно **Поддержка** и выключите трассировку.

Вы также можете создать файлы трассировки во время установки программы из командной строки, в том числе с помощью файла setup.ini.

Файлы трассировки (см. раздел "О составе и хранении файлов трассировки" на стр. 261) хранятся на вашем компьютере в течение всего времени использования программы и безвозвратно удаляются при удалении программы. Файлы трассировки, кроме файлов трассировки Агента аутентификации, хранятся в папке %ProgramData%\Kaspersky Lab\KES\Traces. По умолчанию трассировка выключена.

kaspersky

Трассировка производительности программы

Kaspersky Endpoint Security позволяет получить информацию о проблемах в работе компьютера при использовании программы. Например, вы можете получить информацию о задержках при загрузке операционной системы после установки программы. Для этого Kaspersky Endpoint Security создает файлы трассировки производительности (см. раздел "О составе и хранении файлов трассировки" на стр. 261). *Трассировка производительности* – это запись действий, выполняемых программой, для диагностики проблем производительности Kaspersky Endpoint Security. Для получения информации Kaspersky Endpoint Security использует сервис трассировки событий Windows (англ. ETW – Event Tracing for Windows). Диагностику работы Kaspersky Endpoint Security и установление причин возникновения проблем выполняет Служба технической поддержки "Лаборатории Касперского".

Выполняйте трассировку программы под руководством Службы технической поддержки "Лаборатории Касперского".

► *Чтобы создать файл трассировки производительности, выполните следующие действия:*

1. В главном окне программы нажмите на кнопку .

   Откроется окно **Поддержка**.
2. В окне **Поддержка** нажмите на кнопку **Мониторинг проблем**.
3. Используйте переключатель **Включить трассировку производительности**, чтобы включить или выключить трассировку производительности программы.
4. В раскрывающемся списке **Трассировка** выберите режим трассировки работы программы:
   - **С ротацией**. Сохранить результаты трассировки в ограниченное число файлов ограниченного размера и перезаписать старые файлы при достижении максимального размера. Если выбран этот режим, вы можете указать максимальный размер каждого файла.
   - **Записывать в один файл**. Сохранить один файл трассировки (без ограничений по размеру).
5. В раскрывающемся списке **Уровень** выберите уровень трассировки:
   - **Легкий**. Kaspersky Endpoint Security анализирует основные процессы операционной системы, связанные с производительностью.
   - **Детальный**. Kaspersky Endpoint Security анализирует все процессы операционной системы, связанные с производительностью.
6. В раскрывающемся списке **Тип трассировки** выберите тип трассировки:
   - **Базовая информация**. Kaspersky Endpoint Security анализирует процессы во время работы операционной системы. Используйте этот тип трассировки, если проблема воспроизводится после загрузки операционной системы, например, проблема доступа в интернет в браузере.
   - **При перезагрузке**. Kaspersky Endpoint Security анализирует процессы только на этапе загрузки операционной системы. После загрузки операционной системы Kaspersky Endpoint Security останавливает трассировку. Используйте этот тип трассировки, если проблема связана с задержкой загрузки операционной системы.
7. Перезагрузите компьютер и воспроизведите проблему.
8. Чтобы остановить процесс трассировки, вернитесь в окно **Поддержка** и выключите трассировку.

В результате в папке %ProgramData%\Kaspersky Lab\KES\Traces будет создан файл трассировки производительности. После создания файла трассировки отправьте файл в Службу технической

поддержки "Лаборатории Касперского".

Запись дампов

Файл дампа содержит всю информацию о рабочей памяти процессов Kaspersky Endpoint Security на момент создания этого файла дампа.

Сохраненные дампы могут содержать конфиденциальные данные. Для контроля доступа к данным вам нужно самостоятельно обеспечить защиту файлов дампов.

Файлы дампов хранятся на вашем компьютере в течение всего времени использования программы и безвозвратно удаляются при удалении программы. Файлы дампов хранятся в папке %ProgramData%\Kaspersky Lab\KES\Traces.

► *Чтобы включить или выключить запись дампов, выполните следующие действия:*

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Общие**.
3. В блоке **Отладочная информация** используйте флажок **Включить запись дампов**, чтобы включить или выключить запись дампов программы.
4. Сохраните внесенные изменения.

Защита файлов дампов и трассировок

Файлы дампов и файлы трассировки содержат информацию об операционной системе, а также могут содержать данные пользователя (см. раздел "О составе и хранении файлов трассировки" на стр. 261). Чтобы предотвратить несанкционированный доступ к этим данным, вы можете включить защиту файлов дампов и файлов трассировки.

Если защита файлов дампов и файлов трассировки включена, доступ к файлам имеют следующие пользователи:

- К файлам дампов имеют доступ системный и локальный администраторы, а также пользователь, включивший запись файлов дампов и файлов трассировки.
- К файлам трассировки имеют доступ только системный и локальный администраторы.

► *Чтобы включить или выключить защиту файлов дампов и файлов трассировки, выполните следующие действия:*

1. В нижней части главного окна программы нажмите на кнопку ⚙.
2. В окне параметров программы выберите раздел **Общие**.
3. В блоке **Отладочная информация** используйте флажок **Включить защиту файлов дампов и файлов трассировки**, чтобы включить или выключить защиту файлов.
4. Сохраните внесенные изменения.

Файлы дампов и файлы трассировки, записанные при включенной защите, остаются защищенными

после отключения этой функции.

kaspersky

Глоссарий

О

OLE-объект

Файл, присоединенный или встроенный в другой файл. Программы "Лаборатории Касперского" позволяют проверять на присутствие вирусов OLE-объекты. Например, если вы вставите какую-либо таблицу Microsoft Office Excel® в документ Microsoft Office Word, данная таблица будет проверяться как OLE-объект.

А

Агент администрирования

Компонент программы Kaspersky Security Center, осуществляющий взаимодействие между Сервером администрирования и программами "Лаборатории Касперского", установленными на конкретном сетевом узле (рабочей станции или сервере). Данный компонент является единым для всех программ "Лаборатории Касперского", работающих в операционной системе Windows. Для программ, работающих в других операционных системах, предназначены отдельные версии Агента администрирования.

Агент аутентификации

Интерфейс, позволяющий после шифрования загрузочного жесткого диска пройти процедуру аутентификации для доступа к зашифрованным жестким дискам и для загрузки операционной системы.

Активный ключ

Ключ, используемый в текущий момент для работы программы.

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.

Архив

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

Б

База вредоносных веб-адресов

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

База фишинговых веб-адресов

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

Г

Группа администрирования

Набор устройств, объединенных в соответствии с выполняемыми функциями и устанавливаемым на них набором программ "Лаборатории Касперского". Устройства группируются для удобства управления ими как единым целым. В состав группы могут входить другие группы. Для каждой из установленных в группе программ могут быть созданы групповые политики и сформированы групповые задачи.

Д

Доверенный платформенный модуль

Микрочип, разработанный для предоставления основных функций, связанных с безопасностью (например, для хранения ключей шифрования). Доверенный платформенный модуль обычно устанавливается на материнской плате компьютера и взаимодействует с остальными компонентами системы при помощи аппаратной шины.

Дополнительный ключ

Ключ, подтверждающий право на использование программы, но не используемый в текущий момент.

З

Задача

Функции, выполняемые программой "Лаборатории Касперского", реализованы в виде задач, например: Постоянная защита файлов, Полная проверка устройства, Обновление баз.

Зараженный файл

Файл, внутри которого содержится вредоносный код (при проверке файла был обнаружен код известной программы, представляющей угрозу). Специалисты "Лаборатории Касперского" не рекомендуют вам работать с такими файлами, поскольку это может привести к заражению вашего компьютера.

И

Издатель сертификата

Центр сертификации, выдавший сертификат.

kaspersky

К

Коннектор к Агенту администрирования

Функциональность программы, обеспечивающая связь программы с Агентом администрирования. Агент администрирования предоставляет возможность удаленного управления программой через Kaspersky Security Center.

Л

Лечение объектов

Способ обработки зараженных объектов, в результате применения которого происходит полное или частичное восстановление данных. Не все зараженные объекты можно вылечить.

Лицензионный сертификат

Документ, который передает вам вместе с файлом ключа или кодом активации "Лаборатория Касперского". Документ содержит информацию о предоставляемой лицензии.

Ложное срабатывание

Ситуация, когда незараженный файл определяется программой "Лаборатории Касперского" как зараженный ввиду того, что его код напоминает код вируса.

М

Маска файла

Представление названия и расширения файла общими символами.

Для формирования маски файла можно использовать любые символы, допустимые в названиях файлов, в том числе специальные:

- ***** – символ, заменяющий нуль или более нуля любых символов;
- **?** – символ, заменяющий любой один символ.

Следует иметь в виду, что название и расширение файла всегда пишутся через точку.

Н

Настройки задачи

Настройки работы программы, специфичные для каждого типа задач.

Нормализованная форма адреса веб-ресурса

Нормализованной формой адреса веб-ресурса называется текстовое представление адреса веб-ресурса, полученное в результате применения нормализации. Нормализация – процесс, в результате которого текстовое представление адреса веб-ресурса изменяется в соответствии с определенными правилами (например, исключение из текстового представления адреса веб-ресурса имени пользователя, пароля и

порта соединения, понижение верхнего регистра символов адреса веб-ресурса до нижнего регистра).

В контексте работы компонентов защиты цель нормализации адресов веб-ресурсов заключается в том, чтобы проверять синтаксически различные, но физически эквивалентные адреса веб-ресурсов один раз.

Пример:

Ненормализованная форма адреса: www.Example.com\.

Нормализованная форма адреса: www.example.com.

О

Область защиты

Объекты, которые компонент базовой защиты постоянно проверяет во время своей работы. Область защиты разных компонентов имеет разные свойства.

Область проверки

Объекты, которые Kaspersky Endpoint Security проверяет во время выполнения задачи проверки.

Обновление

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

Отпечаток сертификата

Информация, по которой можно проверить подлинность сертификата сервера. Отпечаток создается путем применения криптографической хеш-функции к содержанию сертификата сервера.

П

Параметры программы

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

Портативный файловый менеджер

Программа, предоставляющая интерфейс для работы с зашифрованными файлами на съемных дисках при недоступности функциональности шифрования на компьютере.

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 др. Риск внедрения в такие файлы вредоносного кода достаточно высок.

Программные модули

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

P

Резервное хранилище

Специальное хранилище, предназначенное для сохранения резервных копий объектов, создаваемых перед их лечением или удалением.

C

Сервер администрирования

Компонент программы Kaspersky Security Center, осуществляющий функции централизованного хранения информации об установленных в сети организации программах "Лаборатории Касперского" и управления ими.

Сертификат

Электронный документ, содержащий открытый ключ, информацию о владельце ключа и области применения ключа, а также подтверждающий принадлежность открытого ключа владельцу. Сертификат должен быть подписан выдавшим его центром сертификации.

Сетевая служба

Набор параметров, характеризующих сетевую активность. Для этой сетевой активности вы можете создать сетевое правило, регулирующее работу Сетевого экрана.

Сигнатурный анализ

Технология обнаружения угроз, которая использует базы Kaspersky Endpoint Security, 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.

Субъект сертификата

Держатель закрытого ключа, связанного с сертификатом. Это может быть пользователь, программа, любой виртуальный объект, компьютер или служба.

Ф

Фишинг

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

Ч

Черный список адресов

Список адресов электронной почты, входящие сообщения с которых блокируются программой "Лаборатории Касперского" независимо от их содержания.

Э

Эвристический анализ

Технология обнаружения угроз, которые невозможно определить с помощью текущей версии баз программ "Лаборатории Касперского". Позволяет находить файлы, которые могут содержать неизвестный вирус или новую модификацию известного вируса.

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.

kaspersky

Информация о стороннем коде

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

Соответствие терминов

В этом разделе приведено соответствие терминов, используемых в документации, и терминов, используемых в требованиях ФСТЭК.

Таблица 12. Соответствие терминов

Термин в документации	Термин в требованиях ФСТЭК
программа	продукт, объект оценки, программное изделие
вирус, программа, представляющая угрозу, вредоносная программа	КВ, компьютерный вирус
антивирусные базы, базы программы	базы данных признаков компьютерных вирусов (БД ПКВ)
события	данные аудита
администратор	администратор безопасности, уполномоченный субъект информационной системы, уполномоченный пользователь

kaspersky

Приложение 1. Значения параметров программы в сертифицированной конфигурации

Этот раздел содержит перечень параметров программы, влияющих на безопасное состояние программы, и безопасные значения (диапазоны значений) параметров в сертифицированной конфигурации.

Изменение каких-либо из перечисленных параметров с их значений (диапазона значений) в сертифицированном конфигурации на другие значения, выводит программу из безопасного состояния.

Таблица 13. Параметры и их безопасные значения для программы в сертифицированной конфигурации

Сущность, к которой относится параметр	Название параметра	Безопасное значение или диапазон значений параметра (сертифицированная конфигурация)
Продвинутая защита		
Kaspersky Security Network	Kaspersky Security Network	Переключатель выключен. Допускается включить переключатель только при использовании Локального KSN (Kaspersky Private Security Network – KPSN).
Откат вредоносных действий	Откат вредоносных действий	Переключатель включен.
Базовая защита		
Защита от файловых угроз	Защита от файловых угроз	Переключатель включен.
Защита от файловых угроз	Уровень безопасности	Одно из следующих значений: • Рекомендуемый. • Высокий.
Защита от файловых угроз	Действие при обнаружении угрозы	Лечить; удалять, если лечение невозможно.
Защита от файловых угроз → Расширенная настройка	Типы файлов	Все файлы.
Защита от файловых угроз → Расширенная настройка	Область защиты	Все съемные диски, Все жесткие диски, Все сетевые диски.
Защита от файловых угроз → Расширенная настройка	Эвристический анализ	Флажок установлен.
Защита от файловых угроз → Расширенная настройка	Проверять архивы	Флажок установлен.

Сущность, к которой относится параметр	Название параметра	Безопасное значение или диапазон значений параметра (сертифицированная конфигурация)
Защита от почтовых угроз	Защита от почтовых угроз	Переключатель включен.
Защита от почтовых угроз	Уровень безопасности	Одно из следующих значений: • Рекомендуемый. • Высокий.
Защита от почтовых угроз	Действие при обнаружении угрозы	Лечить; удалять, если лечение невозможно.
Защита от сетевых угроз	Защита от сетевых угроз	Переключатель включен.
Защита от сетевых угроз	Добавить атакующий компьютер в список блокирования на N минут	Флажок установлен. Время блокирования – 60 мин.
Защита от сетевых угроз	Исключения	Пустой список IP-адресов. Добавление некоторых исключений может вести к выходу из безопасного состояния. Администратору безопасности следует осторожно подходить к выбору исключений. Для минимизации риска рекомендуется оставить значения по умолчанию.
Контроль безопасности		
Контроль программ	Контроль программ	Переключатель включен.
Задачи		
Обновление	Загружать обновления модулей программы	Флажок снят.
Настройки программы		
Общие	Запускать Kaspersky Endpoint Security для Windows при включении компьютера	Флажок установлен.

Сущность, к которой относится параметр	Название параметра	Безопасное значение или диапазон значений параметра (сертифицированная конфигурация)
Общие	Применять технологию лечения активного заражения	Флажок установлен.
Общие	Включить самозащиту	Флажок установлен.
Общие	Выключить внешнее управление системными службами	Флажок установлен.
Угрозы и исключения	Типы обнаруживаемых объектов	Вирусы, черви; Троянские программы; Вредоносные утилиты; Упакованные объекты, способ упаковки которых может использоваться для защиты вредоносного кода; Множественно упакованные файлы
Угрозы и исключения	Исключения	Список исключений пуст. Добавление некоторых исключений может вести к выходу из безопасного состояния. Администратору безопасности следует осторожно подходить к выбору исключений. Для минимизации риска рекомендуется оставить значения по умолчанию.
Угрозы и исключения	Доверенные программы	Список доверенных программ пуст. Добавление некоторых доверенных программ может вести к выходу из безопасного состояния. Администратору безопасности следует осторожно подходить к выбору доверенных программ. Для минимизации риска рекомендуется оставить значения по умолчанию.
Интерфейс	Защита паролем	Переключатель включен. Администратор безопасности должен установить надежный пароль и область действия (все опции).

kaspersky

Приложение 2. Группы доверия программ

Все программы, запускаемые на компьютере, Kaspersky Endpoint Security распределяет на группы доверия. Программы распределяются на группы доверия в зависимости от степени угрозы, которую эти программы могут представлять для операционной системы.

Существуют следующие группы доверия:

- **Доверенные**. В группу входят программы, для которых выполняется одно или более следующих условий:
  - Программы обладают цифровой подписью доверенных производителей.
  - О программах есть записи в базе доверенных программ Kaspersky Security Network.
  - Пользователь поместил программы в группу "Доверенные".

  Запрещенных операций для таких программ нет.
- **Слабые ограничения**. В группу входят программы, для которых выполняются следующие условия:
  - Программы не обладают цифровой подписью доверенных производителей.
  - О программах нет записей в базе доверенных программ Kaspersky Security Network.
  - Пользователь поместил программы в группу "Слабые ограничения".

  Такие программы имеют минимальные ограничения на работу с ресурсами операционной системы.
- **Сильные ограничения**. В группу входят программы, для которых выполняются следующие условия:
  - Программы не обладают цифровой подписью доверенных производителей.
  - О программах нет записей в базе доверенных программ Kaspersky Security Network.
  - Пользователь поместил программы в группу "Сильные ограничения".

  Такие программы имеют значительные ограничения на работу с ресурсами операционной системы.
- **Недоверенные**. В группу входят программы, для которых выполняются следующие условия:
  - Программы не обладают цифровой подписью доверенных производителей.
  - О программах нет записей в базе доверенных программ Kaspersky Security Network.
  - Пользователь поместил программы в группу "Недоверенные".

  Для таких программ запрещены все операции.

kaspersky

Приложение 3. Расширения файлов для быстрой проверки съемных дисков

com – исполняемый файл программы размером не более 64 КБ;

exe – исполняемый файл, самораспаковывающийся архив;

sys – системный файл Microsoft Windows;

prg – текст программы dBase™, Clipper или Microsoft Visual FoxPro®, программа пакета WAVmaker;

bin – бинарный файл;

bat – файл пакетного задания;

cmd – командный файл Microsoft Windows NT (аналогичен bat-файлу для DOS), OS/2;

dpl – упакованная библиотека Borland Delphi;

dll – библиотека динамической загрузки;

scr – файл-заставка экрана Microsoft Windows;

cpl – модуль панели управления (control panel) в Microsoft Windows;

ocx – объект Microsoft OLE (Object Linking and Embedding);

tsp – программа, работающая в режиме разделения времени;

drv – драйвер некоторого устройства;

vxd – драйвер виртуального устройства Microsoft Windows;

pif – файл с информацией о программе;

lnk – файл-ссылка в Microsoft Windows;

reg – файл регистрации ключей системного реестра Microsoft Windows;

ini – файл конфигурации, который содержит данные настроек для Microsoft Windows, Windows NT и некоторых программ;

cla – класс Java;

vbs – скрипт Visual Basic®;

vbe – видеорасширение BIOS;

js, jse – исходный текст JavaScript;

htm – гипертекстовый документ;

htt – гипертекстовая заготовка Microsoft Windows;

hta – гипертекстовая программа для Microsoft Internet Explorer®;

asp – скрипт Active Server Pages;

chm – скомпилированный HTML-файл;

pht – HTML-файл со встроенными скриптами PHP;

php – скрипт, встраиваемый в HTML-файлы;

wsh – файл Microsoft Windows Script Host;

wsf – скрипт Microsoft Windows;

the – файл заставки для рабочего стола Microsoft Windows 95;

hlp – файл справки формата Win Help;

eml – сообщение электронной почты Microsoft Outlook Express;

nws – новое сообщение электронной почты Microsoft Outlook Express;

msg – сообщение электронной почты Microsoft Mail;

plg – сообщение электронной почты;

mbx – сохраненное сообщение электронной почты Microsoft Office Outlook;

doc* – документы Microsoft Office Word, такие как: doc – документ Microsoft Office Word, docx – документ Microsoft Office Word 2007 с поддержкой языка XML, docm – документ Microsoft Office Word 2007 с поддержкой макросов;

dot* – шаблоны документа Microsoft Office Word, такие как: dot – шаблон документа Microsoft Office Word, dotx – шаблон документа Microsoft Office Word 2007, dotm – шаблон документа Microsoft Office Word 2007 с поддержкой макросов;

fpm – программа баз данных, стартовый файл Microsoft Visual FoxPro;

rtf – документ в формате Rich Text Format;

shs – фрагмент Windows Shell Scrap Object Handler;

dwg – база данных чертежей AutoCAD®;

msi – пакет Microsoft Windows Installer;

otm – VBA-проект для Microsoft Office Outlook;

pdf – документ Adobe Acrobat;

swf – объект пакета Shockwave® Flash;

jpg, jpeg – файл графического формата хранения сжатых изображений;

emf – файл формата Enhanced Metafile;

ico – файл значка объекта;

ov? – исполняемые файлы Microsoft Office Word;

xl* – документы и файлы Microsoft Office Excel, такие как: xla – расширение Microsoft Office Excel, xlc – диаграмма, xlt – шаблон документа, xlsx – рабочая книга Microsoft Office Excel 2007, xltm – рабочая книга Microsoft Office Excel 2007 с поддержкой макросов, xlsb – рабочая книга Microsoft Office Excel 2007 в бинарном (не XML) формате, xltx – шаблон Microsoft Office Excel 2007, xlsm – шаблон Microsoft Office Excel 2007 с поддержкой макросов, xlam – надстройка Microsoft Office Excel 2007 с поддержкой макросов;

pp* – документы и файлы Microsoft Office PowerPoint®, такие как: pps – слайд Microsoft Office PowerPoint, ppt – презентация, pptx – презентация Microsoft Office PowerPoint 2007, pptm – презентация Microsoft Office PowerPoint 2007 с поддержкой макросов, potx – шаблон презентации Microsoft Office PowerPoint 2007, potm – шаблон презентации Microsoft Office PowerPoint 2007 с поддержкой макросов, ppsx – слайд-шоу Microsoft Office PowerPoint 2007, ppsm – слайд-шоу Microsoft Office PowerPoint 2007 с поддержкой макросов, ppam – надстройка Microsoft Office PowerPoint 2007 с поддержкой макросов;

md* – документы и файлы Microsoft Office Access®, такие как: mda – рабочая группа Microsoft Office Access, mdb – база данных;

sldx – слайд Microsoft Office PowerPoint 2007;

sldm – слайд Microsoft Office PowerPoint 2007 с поддержкой макросов;

thmx – тема Microsoft Office 2007.

kaspersky

Приложение 4. Типы файлов для фильтра вложений Защиты от почтовых угроз

Следует помнить, что фактический формат файла может не совпадать с форматом, указанным в расширении файла.

Если вы включили фильтрацию вложений в сообщениях электронной почты, то в результате фильтрации компонент Защита от почтовых угроз может переименовывать или удалять файлы следующих расширений:

com – исполняемый файл программы размером не более 64 КБ;

exe – исполняемый файл, самораспаковывающийся архив;

sys – системный файл Microsoft Windows;

prg – текст программы dBase™, Clipper или Microsoft Visual FoxPro®, программа пакета WAVmaker;

bin – бинарный файл;

bat – файл пакетного задания;

cmd – командный файл Microsoft Windows NT (аналогичен bat-файлу для DOS), OS/2;

dpl – упакованная библиотека Borland Delphi;

dll – библиотека динамической загрузки;

scr – файл-заставка экрана Microsoft Windows;

cpl – модуль панели управления (control panel) в Microsoft Windows;

ocx – объект Microsoft OLE (Object Linking and Embedding);

tsp – программа, работающая в режиме разделения времени;

drv – драйвер некоторого устройства;

vxd – драйвер виртуального устройства Microsoft Windows;

pif – файл с информацией о программе;

lnk – файл-ссылка в Microsoft Windows;

reg – файл регистрации ключей системного реестра Microsoft Windows;

ini – файл конфигурации, который содержит данные настроек для Microsoft Windows, Windows NT и некоторых программ;

cla – класс Java;

vbs – скрипт Visual Basic®;

vbe – видеорасширение BIOS;

js, jse – исходный текст JavaScript;

htm – гипертекстовый документ;

htt – гипертекстовая заготовка Microsoft Windows;

hta – гипертекстовая программа для Microsoft Internet Explorer®;

asp – скрипт Active Server Pages;

chm – скомпилированный HTML-файл;

pht – HTML-файл со встроенными скриптами PHP;

php – скрипт, встраиваемый в HTML-файлы;

wsh – файл Microsoft Windows Script Host;

wsf – скрипт Microsoft Windows;

the – файл заставки для рабочего стола Microsoft Windows 95;

hlp – файл справки формата Win Help;

eml – сообщение электронной почты Microsoft Outlook Express;

nws – новое сообщение электронной почты Microsoft Outlook Express;

msg – сообщение электронной почты Microsoft Mail;

plg – сообщение электронной почты;

mbx – сохраненное сообщение электронной почты Microsoft Office Outlook;

doc* – документы Microsoft Office Word, такие как: doc – документ Microsoft Office Word, docx – документ Microsoft Office Word 2007 с поддержкой языка XML, docm – документ Microsoft Office Word 2007 с поддержкой макросов;

dot* – шаблоны документа Microsoft Office Word, такие как: dot – шаблон документа Microsoft Office Word, dotx – шаблон документа Microsoft Office Word 2007, dotm – шаблон документа Microsoft Office Word 2007 с поддержкой макросов;

fpm – программа баз данных, стартовый файл Microsoft Visual FoxPro;

rtf – документ в формате Rich Text Format;

shs – фрагмент Windows Shell Scrap Object Handler;

dwg – база данных чертежей AutoCAD®;

msi – пакет Microsoft Windows Installer;

otm – VBA-проект для Microsoft Office Outlook;

pdf – документ Adobe Acrobat;

swf – объект пакета Shockwave® Flash;

jpg, jpeg – файл графического формата хранения сжатых изображений;

emf – файл формата Enhanced Metafile;

ico – файл значка объекта;

ov? – исполняемые файлы Microsoft Office Word;

xl* – документы и файлы Microsoft Office Excel, такие как: xla – расширение Microsoft Office Excel, xlc – диаграмма, xlt – шаблон документа, xlsx – рабочая книга Microsoft Office Excel 2007, xltm – рабочая книга Microsoft Office Excel 2007 с поддержкой макросов, xlsb – рабочая книга Microsoft Office Excel 2007 в бинарном (не XML) формате, xltx – шаблон Microsoft Office Excel 2007, xlsm – шаблон Microsoft Office Excel 2007 с поддержкой макросов, xlam – надстройка Microsoft Office Excel 2007 с поддержкой макросов;

pp* – документы и файлы Microsoft Office PowerPoint®, такие как: pps – слайд Microsoft Office PowerPoint, ppt – презентация, pptx – презентация Microsoft Office PowerPoint 2007, pptm – презентация Microsoft Office PowerPoint 2007 с поддержкой макросов, potx – шаблон презентации Microsoft Office PowerPoint 2007, potm – шаблон презентации Microsoft Office PowerPoint 2007 с поддержкой макросов, ppsx – слайд-шоу Microsoft Office PowerPoint 2007, ppsm – слайд-шоу Microsoft Office PowerPoint 2007 с поддержкой макросов, ppam – надстройка Microsoft Office PowerPoint 2007 с поддержкой макросов;

md* – документы и файлы Microsoft Office Access®, такие как: mda – рабочая группа Microsoft Office Access, mdb – база данных;

sldx – слайд Microsoft Office PowerPoint 2007;

sldm – слайд Microsoft Office PowerPoint 2007 с поддержкой макросов;

thmx – тема Microsoft Office 2007.

Приложение 5. Сетевые параметры для взаимодействия с внешними службами

Kaspersky Endpoint Security использует следующие сетевые параметры для взаимодействия с внешними службами.

Таблица 14. Сетевые параметры

Описание	Протокол	Адрес	Порт
Активация программы	HTTPS	activation-v2.kaspersky.com/activationservice/activationservice.svc	443
Обновление баз и модулей программы	HTTPS	https://s00.upd.kaspersky.com https://s01.upd.kaspersky.com https://s02.upd.kaspersky.com https://s03.upd.kaspersky.com https://s04.upd.kaspersky.com https://s05.upd.kaspersky.com https://s06.upd.kaspersky.com https://s07.upd.kaspersky.com https://s08.upd.kaspersky.com https://s09.upd.kaspersky.com https://s10.upd.kaspersky.com https://s11.upd.kaspersky.com https://s12.upd.kaspersky.com https://s13.upd.kaspersky.com https://s14.upd.kaspersky.com https://s15.upd.kaspersky.com https://s16.upd.kaspersky.com https://s17.upd.kaspersky.com https://s18.upd.kaspersky.com https://s19.upd.kaspersky.com https://downloads.upd.kaspersky.com https://cm.k.kaspersky-labs.com	443

Описание	Протокол	Адрес	Порт
	HTTP	http://p00.upd.kaspersky.com http://p01.upd.kaspersky.com http://p02.upd.kaspersky.com http://p03.upd.kaspersky.com http://p04.upd.kaspersky.com http://p05.upd.kaspersky.com http://p06.upd.kaspersky.com http://p07.upd.kaspersky.com http://p08.upd.kaspersky.com http://p09.upd.kaspersky.com http://p10.upd.kaspersky.com http://p11.upd.kaspersky.com http://p12.upd.kaspersky.com http://p13.upd.kaspersky.com http://p14.upd.kaspersky.com http://p15.upd.kaspersky.com http://p16.upd.kaspersky.com http://p17.upd.kaspersky.com http://p18.upd.kaspersky.com http://p19.upd.kaspersky.com http://downloads.kaspersky-labs.com http://cm.k.kaspersky-labs.com	80
Использование Kaspersky Security Network	HTTPS	ds.kaspersky.com	443
	Any	ksn-a-stat-geo.kaspersky-labs.com ksn-file-geo.kaspersky-labs.com ksn-verdict-geo.kaspersky-labs.com ksn-url-geo.kaspersky-labs.com ksn-a-p2p-geo.kaspersky-labs.com ksn-info-geo.kaspersky-labs.com ksn-cinfo-geo.kaspersky-labs.com	443 1443
Переход по ссылкам из интерфейса	HTTPS	click.kaspersky.com redirect.kaspersky.com	
Инфраструктура открытых ключей (англ. Public Key Infrastructure – PKI)	HTTP	http://crl.kaspersky.com http://ocsp.kaspersky.com	80