KASPERSKY lab

Kaspersky Endpoint Security для Windows

Версия 11.0.0.6499

Подготовительные процедуры и руководство по эксплуатации

Уважаемый пользователь!

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

Дата редакции документа: 30.03.2018

Обозначение документа: 643.46856491.00100-01 90 01

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

Содержание

Об этом документе

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

Подготовительные процедуры изложены в разделах "Установка программы" 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.

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

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

Источники информации о программе

Перечисленные источники информации носят исключительно справочный характер и не являются заменой данного руководства.

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 на веб-сайте Службы технической поддержки (База знаний);
- электронная справка;
- документация.

Если вы не нашли решения возникшей проблемы самостоятельно, обратитесь в Службу технической поддержки "Лаборатории Касперского" (см. раздел "Обращение в Службу технической поддержки" на стр. 284).

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

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

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

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

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.

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;
- Microsoft® Internet Explorer® 7.0;
- Подключение к интернету для активации программы, обновления антивирусных баз программы;
- Процессор Intel Pentium 1 ГГц (или совместимый аналог);
- Оперативная память:
  - для 32-разрядной операционной системы - 1 ГБ;
  - для 64-разрядной операционной системы - 2 ГБ.

Поддерживаемые операционные системы для рабочих станций:

- Microsoft Windows 7 Professional / Enterprise / Ultimate x86 Edition SP1, Microsoft Windows 7 Professional / Enterprise / Ultimate x64 Edition SP1;
- Microsoft Windows 8 Professional / Enterprise x86 Edition, Microsoft Windows 8 Professional / Enterprise x64 Edition, Microsoft Windows 8.1 Enterprise x86 Edition, Microsoft Windows 8.1 Enterprise x64 Edition;
- Microsoft Windows 10 Pro / Enterprise x86 Edition, Microsoft Windows 10 Pro / Enterprise x64 Edition.

Особенности поддержки операционной системы Microsoft Windows 10 вы можете узнать в статье 13036 базы знаний Службы технической поддержки: http://support.kaspersky.ru/kes11.

Поддерживаемые операционные системы для файловых серверов:

- Microsoft Windows Server 2008 R2 Standard / Enterprise x64 Edition SP1, Microsoft Windows Server 2008 Standard / Enterprise x86 Edition SP2, Microsoft Windows Server 2008 Standard / Enterprise x64 Edition SP2;
- Microsoft Windows Small Business Server 2011 Essentials / Standard x64 Edition;

- Microsoft Windows Server 2012 Standard / Foundation / Essentials x64 Edition, Microsoft Windows Server 2012 R2 Standard / Foundation / Essentials x64 Edition, Microsoft Windows MultiPoint Server 2012 x64 Edition;
- Microsoft Windows Server 2016.

Особенности поддержки операционной системы Microsoft Windows Server 2016 вы можете узнать в статье 13036 базы знаний Службы технической поддержки: http://support.kaspersky.ru/kes11.

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.

Установка программы

Этот раздел содержит информацию о том, как установить Kaspersky Endpoint Security на компьютер и выполнить первоначальную настройку программы.

В этом разделе

О способах установки программы

Kaspersky Endpoint Security для Windows можно установить локально (непосредственно на компьютере пользователя) или удаленно с рабочего места администратора.

Локальную установку Kaspersky Endpoint Security для Windows можно выполнить в одном из следующих режимов:

- В интерактивном режиме с помощью мастера установки программы.

  Интерактивный режим требует вашего участия в процессе установки.

- В тихом режиме из командной строки (см. раздел "Установка программы из командной строки" на стр. 24).

  После запуска установки в тихом режиме ваше участие в процессе установки не требуется.

Удаленную установку программы на компьютеры сети можно выполнить с использованием:

- программного комплекса Kaspersky Security Center (см. *Руководство по внедрению Kaspersky Security Center*);
- редактора управления групповыми политиками Microsoft Windows (см. сопроводительную документацию для операционной системы);
- System Center Configuration Manager.

Перед началом установки Kaspersky Endpoint Security (в том числе удаленной) рекомендуется закрыть все работающие программы.

Установка программы с помощью мастера установки программы

Интерфейс мастера установки программы состоит из последовательности окон, соответствующих шагам установки программы. Чтобы переключаться между окнами мастера установки программы, требуется использовать кнопки **Назад** и **Далее**. Работа мастера установки программы завершается нажатием на кнопку **Завершить**. Чтобы прекратить работу мастера установки программы на любом этапе, можно нажать на кнопку **Отмена**.

► *Чтобы установить программу или обновить предыдущую версию программы с помощью мастера установки программы, выполните следующие действия:*

1. Запустите файл setup_kes.exe, входящий в комплект поставки.

   Запустится мастер установки программы.

2. Следуйте указаниям мастера установки программы.

После запуска файла setup.exe Kaspersky Endpoint Security проверяет, есть ли на компьютере несовместимое программное обеспечение. По умолчанию при его обнаружении установка прерывается и на экране отображается список найденных программ, несовместимых с Kaspersky Endpoint Security. Чтобы продолжить установку, требуется удалить с компьютера эти программы.

В этом разделе

Шаг 1. Проверка соответствия системы необходимым условиям установки

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

- соответствие операционной системы и пакета обновлений (Service Pack) программным требованиям для установки;
- 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 для Windows, а предыдущая версия программы автоматически удаляется. Это относится к следующим версиям программы:

- Kaspersky Endpoint Security 10 для Windows (Service Pack 1 – сборка 10.2.2.10535).
- Kaspersky Endpoint Security 10 для Windows (Service Pack 1 Maintenance Release 1 – сборка 10.2.2.10535).
- Kaspersky Endpoint Security 10 для Windows (Service Pack 1 Maintenance Release 2– сборка 10.2.4.674).
- Kaspersky Endpoint Security 10 для Windows (Service Pack 1 Maintenance Release 3 – сборка 10.2.5.3201).
- Kaspersky Endpoint Security 10 для Windows (Service Pack 1 Maintenance Release 4 – сборка 10.2.6.3733).
- Kaspersky Endpoint Security 10 для Windows (Service Pack 2 – сборка 10.3.0.6294).

Шаг 2. Стартовое окно процедуры установки

Если условия для установки программы полностью соответствуют предъявляемым требованиям, после запуска установочного пакета на экране открывается стартовое окно. Стартовое окно содержит информацию о начале установки Kaspersky Endpoint Security на компьютер.

Чтобы продолжить работу мастера установки программы, нажмите на кнопку **Далее**.

Шаг 3. Просмотр Лицензионного соглашения и Политики конфиденциальности

На этом шаге мастера установки требуется ознакомиться с Лицензионным соглашением, которое заключается между вами и "Лабораторией Касперского", и Политикой конфиденциальности.

Внимательно прочитайте Лицензионное соглашение и Политику конфиденциальности. Если вы согласны со всеми пунктами Лицензионного соглашения и Политики конфиденциальности, в блоке **Я подтверждаю, что полностью прочитал, понимаю и принимаю** установите флажки:

- **положения и условия настоящего Лицензионного соглашения**;
- **Политику конфиденциальности, которая описывает обработку данных**.

Установка программы на ваше устройство будет продолжена после установки обоих флажков.

Если вы не согласны с Лицензионным соглашением и Политикой конфиденциальности, то отмените установку программы, нажав на кнопку **Отмена**.

Шаг 4. Выбор типа установки

На этом шаге вы можете выбрать подходящий тип установки Kaspersky Endpoint Security:

- **Базовая установка**. Если вы выбираете этот тип установки, на компьютер пользователя устанавливаются все компоненты защиты, кроме компонента Защита от атак BadUSB, с параметрами, рекомендуемыми специалистами "Лаборатории Касперского".
- **Стандартная установка**. Если вы выбираете этот тип установки, на компьютер пользователя устанавливаются все компоненты защиты, кроме компонента Защита от атак BadUSB, и компоненты контроля с параметрами, рекомендуемыми специалистами "Лаборатории Касперского".
- **Выборочная установка**. Если вы выбираете этот тип установки, вам предлагается выбрать компоненты для установки и указать папку, в которую будет установлена программа (см. раздел "Шаг 6. Выбор папки для установки программы" на стр. 22). Этот тип установки используется для установки сертифицированной конфигурации программы.

  С помощью этого типа установки вы можете установить компоненты, которые не включены в базовую и стандартную установки.

По умолчанию выбрана стандартная установка.

Чтобы вернуться к предыдущему шагу мастера установки программы, нажмите на кнопку **Назад**. Чтобы продолжить работу мастера установки программы, нажмите на кнопку **Далее**. Чтобы прекратить работу мастера установки программы, нажмите на кнопку **Отмена**.

Шаг 5. Выбор компонентов программы для установки

Этот шаг выполняется, если вы выбрали *Выборочную установку* программы.

На этом шаге вы можете выбрать компоненты Kaspersky Endpoint Security, которые вы хотите установить. Компонент Защита от файловых угроз является обязательным компонентом для установки. Вы не можете отменить его установку.

Для установки сертифицированной конфигурации программы Kaspersky Endpoint Security необходимо исключить установку компонентов Сетевой экран и Контроль устройств.

По умолчанию для установки выбраны все компоненты программы, кроме следующих компонентов:

- Защита от атак BadUSB (на стр. 121).
- Шифрование файлов.
- Полнодисковое шифрование.
- Управление BitLocker.
- Endpoint Sensor (на стр. 172).

Управление BitLocker выполняет следующие функции:

- управление встроенным в операционную систему Windows шифрованием BitLocker;

- настройка шифрования в параметрах политики Kaspersky Security Center и проверка их применимости для управляемого компьютера;
- запуск процессов шифрования и расшифровки;
- мониторинг состояния шифрования на управляемом компьютере;
- централизованное хранение ключей восстановления на Сервере администрирования Kaspersky Security Center.

Endpoint Sensor является компонентом Kaspersky Anti Targeted Attack Platform. Это решение предназначено для своевременного обнаружения таких угроз, как целевые атаки. Компонент постоянно наблюдает за процессами, открытыми сетевыми соединениями и изменяемыми файлами и передает эту информацию в Kaspersky Anti Targeted Attack Platform.

Чтобы выбрать компонент для последующей установки, по левой клавише мыши откройте контекстное меню значка рядом с названием компонента и выберите пункт **Компонент будет установлен на локальный жесткий диск**. Подробную информацию о том, какие задачи выполняет выбранный компонент и сколько места на жестком диске требуется для установки компонента, вы можете посмотреть в нижней части текущего окна мастера установки программы.

Чтобы узнать подробную информацию о свободном месте на жестких дисках компьютера, нажмите на кнопку **Диск**. Информация будет отображена в открывшемся окне **Доступное дисковое пространство**.

Для отказа от установки компонента в контекстном меню выберите пункт **Компонент будет недоступен**.

Чтобы вернуться к списку компонентов, устанавливаемых по умолчанию, нажмите на кнопку **Сброс**.

Чтобы вернуться к предыдущему шагу мастера установки программы, нажмите на кнопку **Назад**. Чтобы продолжить работу мастера установки программы, нажмите на кнопку **Далее**. Чтобы прекратить работу мастера установки программы, нажмите на кнопку **Отмена**.

Шаг 6. Выбор папки для установки программы

Этот шаг доступен, если вы выбрали *Выборочную установку* программы.

На этом шаге вы можете указать путь к папке назначения, в которую будет установлена программа. Для выбора папки для установки программы нажмите на кнопку **Обзор**.

Для просмотра информации о свободном месте на жестких дисках компьютера, нажмите на кнопку **Диск**. Информация будет предоставлена в открывшемся окне **Доступное дисковое пространство**.

Чтобы вернуться к предыдущему шагу мастера установки программы, нажмите на кнопку **Назад**. Чтобы продолжить работу мастера установки программы, нажмите на кнопку **Далее**. Чтобы прекратить работу мастера установки программы, нажмите на кнопку **Отмена**.

Шаг 7. Добавление исключений из проверки

Этот шаг доступен, если вы выбрали *Выборочную установку* программы.

На этом шаге вы можете указать, какие исключения из проверки требуется добавить в параметры программы.

Флажок **Исключить из проверки области, рекомендованные компанией Microsoft** / **Исключить из проверки области, рекомендованные компанией "Лаборатория Касперского"** включает / исключает из доверенной зоны области, рекомендованные компанией Microsoft / "Лаборатория Касперского".

Если флажок установлен, то Kaspersky Endpoint Security включает области, рекомендованные компанией Microsoft / "Лаборатория Касперского", в доверенную зону. Такие области Kaspersky Endpoint Security не проверяет на наличие вирусов и других программ, представляющих угрозу.

Флажок **Исключить из проверки области, рекомендованные компанией Microsoft** доступен при установке Kaspersky Endpoint Security на компьютер под управлением операционной системы Microsoft Windows для файловых серверов.

Чтобы вернуться к предыдущему шагу мастера установки программы, нажмите на кнопку **Назад**. Чтобы продолжить работу мастера установки программы, нажмите на кнопку **Далее**. Чтобы прекратить работу мастера установки программы, нажмите на кнопку **Отмена**.

Шаг 8. Подготовка к установке программы

Процесс установки рекомендуется защищать, поскольку на компьютере могут присутствовать вредоносные программы, способные помешать установке Kaspersky Endpoint Security для Windows.

По умолчанию защита процесса установки включена.

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). В этом случае прервите установку и запустите мастер установки программы заново. На шаге «Подготовка к установке программы» снимите флажок **Защитить процесс установки**.

Флажок **Обеспечить совместимость с Citrix PVS** включает / выключает функцию, которая выполняет установку драйверов в режиме совместимости с Citrix PVS.

Установите этот флажок, только если вы работаете с технологией Citrix Provisioning Services.

Флажок **Добавить путь к файлу avp.com в системную переменную %PATH%** включает / выключает функцию, которая добавляет в системную переменную %PATH% путь к файлу avp.com.

Если флажок установлен, то для запуска Kaspersky Endpoint Security или любых задач программы из командной строки не требуется вводить путь к исполняемому файлу. Достаточно ввести имя исполняемого файла и команду для запуска соответствующей задачи.

Чтобы вернуться к предыдущему шагу мастера установки программы, нажмите на кнопку **Назад**. Для установки программы нажмите на кнопку **Установить**. Чтобы прекратить работу мастера установки программы, нажмите на кнопку **Отмена**.

Во время установки программы на компьютер возможен разрыв текущих сетевых соединений. Большинство разорванных сетевых соединений восстанавливается после завершения установки программы.

Шаг 9. Установка программы

Установка программы занимает некоторое время. Дождитесь ее завершения.

Если вы выполняете обновление предыдущей версии программы, то на этом шаге также выполняется миграция параметров и удаление предыдущей версии программы.

После завершения установки Kaspersky Endpoint Security запускается мастер первоначальной настройки программы (на стр. 32).

Установка программы из командной строки

Из командной строки вы можете запустить установку программы в интерактивном или тихом режиме.

Также при установке программы из командной строки вы можете настроить имя пользователя и пароль для доступа к программе. Программа будет запрашивать имя пользователя и пароль при попытке пользователя удалить или остановить ее, а также изменить ее параметры.

► *Чтобы запустить мастер установки программы из командной строки,*

введите в командной строке `setup.exe` или `msiexec /i <название дистрибутива>`.

► *Чтобы установить программу или обновить версию программы в тихом режиме (без запуска мастера установки программы),*

введите в командной строке `setup.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=1|0 /pINSTALLLEVEL=<значение> /pALLOWREBOOT=1|0 /pSKIPPRODUCTCHECK=1|0 /pSKIPPRODUCTUNINSTALL=1|0 /s`

или

`msiexec /i <название дистрибутива> EULA=1 PRIVACYPOLICY=1 KSN=1|0 INSTALLLEVEL=<значение> ALLOWREBOOT=1|0 ADDLOCAL=<значение> SKIPPRODUCTCHECK=1|0 SKIPPRODUCTUNINSTALL=1|0 /qn`,

где:

- `EULA=1` означает, что вы принимаете положения Лицензионного соглашения. Текст Лицензионного соглашения входит в комплект поставки Kaspersky Endpoint Security. Согласие с положениями Лицензионного соглашения является необходимым условием для установки программы или обновления версии программы. Если значение этого параметра не указано при установке в тихом режиме, программа не будет установлена.
- `PRIVACYPOLICY=1` означает, что вы принимаете Положение о конфиденциальности. Текст Положения о конфиденциальности входит в комплект поставки Kaspersky Endpoint Security.

Согласие с Положением о конфиденциальности является необходимым условием для установки программы или обновления версии программы. Если значение этого параметра не указано при установке в тихом режиме, программа не будет установлена.

- KSN=1|0 означает согласие (1) или отказ (0) участвовать в программе Kaspersky Security Network (далее также "KSN"). Текст Положения о Kaspersky Security Network входит в комплект поставки Kaspersky Endpoint Security. Указание значения параметра необязательно. Если в команде не указано значение параметра KSN, то при первом запуске Kaspersky Endpoint Security откроется окно с запросом на участие в программе KSN.

  Дистрибутив Kaspersky Endpoint Security оптимизирован для использования Kaspersky Security Network. Если вы отказались от участия в Kaspersky Security Network, то сразу после завершения установки обновите Kaspersky Endpoint Security.

- INSTALLLEVEL=<значение> указывает на тип установки Kaspersky Endpoint Security (см. раздел "Шаг 4. Выбор типа установки" на стр. 21). Указание значения параметра необязательно. Если в команде не указано значение параметра INSTALLLEVEL, по умолчанию выполняется стандартная установка программы.

  Вместо <значение> вы можете указать следующие значения параметра INSTALLLEVEL:

  - 100. Выполняется базовая установка программы.
  - 200. Выполняется стандартная установка программы.
  - 300. Выполняется установка всех компонентов программы.

- ALLOWREBOOT=1|0 означает согласие (1) или запрет (0) на автоматическую перезагрузку компьютера, если она потребуется после установки или обновления программы. Указание значения параметра необязательно. Если в команде не указано значение параметра ALLOWREBOOT, по умолчанию автоматическая перезагрузка компьютера после установки или обновления программы запрещена.

  Перезагрузка компьютера может понадобиться после обновления версии программы или в случае, если во время установки Kaspersky Endpoint Security обнаружено и удалено стороннее антивирусное программное обеспечение.

  Автоматическая перезагрузка компьютера может быть выполнена только в режиме тихой установки (с ключом /qn).

- ADDLOCAL=<значение> указывает, какие компоненты должны быть установлены дополнительно к компонентам, выбранным по умолчанию в режиме стандартной установки. Указание значения параметра необязательно.

  Вместо <значение> вы можете указать следующие значения параметра ADDLOCAL:

  - MSBitLockerFeature. Выполняется установка компонента Microsoft BitLocker Manager.
  - AntiAPTFeature. Выполняется установка компонента Endpoint Sensor.

- SKIPPRODUCTCHECK=1|0 означает включение (1) или выключение (0) проверки на наличие несовместимого программного обеспечения. Указание значения параметра необязательно. Если в

команде не указано значение параметра SKIPPRODUCTCHECK, Kaspersky Endpoint Security проводит проверку.

- SKIPPRODUCTUNINSTALL=1|0 означает согласие (1) или запрет (0) на автоматическое удаление найденных программ, несовместимых с Kaspersky Endpoint Security. Указание значения параметра необязательно. Если в команде не указано значение параметра SKIPPRODUCTUNINSTALL, по умолчанию Kaspersky Endpoint Security пытается удалить все найденные несовместимые программы.

► *Чтобы установить программу или обновить версию программы с установкой имени пользователя и пароля, подтверждающих право на изменение параметров программы и операции с программой, выполните следующие действия:*

- Если вы хотите установить программу или обновить версию программы в интерактивном режиме, введите в командной строке следующую команду:

  ```
  setup.exe /pKLLOGIN=<Имя пользователя> /pKLPASSWD=***** /pKLPASSWDAREA=<область действия пароля>
  ```

  или

  ```
  msiexec /i <название дистрибутива> KLLOGIN=<Имя пользователя> KLPASSWD=***** KLPASSWDAREA=<область действия пароля>.
  ```

- Если вы хотите установить программу или обновить версию программы в тихом режиме, введите в командной строке следующую команду:

  ```
  setup.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=1|0 /pINSTALLLEVEL=<значение> /pKLLOGIN=<Имя пользователя> /pKLPASSWD=***** /pKLPASSWDAREA=<область действия пароля> /s
  ```

  или

  ```
  msiexec /i <название дистрибутива> EULA=1 PRIVACYPOLICY=1 KSN=1|0 INSTALLLEVEL=<значение> KLLOGIN=<Имя пользователя> KLPASSWD=***** KLPASSWDAREA=<область действия пароля> ALLOWREBOOT=1|0/qn.
  ```

Вместо <область действия пароля> вы можете указать одно или несколько из следующих значений параметра KLPASSWDAREA (через точку с запятой), соответствующих операциям, для которых требуется подтверждение:

- SET. Изменение параметров программы.
- EXIT. Завершение работы программы.
- DISPROTECT. Выключение компонентов защиты и остановка задач проверки.
- DISPOLICY. Выключение политики Kaspersky Security Center.
- DISCTRL. Выключение компонентов контроля.
- REMOVELIC. Удаление ключа.
- UNINST. Удаление, изменение или восстановление программы.
- REPORTS. Просмотр отчетов.

Во время установки программы или обновления версии программы в тихом режиме поддерживается использование следующих файлов:

- setup.ini (см. раздел "Описание параметров установки в файле setup.ini" на стр. 28), содержащего общие параметры установки программы;
- конфигурационного файла install.cfg (см. раздел "Создание и использование конфигурационного файла" на стр. 241), содержащего параметры работы Kaspersky Endpoint Security;
- setup.reg, содержащего ключи реестра.

Файлы setup.ini, install.cfg и setup.reg должны быть расположены в одной папке с дистрибутивом Kaspersky Endpoint Security для Windows.

Удаленная установка программы с помощью System Center Configuration Manager

Инструкция актуальна для версии System Center Configuration Manager 2012 R2.

► *Чтобы удаленно установить программу с помощью System Center Configuration Manager, выполните следующие действия:*

1. Откройте консоль Configuration Manager.
2. В правой части консоли в блоке **Управление приложениями** выберите раздел **Пакеты**.
3. В верхней части консоли в панели управления нажмите на кнопку **Создать пакет**.

   Запустится *мастер создания пакетов и программ*.
4. В мастере создания пакетов и программ выполните следующие действия:
   a. В разделе **Пакет** выполните следующие действия:
      - В поле **Имя** введите имя инсталляционного пакета.
      - В поле **Исходная папка** укажите путь к папке, в которой расположен дистрибутив Kaspersky Endpoint Security.
   b. В разделе **Тип программы** выберите вариант **Стандартная программа**.
   c. В разделе **Стандартная программа** выполните следующие действия:
      - В поле **Имя** введите уникальное имя инсталляционного пакета (например, название программы с указанием версии).
      - В поле **Командная строка** укажите параметры установки Kaspersky Endpoint Security из командной строки.
      - По кнопке **Обзор** задайте путь к исполняемому файлу программы.

- Убедитесь, что в раскрывающемся списке **Режим выполнения** выбран элемент **Запустить с правами администратора**.

d. В разделе **Требования** выполните следующие действия:

- Установите флажок **Запустить сначала другую программу**, если вы хотите, чтобы перед установкой Kaspersky Endpoint Security была запущена другая программа.

  Выберите программу из раскрывающегося списка **Программа** или укажите путь к исполняемому файлу этой программы по кнопке **Обзор**.

- Выберите вариант **Эту программу можно запускать только на указанных платформах** в блоке **Требования к платформе**, если вы хотите, чтобы программа была установлена только в указанных операционных системах.

  В списке ниже установите флажки напротив тех операционных систем, в которых должен быть установлен Kaspersky Endpoint Security.

Этот шаг является необязательным.

e. В разделе **Сводка** проверьте все заданные значения параметров и нажмите на кнопку **Далее**.

Созданный инсталляционный пакет появится в разделе **Пакеты** в списке доступных инсталляционных пакетов.

5. В контекстном меню инсталляционного пакета выберите пункт **Развернуть**.

   Запустится *мастер развертывания программного обеспечения*.

6. В мастере развертывания программного обеспечения выполните следующие действия:

   a. В разделе **Общие** выполните следующие действия:

   - В поле **Программное обеспечение** введите уникальное имя инсталляционного пакета или выберите инсталляционный пакет из списка по кнопке **Обзор**.
   - В поле **Коллекция** введите название коллекции компьютеров, на которые должна быть установлена программа, или выберите эту коллекцию по кнопке **Обзор**.

   b. В разделе **Содержимое** добавьте точки распространения (более подробную информацию вы можете найти в сопроводительной документации для System Center Configuration Manager).

   c. Если требуется, укажите значения других параметров в мастере развертывания программного обеспечения. Эти параметры являются необязательными для удаленной установки Kaspersky Endpoint Security.

   d. В разделе **Сводка** проверьте все заданные значения параметров и нажмите на кнопку **Далее**.

   После завершения работы мастера развертывания программного обеспечения будет создана задача по удаленной установке Kaspersky Endpoint Security.

Описание параметров установки в файле setup.ini

Файл setup.ini используется при установке программы из командной строки или с помощью редактора управления групповыми политиками Microsoft Windows Server. Файл setup.ini располагается в папке с дистрибутивом Kaspersky Endpoint Security.

Файл setup.ini содержит следующие параметры:

1. [Setup] - общие параметры установки программы:

- `InstallDir` - путь к папке установки программы.
- `ActivationCode` - код активации Kaspersky Endpoint Security.
- `Eula` - согласие или несогласие с положениями Лицензионного соглашения. Возможные значения параметра `Eula`:
  - `1`. Согласие с положениями Лицензионного соглашения.
  - `0`. Несогласие с положениями Лицензионного соглашения.
- `PrivacyPolicy` - согласие или несогласие с Положением о конфиденциальности. Возможные значения параметра `PrivacyPolicy`:
  - `1`. Согласие с Положением о конфиденциальности.
  - `0`. Несогласие с Положением о конфиденциальности.

  Текст Положения о конфиденциальности входит в комплект поставки Kaspersky Endpoint Security. Согласие с Положением о конфиденциальности является необходимым условием для установки программы или обновления версии программы.
- `KSN` - согласие или отказ участвовать в Kaspersky Security Network. Возможные значения параметра `KSN`:
  - `1`. Согласие участвовать в Kaspersky Security Network.
  - `0`. Отказ участвовать в Kaspersky Security Network.

  Комплект поставки Kaspersky Endpoint Security оптимизирован для использования Kaspersky Security Network. Если вы отказались от участия в Kaspersky Security Network, то сразу после завершения установки обновите Kaspersky Endpoint Security.
- `Login` - установка имени пользователя для доступа к управлению функциями и параметрами Kaspersky Endpoint Security (имя пользователя устанавливается вместе с параметрами `Password` и `Password Area`).
- `Password` - установка пароля для доступа к управлению функциями и параметрами Kaspersky Endpoint Security (пароль устанавливается вместе с параметрами `Login` и `Password Area`).

  Если вы указали пароль, но не задали имя пользователя с помощью параметра `Login`, то по умолчанию используется имя пользователя KLAdmin.
- `PasswordArea` - определение области действия пароля для доступа к управлению функциями и параметрами Kaspersky Endpoint Security. Возможные значения параметра `PasswordArea`, соответствующие операциям, для которых требуется подтверждение:
  - `SET`. Изменение параметров программы.
  - `EXIT`. Завершение работы программы.
  - `DISPROTECT`. Выключение компонентов защиты и остановка задач проверки.

- DISPOLICY. Выключение политики Kaspersky Security Center.
- UNINST. Удаление программы с компьютера.
- DISCTRL. Выключение компонентов контроля.
- REMOVELIC. Установка пароля на удаление ключа.
- REPORTS. Установка пароля на просмотр отчетов.

- SelfProtection - включение или выключение механизма защиты установки программы. Возможные значения параметра SelfProtection:
  - 1. Механизм защиты установки программы включен.
  - 0. Механизм защиты установки программы выключен.
- Reboot - необходимость перезагрузки компьютера по завершении установки программы. Возможные значения параметра Reboot:
  - 1. Перезагрузка компьютера по завершении установки программы выполняется.
  - 0. Перезагрузка компьютера по завершении установки программы не выполняется.
- MSExclusions - добавление программ, рекомендованных компанией Microsoft, в исключения из проверки.

  Параметр доступен только для файловых серверов, управляемых операционной системой Microsoft Windows Server.

  Возможные значения параметра MSExclusions:
  - 1. Программы, рекомендованные компанией Microsoft, добавляются в исключения из проверки.
  - 0. Программы, рекомендованные компанией Microsoft, не добавляются в исключения из проверки.
- KLExclusions - добавление программ, рекомендованных компанией "Лаборатория Касперского", в исключения из проверки. Возможные значения параметра KLExclusions:
  - 1. Программы, рекомендованные компанией "Лаборатория Касперского", добавляются в исключения из проверки.
  - 0. Программы, рекомендованные компанией "Лаборатория Касперского", не добавляются в исключения из проверки.
- AddEnvironment - добавление в системную переменную %PATH% пути к исполняемым файлам, расположенным в папке установки Kaspersky Endpoint Security. Возможные значения параметра AddEnvironment:
  - 1. В системную переменную %PATH% добавляется путь к исполняемым файлам, расположенным в папке установки Kaspersky Endpoint Security.
  - 0. В системную переменную %PATH% не добавляется путь к исполняемым файлам, расположенным в папке установки Kaspersky Endpoint Security.

2. [Components] - выбор компонентов программы для установки:

- `ALL` - установка всех компонентов.

  > Если указано значение параметра 1, все компоненты будут установлены независимо от параметров установки отдельных компонентов.

- `MailThreatProtection` - установка компонента Защита от почтовых угроз.
- `WebThreatProtection` - установка компонента Защита от веб-угроз.
- `HostIntrusionPrevention` - установка компонента Предотвращение вторжений.
- `BehaviorDetection` - установка компонента Анализ поведения.
- `ExploitPrevention` - установка компонента Защита от эксплойтов.
- `RemediationEngine` - установка компонента Откат вредоносных действий.
- `NetworkThreatProtection` - установка компонента Защита от сетевых угроз.
- `WebControl` - установка компонента Веб-Контроль.
- `DeviceControl` - установка компонента Контроль устройств.
- `ApplicationControl` - установка компонента Контроль программ.
- `FileEncryption` - установка библиотек для шифрования файлов.
- `DiskEncryption` - установка библиотек для полнодискового шифрования.
- `BadUSBAttackPrevention` - установка компонента Защита от атак BadUSB.
- `AntiAPT` - установка компонента Endpoint Sensor.
- `MSBitLocker` - установка компонента Microsoft BitLocker Manager.
- `AdminKitConnector` - установка коннектора к Агенту администрирования для удаленного управления программой через Kaspersky Security Center.

  Возможные значения параметра установки коннектора:

  - `1`. Коннектор к Агенту администрирования устанавливается.
  - `0`. Коннектор к Агенту администрирования не устанавливается.

Если не указан ни один из компонентов, то устанавливаются все доступные для операционной системы компоненты.

Защита от файловых угроз является обязательным компонентом и устанавливается на компьютер независимо от того, какие параметры указаны в этом блоке.

3. [Tasks] - выбор задач для включения в список задач Kaspersky Endpoint Security:

   - `ScanMyComputer` - задача полной проверки.
   - `ScanCritical` - задача проверки важных областей.
   - `Updater` - задача обновления.

   Возможные значения параметров:

   - `1`. Задача включается в список задач Kaspersky Endpoint Security.

- `0`. Задача не включается в список задач Kaspersky Endpoint Security.

Если не указана ни одна задача, все задачи включаются в список задач Kaspersky Endpoint Security.

Вместо значения `1` могут использоваться значения `yes`, `on`, `enable`, `enabled`. Вместо значения `0` могут использоваться значения `no`, `off`, `disable`, `disabled`.

Мастер первоначальной настройки программы

Мастер первоначальной настройки Kaspersky Endpoint Security запускается в конце процедуры установки программы. Мастер первоначальной настройки программы позволяет активировать программу и получает информацию о программах, входящих в состав операционной системы. Эти программы попадают в список доверенных программ, которые не имеют ограничений на действия, совершаемые в операционной системе.

Интерфейс мастера первоначальной настройки программы состоит из последовательности окон (шагов). Чтобы переключаться между окнами мастера первоначальной настройки программы, требуется использовать кнопки **Назад** и **Далее**. Завершение работы мастера первоначальной настройки программы осуществляется при помощи кнопки **Завершить**. Для прекращения работы мастера первоначальной настройки программы на любом этапе служит кнопка **Отмена**.

Если по каким-либо причинам работа мастера первоначальной настройки программы прерывается, то уже заданные значения параметров не сохраняются. Далее при попытке начать работу с программой мастер первоначальной настройки программы запускается вновь, и вам требуется заново настроить параметры.

В этом разделе

Шаг 1. Активация 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.

На этом шаге выберите вариант активации Kaspersky Endpoint Security **Активировать с помощью файла ключа** и нажмите на кнопку **Далее**. Чтобы прекратить работу мастера первоначальной настройки программы, нажмите на кнопку **Отмена**.

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

Шаг 3. Активация с помощью файла ключа

Этот шаг доступен только при активации программы с помощью файла ключа.

На этом шаге требуется указать путь к файлу ключа. Для этого нажмите на кнопку **Обзор** и выберите файл ключа, имеющий вид `<ID файла>.key`.

После того как вы выбрали файл ключа, в нижней части окна отобразится следующая информация:

- ключ;
- тип лицензии (коммерческая или пробная) и количество компьютеров, на которые эта лицензия распространяется;
- дата активации программы на компьютере;
- дата окончания срока действия лицензии;
- функциональность программы, которая доступна по лицензии;
- сообщение о каких-либо проблемах, связанных с ключом (при их наличии). Например, *Поврежден черный список ключей*.

Чтобы вернуться к предыдущему шагу мастера первоначальной настройки программы, нажмите на кнопку **Назад**. Чтобы продолжить работу мастера первоначальной настройки программы, нажмите на кнопку **Далее**. Чтобы прекратить работу мастера первоначальной настройки программы, нажмите на кнопку **Отмена**.

Шаг 4. Выбор активируемой функциональности

Этот шаг доступен только при активации пробной версии программы.

На этом шаге предлагается выбрать, какая функциональность будет доступна после активации программы:

- **Базовая установка**. Если выбран этот вариант, то после активации программы будут доступны только компоненты защиты и компонент Предотвращение вторжений.
- **Стандартная установка**. Если выбран этот вариант, то после активации программы будут доступны компоненты защиты и контроля.
- **Полная установка**. Если выбран этот вариант, то после активации программы будут доступны все установленные компоненты программы, включая функциональность шифрования данных.

Если на этапе установки вы выбрали больше компонентов, чем допускает приобретенная лицензия, то после активации программы недоступные по лицензии компоненты будут установлены, но не будут работать. Если приобретенная лицензия допускает больший набор компонентов, чем установлено, то после активации программы о неустановленных компонентах программы будет указано в окне **Лицензирование**.

По умолчанию выбрана стандартная установка.

Чтобы вернуться к предыдущему шагу мастера первоначальной настройки программы, нажмите на кнопку **Назад**. Чтобы продолжить работу мастера первоначальной настройки программы, нажмите на кнопку **Далее**. Чтобы прекратить работу мастера первоначальной настройки программы, нажмите на кнопку **Отмена**.

Шаг 5. Завершение активации программы

На этом шаге мастер первоначальной настройки программы информирует вас об успешном завершении активации Kaspersky Endpoint Security. Кроме того, приводится информация о лицензии:

- тип лицензии (коммерческая или пробная) и количество компьютеров, на которые эта лицензия распространяется;
- дата окончания срока действия лицензии;
- функциональность программы, которая доступна по лицензии.

Чтобы продолжить работу мастера первоначальной настройки программы, нажмите на кнопку **Далее**. Чтобы прекратить работу мастера первоначальной настройки программы, нажмите на кнопку **Отмена**.

Шаг 6. Завершение первоначальной настройки программы

Окно завершения мастера первоначальной настройки содержит информацию об окончании процесса установки Kaspersky Endpoint Security.

Если вы хотите запустить Kaspersky Endpoint Security, нажмите на кнопку **Завершить**.

Если вы хотите выйти из мастера первоначальной настройки программы без последующего запуска Kaspersky Endpoint Security, снимите флажок **Запустить Kaspersky Endpoint Security для Windows** и нажмите на кнопку **Завершить**.

Шаг 7. Анализ операционной системы

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

Анализ других программ происходит после первого их запуска после установки Kaspersky Endpoint Security.

Чтобы прекратить работу мастера первоначальной настройки программы, нажмите на кнопку **Отмена**.

Шаг 8. Соглашение об участии в Kaspersky Security Network

На этом шаге вам предлагается принять участие в Kaspersky Security Network.

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

Ознакомьтесь с «Положением о Kaspersky Security Network»:

- Если вы согласны со всеми его пунктами, в окне мастера первоначальной настройки программы выберите вариант **Я принимаю условия использования Kaspersky Security Network**.
- Если вы не согласны с условиями участия в Kaspersky Security Network, в окне мастера первоначальной настройки программы выберите вариант **Я не принимаю условия использования Kaspersky Security Network**.

Чтобы продолжить работу мастера первоначальной настройки программы, нажмите на кнопку **ОК**.

О способах обновления предыдущей версии программы

Для обновления предыдущей версии программы до Kaspersky Endpoint Security 11 для Windows требуется расшифровать все зашифрованные жесткие диски.

Вы можете обновить до версии Kaspersky Endpoint Security 11 для Windows следующие программы:

- Kaspersky Endpoint Security 10 Service Pack 1 для Windows (сборка 10.2.2.10535).
- Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 1 для Windows (сборка 10.2.2.10535(MR1)).
- Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 2 для Windows (сборка

10.2.4.674).

- Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 3 для Windows (сборка 10.2.5.3201).
- 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).

При обновлении Kaspersky Endpoint Security 10 Service Pack 2 для Windows до Kaspersky Endpoint Security 11 для Windows в резервное хранилище новой версии программы переносятся файлы, помещенные в резервное хранилище и на карантин в предыдущей версии программы. Для более ранних версий Kaspersky Endpoint Security, чем Kaspersky Endpoint Security 10 Service Pack 2 для Windows, перенос файлов, помещенных в резервное хранилище и на карантин в предыдущей версии программы, не осуществляется.

Вы можете обновить предыдущую версию программы следующими способами:

- локально в интерактивном режиме с помощью мастера установки программы;
- локально в тихом режиме из командной строки (см. раздел "Установка программы из командной строки" на стр. 24);
- удаленно с помощью программного комплекса Kaspersky Security Center (см. справку для Kaspersky Security Center);
- удаленно через редактор управления групповыми политиками Microsoft Windows (см. сопроводительную документацию для операционной системы).

Для обновления предыдущей версии программы до Kaspersky Endpoint Security 11 для Windows не нужно удалять предыдущую версию программы. Перед началом обновления предыдущей версии программы рекомендуется закрыть все работающие программы.
Перед обновлением предыдущей версии программы до Kaspersky Endpoint Security 11 для Windows блокируется функциональность полнодискового шифрования. Если функциональность полнодискового шифрования не удалось заблокировать, установка обновления не начнется.

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 на стр. 300.

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 http://www.eicar.org/anti_virus_test_file.htm.

Перед сохранением файла в папке на диске компьютера убедитесь, что постоянная защита файлов в этой папке отключена.

► *Чтобы проверить работоспособность функции защиты виртуальной машины с гостевой операционной системой Microsoft Windows, выполните следующие действия:*

1. Убедитесь, что защита виртуальной машины включена и работает в нормальном режиме.
2. В окне веб-браузера перейдите по ссылке для загрузки тестового файла http://www.eicar.org/download/eicar.com.

Kaspersky Endpoint Security сообщает о запрете загрузки, отобразив уведомление в окне браузера.

3. Проверьте информацию в отчете об обнаруженных вирусах:
   1. В главном окне программы нажмите на кнопку **Отчеты** и перейдите в раздел **Веб-Контроль**.
   2. Убедитесь, что в отчете присутствует сообщение об обнаружении вируса и информация об этом событии верна.
4. Отключите защиту виртуальной машины:

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

   1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 46).
   2. В левой части окна в разделе **Базовая защита** выберите подраздел **Защита от файловых угроз**.
   3. В правой части окна настройки программы снимите флажок **Включить Защиту от файловых угроз**.
   4. Нажмите на кнопку **Сохранить**.
5. Загрузите тестовый файл EICAR по ссылке http://www.eicar.org/download/eicar.com и разместите его в новую папку на системном диске виртуальной машины.
6. Включите защиту виртуальной машины:
   1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 46).
   2. В левой части окна в разделе **Базовая защита** выберите подраздел **Защита от файловых угроз**.
   3. В правой части окна настройки программы установите флажок **Включить Защиту от файловых угроз**.
   4. Нажмите на кнопку **Сохранить**.
7. Перейдите в папку с тестовым файлом, загруженным на шаге 5, и запустите его.

   Kaspersky Endpoint Security сообщает о том, что указанный файл отсутствует или доступ к нему запрещен.
8. Убедитесь, что тестовый файл был удален с виртуальной машины.
9. Проверьте информацию в отчете об обнаруженных вирусах:
   1. В главном окне программы нажмите на кнопку **Отчеты** и перейдите в раздел **Защита от файловых угроз**.
   2. Убедитесь, что в отчете отображается верная информация об обнаружении зараженного файла (время события, путь к файлу).
10. Повторите шаги 4 и 5.
11. Добавьте в область проверки папку с тестовым файлом, загруженным на шаге 5:
    1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 46).
    2. В левой части окна в разделе **Задачи** выберите подраздел **Полная проверка**, **Проверка**

важных областей и **Выборочная проверка**.

3. В правой части окна настройки программы нажмите на кнопку **Область проверки**.
4. Добавьте в область проверки папку с тестовым файлом, загруженным на шаге 5
5. Нажмите на кнопку **ОК**.
6. Нажмите на кнопку **Сохранить**.

12. В главном окне программы перейдите в раздел **Задачи**.
13. Выберите задачу, выбранную на шаге 11, и нажмите на кнопку **Запустить**.
14. По окончании выполнения задачи проверки проверьте информацию в отчете об обнаруженных вирусах:
    1. В главном окне программы нажмите на кнопку **Отчеты** и перейдите в раздел **Задачи проверки**.
    2. Убедитесь, что в отчете отображается верная информация об обнаружении зараженного файла (время события, путь к файлу).

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

1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 46).
2. В левой части окна в разделе **Контроль безопасности** выберите подраздел **Контроль программ**.
3. В правой части окна настройки программы нажмите на кнопку **Добавить**.

   Откроется окно для добавления условий контроля программы.
4. В открывшемся окне выполните следующие действия:
    1. В поле **Название правила** укажите произвольное имя.
    2. В блоке **Включающие условия** нажмите на кнопку **Добавить** и выберите пункт **Условие вручную** в раскрывающемся списке.

       Откроется окно **Пользовательское условие**.
    3. В открывшемся окне выберите вариант **Метаданные**, установите флажок **Название файла,** в поле ввода введите notepad.exe и нажмите на кнопку **ОК**.
    4. Установите флажок **Запретить остальным пользователям**.
    5. Сохраните изменения.
5. Запустите программу Блокнот.
6. Убедитесь, что запуск программы запрещен.
7. Проверьте информацию в отчете:
    1. В главном окне программы нажмите на кнопку **Отчеты** и перейдите в раздел **Контроль программ**.
    2. Убедитесь, что в отчете присутствует сообщение о запрете запуска программы Блокнот и информация об этом событии верна.

Разделение доступа к функциям программы по пользовательским ролям

По умолчанию пользователи, входящие в группу "Администраторы" на защищаемом сервере, имеют доступ ко всем функциям Kaspersky Endpoint Security.

Пользователи, которые имеют доступ к функции **Изменение прав** Kaspersky Endpoint Security, могут предоставлять доступ к функциям Kaspersky Endpoint Security другим пользователям, зарегистрированным на защищаемом сервере или входящим в домен.

Если пользователь не зарегистрирован в списке пользователей Kaspersky Endpoint Security, он не может открыть Консоль Kaspersky Endpoint Security.

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

- **Полный контроль** – доступ ко всем функциям программы: возможность просматривать и изменять общие параметры работы Kaspersky Endpoint Security, параметры работы компонентов Kaspersky Endpoint Security, права пользователей Kaspersky Endpoint Security, а также просматривать статистику работы 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.
- **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.

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

Если вы вручную настроили права доступа для пользователя или группы, то для этого пользователя или группы установлен уровень доступа **Особые разрешения**.

Таблица 1. Права доступа к функциям Kaspersky Endpoint Security

Права доступа	Описание
Управление задачами	Возможность запускать / останавливать / приостанавливать / возобновлять задачи Kaspersky Endpoint Security.
Создание и удаление задач	Возможность создавать и удалять задачи проверки по требованию.

Права доступа	Описание
Изменение параметров	Возможности: • просматривать и изменять общие параметры работы Kaspersky Endpoint Security; • импортировать из конфигурационного файла и экспортировать в конфигурационный файл параметры работы Kaspersky Endpoint Security; • просматривать и изменять параметры задач; • просматривать и изменять параметры журналов выполнения задач, журнала системного аудита и уведомлений.
Чтение параметров	Возможности: • просматривать общие параметры работы Kaspersky Endpoint Security и параметры задач; • экспортировать в конфигурационный файл параметры работы Kaspersky Endpoint Security; • просматривать параметры журналов выполнения задач, журнала системного аудита и уведомлений.
Управление хранилищами	Возможности: • помещать объекты на карантин; • удалять объекты из карантина и резервного хранилища; • восстанавливать объекты из карантина и резервного хранилища.
Управление журналами	Возможность удалять журналы выполнения задач и очищать журнал системного аудита.
Чтение журналов	Возможность просматривать события в журналах выполнения задач и журнале системного аудита.
Чтение статистики	Возможность просматривать статистику работы каждой задачи Kaspersky Endpoint Security.
Лицензирование программы	Возможность активировать и деактивировать Kaspersky Endpoint Security.
Чтение прав	Возможность просматривать список пользователей Kaspersky Endpoint Security и права доступа каждого пользователя.
Изменение прав	Возможности: • изменять список пользователей, имеющих доступ к управлению программой; • изменять права доступа пользователей к функциям Kaspersky Endpoint Security.

Интерфейс программы

Этот раздел содержит информацию об основных элементах интерфейса программы.

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.

Индикация работы программы

Значок программы служит индикатором работы программы:

- Значок  означает, что работа всех компонентов защиты программы включена.
- Значок  означает, что в работе Kaspersky Endpoint Security произошли важные события, на которые нужно обратить внимание. Например, выключен компонент Защита от файловых угроз, базы программы устарели.
- Значок  означает, что в работе Kaspersky Endpoint Security произошли события критической важности. Например, сбой в работе компонента, повреждение баз программы.

Контекстное меню значка программы

Контекстное меню значка программы содержит следующие пункты:

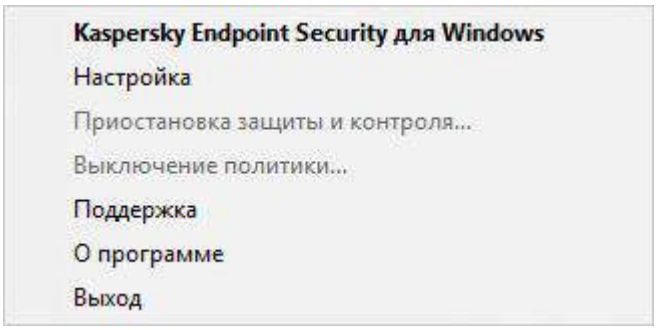
- **Kaspersky Endpoint Security для Windows**. Открывает главное окно программы. В этом окне вы можете регулировать работу компонентов и задач программы, просматривать статистику об обработанных файлах и найденных угрозах.
- **Настройка**. Открывает окно **Настройка**. С помощью закладки **Настройка** вы можете изменить

параметры программы, установленные по умолчанию.

- **Приостановка защиты и контроля** / **Возобновление защиты и контроля**. Временно приостанавливает / возобновляет работу компонентов защиты и компонентов контроля. Этот пункт контекстного меню не влияет на выполнение задачи обновления и задач проверки и доступен только при выключенной политике Kaspersky Security Center.

  Kaspersky Security Network используется в работе Kaspersky Endpoint Security вне зависимости от приостановки / возобновления работы компонентов защиты и компонентов контроля.

- **Выключение политики** / **Включение политики**. Выключает / включает политику Kaspersky Security Center. Этот пункт контекстного меню доступен, если к компьютеру с установленной программой Kaspersky Endpoint Security применена политика и в параметрах политики установлен пароль на выключение политики Kaspersky Security Center.
- **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.



Вы можете открыть контекстное меню значка программы наведением курсора мыши на значок программы в области уведомлений панели задач Microsoft Windows и нажатием на правую клавишу мыши.

Главное окно программы

В главном окне Kaspersky Endpoint Security находятся элементы интерфейса, предоставляющие вам доступ к основным функциям программы.

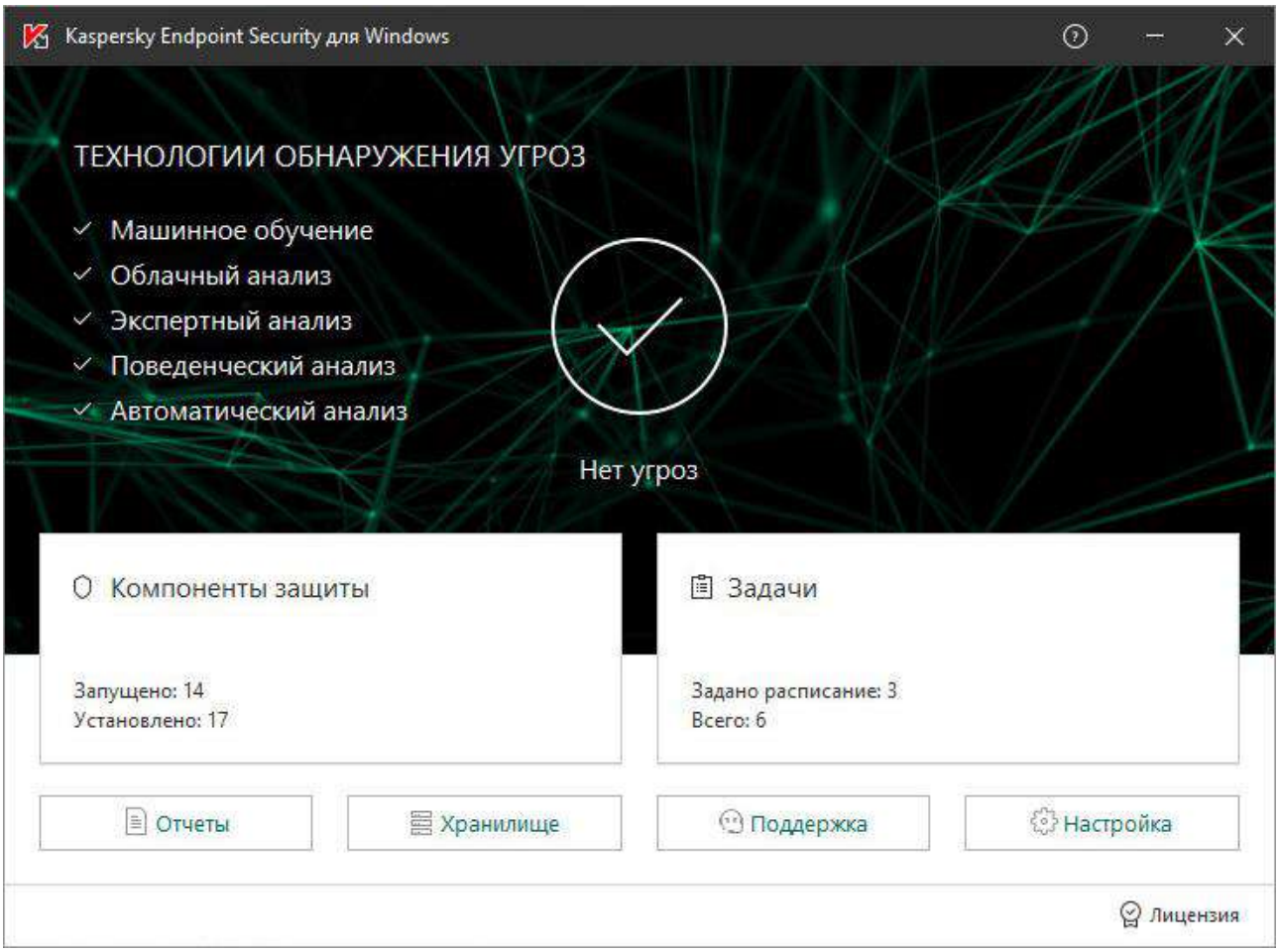
Главное окно программы содержит следующие элементы:

- Ссылка **Kaspersky Endpoint Security для Windows**. При нажатии на ссылку открывается окно **О программе** со сведениями о версии программы.
- Кнопка ⓘ. При нажатии на кнопку осуществляется переход к справочной системе Kaspersky Endpoint Security.
- Блок **Технологии обнаружения угроз**. Блок содержит следующую информацию:
  - В левой части блока отображается список технологий обнаружения угроз. Справа от названия каждой из технологий обнаружения угроз отображается количество угроз, обнаруженных с помощью этой технологии.
  - В центре блока в зависимости от наличия активных угроз отображается одна из следующих надписей:

  - **Нет угроз**. Если отображается эта надпись, то при нажатии на блок **Технологии обнаружения угроз** открывается окно **Технологии обнаружения угроз**, в котором приведено краткое описание технологий обнаружения угроз, а также статус и глобальная статистика инфраструктуры облачных служб Kaspersky Security Network.
  - **N активных угроз**. Если отображается эта надпись, то при нажатии на блок **Технологии обнаружения угроз** открывается окно **Активные угрозы**, в котором приведен список событий, связанных с зараженными файлами, которые по каким-либо причинам не были обработаны.

- Блок **Компоненты защиты**. При нажатии на блок открывается окно **Компоненты защиты**. В этом окне вы можете посмотреть статус работы установленных компонентов. Также из этого окна вы можете для любого из установленных компонентов, кроме компонентов шифрования, открыть подраздел в окне **Настройка**, содержащий параметры этого компонента.
- Блок **Задачи**. При нажатии на блок открывается окно **Задачи**. В этом окне вы можете управлять работой задач Kaspersky Endpoint Security, посредством которых обеспечивается актуальность антивирусных баз программы, выполняется проверка на присутствие вирусов или других программ, представляющих угрозу, а также выполняется проверка целостности.
- Кнопка **Отчеты**. При нажатии на кнопку открывается окно **Отчеты**, содержащее информацию о событиях, произошедших в ходе работы программы в целом, работы отдельных компонентов и выполнения задач.
- Кнопка **Хранилища**. При нажатии на кнопку открывается окно **Резервное хранилище**. В этом окне вы можете просмотреть список копий зараженных файлов, которые были удалены в ходе работы программы.
- Кнопка **Поддержка**. При нажатии на кнопку открывается окно **Поддержка** с информацией об операционной системе, текущей версии Kaspersky Endpoint Security и ссылками на информационные ресурсы "Лаборатории Касперского".
- Кнопка **Настройка**. При нажатии на кнопку открывается окно **Настройка**, в котором вы можете изменять параметры программы, установленные по умолчанию.
- Кнопка  /  /  . При нажатии на кнопку открывается окно **События** с информацией о доступных обновлениях, а также с запросами доступа к зашифрованным файлам и устройствам.

- Ссылка **Лицензия**. При нажатии на ссылку открывается окно **Лицензирование** с информацией о действующей лицензии.



► *Чтобы открыть главное окно Kaspersky Endpoint Security, выполните одно из следующих действий:*

- Нажмите на значок программы в области уведомлений панели задач Microsoft Windows.
- Выберите пункт **Kaspersky Endpoint Security для Windows** в контекстном меню значка программы (см. раздел "Контекстное меню значка программы" на стр. 42).

Продление срока действия лицензии

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

Когда срок действия лицензии подходит к концу, вы можете его продлить. Это позволит не прерывать защиту компьютера в период после окончания срока действия лицензии и до активации программы по новой лицензии.

► *Чтобы продлить срок действия лицензии, выполните следующие действия:*

1. Получите (см. раздел "Приобретение лицензии" на стр. 54) новый код активации программы или файл ключа.
2. Добавьте дополнительный ключ (см. раздел "О способах активации программы" на стр. 55) с помощью полученного кода активации или файла ключа.

В результате будет добавлен дополнительный ключ, который станет активным по истечении срока действия лицензии.

Обновление ключа с дополнительного на активный может происходить с произвольной задержкой, связанной с распределением нагрузки на серверы активации "Лаборатории Касперского".

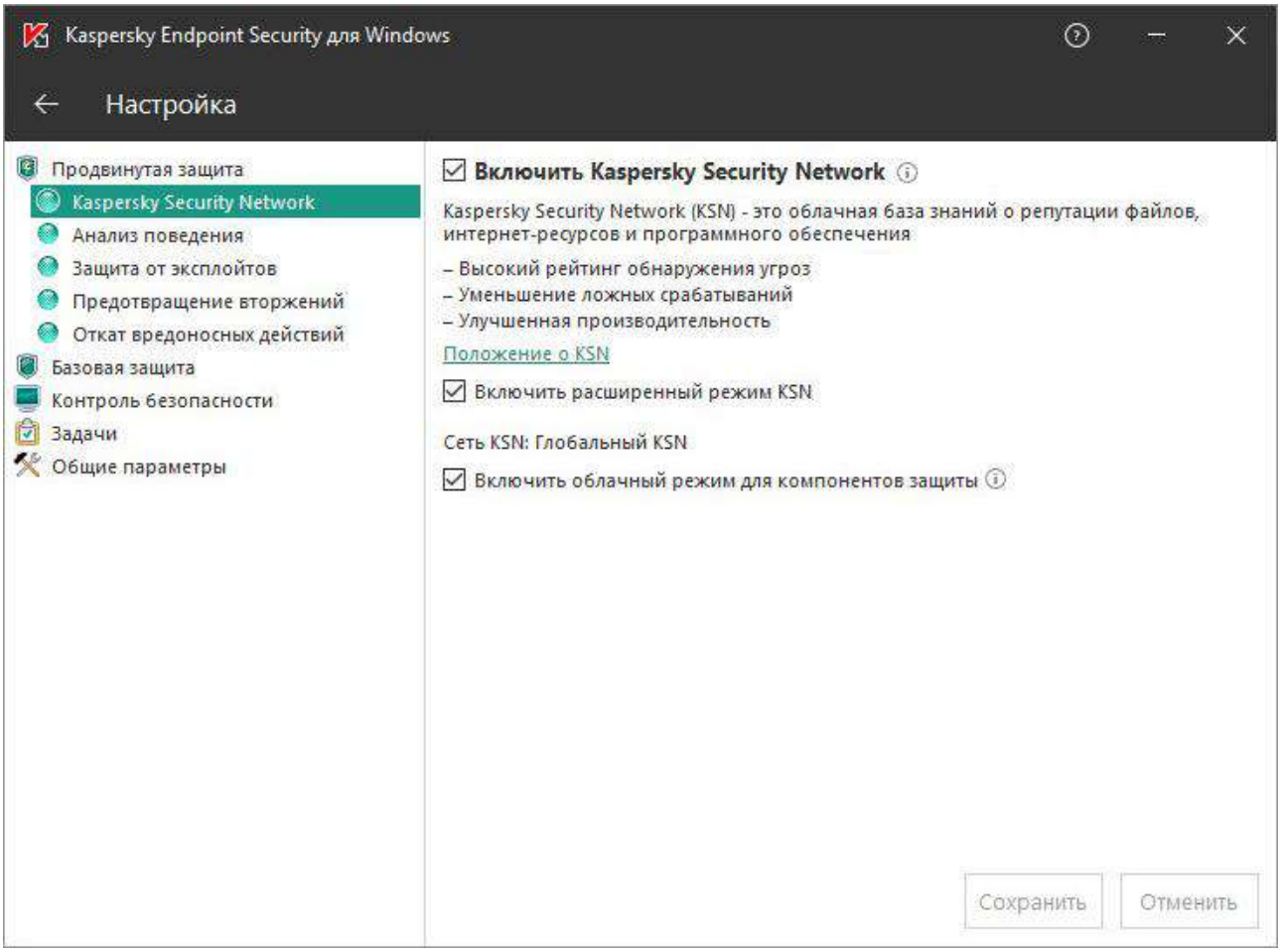
Закладка настройки параметров программы

Окно настройки параметров Kaspersky Endpoint Security позволяет настроить параметры работы программы в целом, отдельных ее компонентов, отчетов и хранилищ, задач проверки и задачи обновления, а также параметры связи с серверами Kaspersky Security Network.

Закладка настройки параметров программы состоит из двух частей (см. рис. ниже):

- В левой части содержатся компоненты программы, задачи и раздел с дополнительными параметрами, состоящий из нескольких подразделов.

- В правой части содержатся элементы управления, с помощью которых вы можете настроить параметры компонента или задачи, выбранных в левой части окна, а также дополнительные параметры.



► *Чтобы открыть окно настройки параметров программы, выполните одно из следующих действий:*

- Выберите закладку **Настройка** в главном окне программы (см. раздел "Главное окно программы" на стр. 43).
- Выберите пункт **Настройка** в контекстном меню значка программы (см. раздел "Контекстное меню значка программы" на стр. 42).

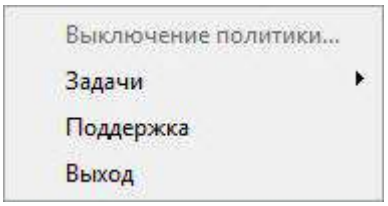
Упрощенный интерфейс программы

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. 258), 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:

- **Выключение политики**. Выключает политику Kaspersky Security Center на клиентском компьютере с установленной программой Kaspersky Endpoint

Security. Этот пункт контекстного меню доступен, если к компьютеру применена политика и в параметрах политики установлен пароль на выключение политики Kaspersky Security Center.

- **Задачи**. Раскрывающийся список, содержащий следующие элементы:
  - **Обновление**.
  - **Откат обновления**.
  - **Полная проверка**.
  - **Выборочная проверка**.
  - **Проверка важных областей**.
  - **Проверка целостности**.
- **Поддержка**. Вызов окна **Поддержка**, содержащего информацию, необходимую для обращения в Службу технической поддержки "Лаборатории Касперского".
- **Выход**. Завершение работы Kaspersky Endpoint Security.



Лицензирование программы

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

В этом разделе

О Лицензионном соглашении

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

Рекомендуется внимательно ознакомиться с условиями Лицензионного соглашения перед началом работы с программой.

Вы можете ознакомиться с условиями Лицензионного соглашения следующими способами:

- Во время установки Kaspersky Endpoint Security в интерактивном режиме (см. раздел "О способах установки программы" на стр. 18).
- Прочитав документ license.txt. Этот документ включен в комплект поставки программы.

Вы принимаете условия Лицензионного соглашения, подтверждая свое согласие с текстом Лицензионного соглашения во время установки программы. Если вы не согласны с условиями Лицензионного соглашения, вы должны прервать установку программы.

О лицензии

Лицензия - это ограниченное по времени право на использование программы, предоставляемое вам на основе Лицензионного соглашения.

Лицензия включает в себя право на получение следующих видов услуг:

- использование программы в соответствии с условиями Лицензионного соглашения;
- получение технической поддержки.

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

Предусмотрены следующие типы лицензий:

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

  Пробная лицензия обычно имеет небольшой срок действия. По истечении срока действия пробной лицензии Kaspersky Endpoint Security прекращает выполнять все свои функции. Чтобы продолжить использование программы, вам нужно приобрести коммерческую лицензию.

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

  Функциональность программы, доступная по коммерческой лицензии, зависит от выбора продукта. Выбранный продукт указан в Лицензионном сертификате (см. раздел "О лицензионном сертификате" на стр. 50). Информацию о доступных продуктах вы можете найти на сайте "Лаборатории Касперского" http://www.kaspersky.ru/business-security/small-to-medium-business.

  По истечении срока действия коммерческой лицензии программа продолжает работу, но с ограниченной функциональностью. Вы можете использовать компоненты защиты и контроля и выполнять проверку на основе баз программы, установленных до истечения срока действия лицензии. Кроме того, программа продолжает шифровать изменяющиеся файлы, зашифрованные до истечения срока действия лицензии, но не шифрует новые файлы. Использование Kaspersky Security Network недоступно.

  Для снятия ограничений на функциональность Kaspersky Endpoint Security требуется продлить срок действия коммерческой лицензии или приобрести новую лицензию.

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

О лицензионном сертификате

Лицензионный сертификат – это документ, который передается вам вместе с файлом ключа или кодом активации.

В Лицензионном сертификате содержится следующая информация о предоставляемой лицензии:

- номер заказа;
- информация о пользователе, которому предоставляется лицензия;
- информация о программе, которую можно активировать по предоставляемой лицензии;
- ограничение на количество единиц лицензирования (например, устройств, на которых можно использовать программу по предоставляемой лицензии);
- дата начала срока действия лицензии;
- дата окончания срока действия лицензии или срок действия лицензии;
- тип лицензии.

О ключе

Ключ - это уникальная буквенно-цифровая последовательность. Ключ обеспечивает использование программы в соответствии с условиями, указанными в Лицензионном сертификате (типом лицензии, сроком действия лицензии, лицензионным ограничением).

Для ключа, установленного по подписке, Лицензионный сертификат не предоставляется.

Ключ может быть добавлен в программу с помощью кода активации или файла ключа.

Вы можете добавлять, заменять или удалять ключи. Ключ может быть заблокирован "Лабораторией Касперского", если условия Лицензионного соглашения нарушены. Если ключ заблокирован, для обеспечения работы программы требуется добавить другой ключ.

Если ключ для лицензии с истекшим сроком действия удален, то функциональность программы недоступна. Добавить заново такой ключ после удаления невозможно.

Ключ может быть активным и дополнительным.

Активный ключ - ключ, используемый в текущий момент для работы программы. В качестве активного ключа может быть добавлен ключ для пробной или коммерческой лицензии. В программе не может быть больше одного активного ключа.

Дополнительный ключ - ключ, подтверждающий право на использование программы, но не используемый в текущий момент. По истечении срока годности активного ключа дополнительный ключ автоматически становится активным. Дополнительный ключ может быть добавлен только при наличии активного ключа.

Ключ для пробной лицензии может быть добавлен только в качестве активного ключа. Он не может быть добавлен в качестве дополнительного ключа. Ключ для пробной лицензии не может заменить активный ключ для коммерческой лицензии.

Если ключ попадает в черный список ключей, в течение восьми дней доступна функциональность программы, определенная лицензией, по которой программа активирована (см. раздел "О лицензии" на стр. 49). Kaspersky Security Network и обновления антивирусных баз программы доступны без ограничений. Программа уведомляет пользователя о том, что ключ помещен в черный список ключей. По истечении восьми дней функциональность программы соответствует ситуации, когда истекает срок действия лицензии, - программа работает без обновлений и Kaspersky Security Network недоступен.

О файле ключа

Файл ключа - это файл с расширением key, который вам предоставляет "Лаборатория Касперского" после приобретения Kaspersky Endpoint Security. Файл ключа предназначен для добавления ключа, активирующего программу.

Чтобы активировать программу с помощью файла ключа, не требуется подключение к серверам активации

"Лаборатории Касперского".

Если файл ключа был случайно удален, вы можете его восстановить. Файл ключа может потребоваться вам, например, для регистрации в Kaspersky CompanyAccount.

Для восстановления файла ключа вам нужно выполнить одно из следующих действий:

- обратиться в Службу технической поддержки "Лаборатории Касперского";
- получить файл ключа на веб-сайте "Лаборатории Касперского" (https://activation.kaspersky.com/ru/) на основе имеющегося кода активации.

О предоставлении данных

Если для активации Kaspersky Endpoint Security применяется код активации, с целью проверки правомерности использования программы вы соглашаетесь периодически передавать в автоматическом режиме следующую информацию:

- тип, версию и локализацию Kaspersky Endpoint Security;
- версии установленных обновлений Kaspersky Endpoint Security;
- идентификатор компьютера и идентификатор установки Kaspersky Endpoint Security на компьютере;
- код активации и уникальный идентификатор активации действующей лицензии;
- тип, версию и разрядность операционной системы, название виртуальной среды, если программа Kaspersky Endpoint Security установлена в виртуальной среде;
- идентификаторы компонентов Kaspersky Endpoint Security, активных на момент предоставления информации.

"Лаборатория Касперского" может также использовать эту информацию для формирования статистической информации о распространении и использовании программного обеспечения "Лаборатории Касперского".

Используя код активации, вы соглашаетесь на автоматическую передачу данных, перечисленных выше. Если вы не согласны предоставлять эту информацию "Лаборатории Касперского", для активации Kaspersky Endpoint Security следует использовать файл ключа.

Принимая условия Лицензионного соглашения, вы соглашаетесь передавать в автоматическом режиме следующую информацию:

- При обновлении Kaspersky Endpoint Security:
  - версию Kaspersky Endpoint Security;
  - идентификатор действующей лицензии;
  - идентификатор Kaspersky Endpoint Security;
  - серийный номер действующей лицензии;
  - уникальный идентификатор запуска задачи обновления;
  - уникальный идентификатор установки Kaspersky Endpoint Security.
- При переходе по ссылкам из интерфейса Kaspersky Endpoint Security:
  - версию Kaspersky Endpoint Security;
  - версию операционной системы;

- дату активации Kaspersky Endpoint Security;
- дату окончания действия лицензии;
- дату создания ключа;
- дату установки Kaspersky Endpoint Security;
- идентификатор Kaspersky Endpoint Security;
- идентификатор действующей лицензии;
- идентификатор обнаруженной уязвимости операционной системы;
- идентификатор последнего установленного обновления для Kaspersky Endpoint Security;
- идентификатор уязвимости, найденной при проверке на уязвимые программы;
- хеш обнаруженного объекта, представляющего угрозу, и имя этой угрозы по классификации "Лаборатории Касперского";
- категорию ошибки активации Kaspersky Endpoint Security;
- код возникшей ошибки;
- код ошибки активации Kaspersky Endpoint Security;
- количество дней до истечения срока годности ключа;
- количество дней, прошедших с момента добавления ключа;
- количество дней, прошедших с момента окончания срока действия лицензии;
- количество компьютеров, на которые распространяются действующие лицензии;
- серийный номер действующей лицензии;
- срок действия лицензии Kaspersky Endpoint Security;
- текущий статус лицензии;
- тип действующей лицензии;
- тип программы;
- уникальный идентификатор запуска задачи обновления;
- уникальный идентификатор установки Kaspersky Endpoint Security;
- уникальный идентификатор установки программного обеспечения на компьютере;
- язык интерфейса Kaspersky Endpoint Security.

- Об участии в Kaspersky Security Network:
  - факт, было ли Положение о Kaspersky Security Network принято или отклонено;
  - дату и время принятия/отклонения Положения о Kaspersky Security Network;
  - идентификатор Положения о Kaspersky Security Network и версии Положения о Kaspersky Security Network, принятого или отклоненного пользователем;
  - информацию об установке/снятии флажка **Включить Kaspersky Security Network**;
  - информацию об установке/снятии флажка **Включить расширенный режим KSN**;
  - уникальные идентификаторы персонального компьютера и пользователя;

- полную версию программы и тип программы.

  При полном выключении Kaspersky Security Network эта статистика будет отправляться каждые 4 часа в течение суток с момента выключения. При отказе от участия в Kaspersky Security Network в процессе установки Kaspersky Endpoint Security эта статистика также будет отправляться каждые 4 часа в течение суток с момента выключения Kaspersky Security Network на компьютере.

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

Более подробную информацию о получении, обработке, хранении и уничтожении информации об использовании программы после принятия Лицензионного соглашения и согласия с Положением о Kaspersky Security Network вы можете узнать, прочитав тексты этих документов, а также на веб-сайте "Лаборатории Касперского" (http://www.kaspersky.ru/privacy). Файлы license.txt и ksn_<ID языка>.txt с текстами Лицензионного соглашения и Положения о Kaspersky Security Network входят в комплект поставки программы.

Просмотр информации о лицензии

► *Чтобы просмотреть информацию о лицензии, выполните следующие действия:*

1. Откройте главное окно программы (на стр. 43).
2. Нажмите на кнопку / , расположенную в нижней части главного окна программы.

Откроется окно **Лицензирование**. В блоке, расположенном в верхней части окна **Лицензирование**, представлена информация о лицензии.

Приобретение лицензии

Вы можете приобрести лицензию уже после установки программы. Приобретя лицензию, вы получите код активации или файл ключа, с помощью которых нужно активировать программу.

► *Чтобы приобрести лицензию, выполните следующие действия:*

1. Откройте главное окно программы (на стр. 43).
2. Нажмите на кнопку / , расположенную в нижней части главного окна программы.

   Откроется окно **Лицензирование**.
3. В окне **Лицензирование** выполните одно из следующих действий:
   - Нажмите на кнопку **Приобрести лицензию**, если не добавлен ни один ключ или добавлен ключ для пробной лицензии.
   - Нажмите на кнопку **Продлить срок действия лицензии**, если добавлен ключ для коммерческой лицензии.

   Откроется веб-сайт интернет-магазина "Лаборатории Касперского", где вы можете приобрести лицензию.

О способах активации программы

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

Активация - это процедура введения в действие лицензии, дающей право на использование полнофункциональной версии программы в течение срока действия лицензии. Процедура активации программы заключается в добавлении ключа.

Вы можете активировать программу одним из следующих способов:

- Во время установки программы с помощью мастера первоначальной настройки программы (см. раздел "Мастер первоначальной настройки программы" на стр. 32). Этим способом вы можете добавить активный ключ.
- Локально из интерфейса программы с помощью мастера активации программы (см. раздел "Активация программы с помощью мастера активации программы" на стр. 55). Этим способом вы можете добавить и активный, и дополнительный ключ.
- Удаленно с помощью программного комплекса Kaspersky Security Center путем создания (см. раздел "Управление задачами" на стр. 246) и последующего запуска (см. раздел "Запуск, остановка, приостановка и возобновление выполнения задачи" на стр. 250) задачи добавления ключа. Этим способом вы можете добавить и активный, и дополнительный ключ.
- Удаленно путем распространения на клиентские компьютеры ключей и кодов активации, размещенных в хранилище ключей на Сервере администрирования Kaspersky Security Center (информация об этом приведена в *Руководстве администратора для Kaspersky Security Center*). Этим способом вы можете добавить и активный, и дополнительный ключ.

  Код активации, приобретенный по подписке, распространяется в первую очередь.

- С помощью командной строки (см. раздел "Активация программы с помощью командной строки" на стр. 56).

Во время активации программы, удаленно или во время установки программы в тихом режиме, с помощью кода активации возможна произвольная задержка, связанная с распределением нагрузки на серверы активации "Лаборатории Касперского". Если требуется немедленная активация программы, вы можете прервать выполняющуюся активацию и запустить активацию программы с помощью мастера активации программы.

Активация программы с помощью мастера активации программы

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

1. Нажмите на кнопку / , расположенную в нижней части главного окна программы.

Откроется окно **Лицензирование**.

2. В окне **Лицензирование** нажмите на кнопку **Активировать программу по новой лицензии**.

   Запустится мастер активации программы.

3. Следуйте указаниям мастера активации программы.

Более подробную информацию о процедуре активации программы вы можете найти в разделе о мастере первоначальной настройки программы (см. стр. 32).

Активация программы с помощью командной строки

► *Чтобы активировать программу с помощью командной строки,*

введите в командной строке `avp.com license /add <код активации или файл ключа> /password=<пароль>`.

Запуск и остановка программы

Этот раздел содержит информацию о том, как настроить автоматический запуск программы, как запускать и завершать работу программы вручную, а также как приостанавливать и возобновлять работу компонентов защиты и компонентов контроля.

В этом разделе

Включение и выключение автоматического запуска программы

Под автоматическим запуском программы подразумевается запуск Kaspersky Endpoint Security, который выполняется без участия пользователя после старта операционной системы. Этот вариант запуска программы установлен по умолчанию.

В первый раз программа Kaspersky Endpoint Security запускается автоматически после ее установки.

Загрузка антивирусных баз Kaspersky Endpoint Security после запуска 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 загруженной операционной системе не вызывает снижения уровня защиты компьютера.

► *Чтобы включить или выключить автоматический запуск программы, выполните следующие действия:*

1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 46).
2. В левой части окна в разделе **Общие параметры** выберите подраздел **Параметры программы**.
3. Выполните одно из следующих действий:
   - Установите флажок **Запускать Kaspersky Endpoint Security для Windows при включении компьютера**, если вы хотите включить автоматический запуск программы.
   - Снимите флажок **Запускать Kaspersky Endpoint Security для Windows при включении компьютера**, если вы хотите выключить автоматический запуск программы.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Запуск и завершение работы программы вручную

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. 58) на необходимый срок, не завершая работу программы.

Запускать Kaspersky Endpoint Security вручную требуется в том случае, если вы выключили автоматический запуск программы (см. раздел "Включение и выключение автоматического запуска программы" на стр. 57).

► *Чтобы запустить программу вручную,*

в меню **Пуск** выберите пункт **Программы** → **Kaspersky Endpoint Security для Windows**.

► *Чтобы завершить работу программы вручную, 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 **Выход**.

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. 42):

- 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 **Приостановка защиты и контроля**.

   Откроется окно **Приостановка защиты**.
3. Выберите один из следующих вариантов:
   - **Приостановить на указанное время** - защита и контроль компьютера включатся через

интервал времени, указанный в раскрывающемся списке ниже.

- **Приостановить до перезагрузки** - 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. Если на предыдущем шаге вы выбрали вариант **Приостановить на указанное время**, выберите нужный интервал в раскрывающемся списке.

► *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 **Возобновление защиты и контроля**.

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

Участие в Kaspersky Security Network

Этот раздел содержит информацию об участии в Kaspersky Security Network и инструкции о том, как включить и выключить использование Kaspersky Security Network.

В этом разделе

Об участии в 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.

После изменения лицензии для использования Локального KSN требуется предоставить поставщику услуг информацию о новом ключе. В противном случае обмен информацией с Локальным KSN невозможен.

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" (http://www.kaspersky.ru/privacy).Файл).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. 63).

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* (см. раздел "*Управление политиками*" на стр. 254).

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

Об участии в 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" (http://www.kaspersky.ru/privacy).Файл).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. 63).

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* (см. раздел "*Управление политиками*" на стр. 254).

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

Включение и выключение использования Kaspersky Security Network

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

1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 46).
2. В левой части окна в разделе **Продвинутая защита** выберите подраздел **Kaspersky Security Network**.

   В правой части окна отобразятся параметры Kaspersky Security Network.

3. Выполните одно из следующих действий:

   - Установите флажок **Включить Kaspersky Security Network**, если вы хотите, чтобы в работе компонентов Kaspersky Endpoint Security использовалась информация о репутации файлов, веб-ресурсов и программ, полученная из баз Kaspersky Security Network.

     Для настройки расширенного использования Kaspersky Security Network в работе Kaspersky Endpoint Security выполните следующие действия:

     - Установите флажок **Включить расширенный режим KSN**, если вы хотите, чтобы Kaspersky Endpoint Security отправлял на сервер Kaspersky Security Network статистическую информацию, полученную в результате своей работы, а также мог отправлять в "Лабораторию Касперского" для дополнительной проверки файлы (или части файлов), которые могут быть использованы злоумышленниками для нанесения вреда компьютеру или данным.
     - Снимите флажок **Включить расширенный режим KSN**, если вы хотите, чтобы Kaspersky Endpoint Security использовал базовые функции Kaspersky Security Network.

   - Снимите флажок **Включить Kaspersky Security Network**, если вы хотите выключить использование Kaspersky Security Network.

4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Проверка подключения к Kaspersky Security Network

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

1. Откройте главное окно программы.
2. В верхней части окна нажмите на блок **Технологии обнаружения угроз**.

   Откроется окно **Технологии обнаружения угроз**.

   В нижней части окна **Технологии обнаружения угроз** отображается следующая информация о работе Kaspersky Security Network:

   - Под строкой **KASPERSKY SECURITY NETWORK (KSN)** отображается один из следующих статусов подключения Kaspersky Endpoint Security к Kaspersky Security Network:
     - *Включено. Доступно*.

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

     - *Включено. Недоступно*.

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

     - *Отключено*.

       Статус означает, что Kaspersky Security Network не используется в работе Kaspersky Endpoint Security.
   - В строках **Безопасных объектов**, **Опасных объектов**, **Нейтрализованных угроз за сутки** отображается глобальная статистика инфраструктуры облачных служб Kaspersky Security Network.

- В строке **Последняя синхронизация** отображается дата и время последней синхронизации Kaspersky Endpoint Security с серверами KSN.

  Получение статистических данных по использованию KSN программа производит при открытии окна **Технологии обнаружения угроз**. Обновление глобальной статистики инфраструктуры облачных служб Kaspersky Security Network, а также строки **Последняя синхронизация** в реальном времени не производится.
  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*.

  Связь с серверами Kaspersky Security Network может отсутствовать по следующим причинам:

  - Ваш компьютер не подключен к интернету.
  - Программа не активирована.
  - Срок действия лицензии истек.
  - Выявлены проблемы, связанные с ключом (например, ключ попал в черный список ключей).

  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

Служба KSN позволяет получать информацию о программах, содержащуюся в репутационных базах "Лаборатории Касперского". Это дает возможность гибко управлять политиками запуска программ на уровне компании, предотвращая запуск рекламных программ и легальных программ, которые могут быть использованы злоумышленниками для нанесения вреда компьютеру или данным пользователя.

► *Чтобы проверить репутацию файла в Kaspersky Security Network, выполните следующие действия:*

1. По правой клавише мыши откройте контекстное меню файла, репутацию которого вы хотите проверить.
2. Выберите пункт **Проверить репутацию в KSN**.

   Этот пункт доступен, если вы приняли условия "Положения о Kaspersky Security Network" (см. раздел "Включение и выключение использования Kaspersky Security Network" на стр. 62).

   Откроется окно **<Название файла> - Репутация в KSN**. В окне **<Название файла> - Репутация в KSN** отображается следующая информация о проверяемом файле:

   - **Путь**. Путь, по которому файл хранится на диске.
   - **Версия**. Версия программы (информация отображается только для исполняемых файлов).

- **Цифровая подпись**. Наличие у файла цифровой подписи.
- **Подписан**. Дата подписания сертификата цифровой подписью.
- **Создан**. Дата создания файла.
- **Изменен**. Дата последнего изменения файла.
- **Размер**. Место, занимаемое файлом на диске.
- Информация о том, сколько пользователей доверяют файлу или блокируют файл.

Дополнительная защита с использованием Kaspersky Security Network

«Лаборатория Касперского» предоставляет дополнительный уровень защиты с использованием Kaspersky Security Network. Этот способ защиты нацелен на эффективную борьбу против постоянных угроз повышенной сложности и угроз нулевого дня. Объединенные с Kaspersky Endpoint Security облачные технологии и экспертные знания вирусных аналитиков «Лаборатории Касперского» обеспечивают мощную защиту против сложнейших угроз в сети.

Более подробную информацию о дополнительной защите в Kaspersky Endpoint Security вы можете найти на веб-сайте «Лаборатории Касперского».

Анализ поведения программ

Этот раздел содержит информацию об Анализе поведения программ и инструкции о том, как настроить параметры компонента.

В этом разделе

Об Анализе поведения программ

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

Компонент Анализ поведения программ использует шаблоны опасного поведения программ (далее также "шаблоны опасного поведения"). Шаблоны состоят из последовательностей действий, которые Kaspersky Endpoint Security классифицирует как опасные. 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.

Включение и выключение Анализа поведения программ

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

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

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

1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 46).
2. В левой части окна в разделе **Продвинутая защита** выберите подраздел **Анализ поведения**.

В правой части окна отобразятся параметры компонента Анализ поведения программ.

3. Выполните одно из следующих действий:
   - Установите флажок **Включить Анализ поведения**, если вы хотите, чтобы Kaspersky Endpoint Security анализировал активность программ в операционной системе, используя шаблоны опасного поведения.
   - Снимите флажок **Включить Анализ поведения**, если вы не хотите, чтобы Kaspersky Endpoint Security анализировал активность программ в операционной системе, используя шаблоны опасного поведения.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Выбор действия при обнаружении вредоносной активности программы

При обнаружении вредоносной активности программы Kaspersky Endpoint Security всегда создает в журнале запись, содержащую информацию об обнаруженной активности программы.

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

1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 46).
2. В левой части окна в разделе **Продвинутая защита** выберите подраздел **Анализ поведения**.

   В правой части окна отобразятся параметры компонента Анализ поведения программ.
3. В раскрывающемся списке **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. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Настройка защиты 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 отслеживание следующих операций, выполняемых с удаленного компьютера:

- удаление файла;
- изменение содержимого файла;
- изменение размера файла;
- перемещение файла.

Вы можете выполнить следующие действия для настройки защиты папок общего доступа от внешнего шифрования:

- выбрать действие при обнаружении внешнего шифрования папок общего доступа;
- настроить адреса исключений из защиты папок общего доступа от внешнего шифрования.

В этом разделе

Включение и выключение защиты папок общего доступа от внешнего шифрования

По умолчанию защита папок общего доступа от внешнего шифрования выключена.

После установки Kaspersky Endpoint Security функциональность 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. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 46).
2. В левой части окна в разделе **Продвинутая защита** выберите подраздел **Анализ поведения**.

   В правой части окна отобразятся параметры компонента Анализ поведения программ.

3. Выполните одно из следующих действий:
   - В блоке **Защита папок общего доступа от внешнего шифрования** установите флажок **Включить защиту папок общего доступа от внешнего шифрования**, если вы хотите, чтобы Kaspersky Endpoint Security отслеживал операции, выполняемые с удаленного компьютера:
   - В блоке **Защита папок общего доступа от внешнего шифрования** снимите флажок **Включить защиту папок общего доступа от внешнего шифрования**, если вы не хотите, чтобы Kaspersky Endpoint Security отслеживал операции, выполняемые с удаленного компьютера.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Выбор действия при обнаружении внешнего шифрования папок общего доступа

При обнаружении попытки изменения файлов в папках общего доступа, Kaspersky Endpoint Security создает в журнале запись, содержащую информацию об обнаруженной попытке изменения файлов в папках общего доступа.

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

1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 46).
2. В левой части окна в разделе **Продвинутая защита** выберите подраздел **Анализ поведения**.

   В правой части окна отобразятся параметры компонента Анализ поведения программ.
3. В блоке **Защита папок общего доступа от внешнего шифрования** в раскрывающемся списке **При обнаружении внешнего шифрования папок общего доступа** выберите нужное действие:
   - **Блокировать соединение**.

     Если выбран этот элемент, то, обнаружив попытку изменения файлов в папках общего доступа, Kaspersky Endpoint Security блокирует сетевую активность компьютера, осуществляющего изменение, создает резервные копии подверженных изменению файлов и создает в журнале запись, содержащую информацию об этой попытке изменения файлов в папках общего доступа. Если при этом включен компонент Откат вредоносных действий, то выполняется восстановление подверженных изменению файлов из резервных копий.

     Если вы выбрали элемент **Блокировать соединение**, то вы можете указать время в минутах, на которое будет заблокировано сетевое соединение, в поле **Блокировать соединение на**.
   - **Информировать**.

     Если выбран этот элемент, то, обнаружив попытку изменения файлов в папках общего доступа, Kaspersky Endpoint Security добавляет информацию об этой попытке изменения файлов в папках общего доступа в список активных угроз.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить 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. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 46).
2. В левой части окна в разделе **Продвинутая защита** выберите подраздел **Анализ поведения**.

   В правой части окна отобразятся параметры компонента Анализ поведения программ.
3. В блоке **Защита папок общего доступа от внешнего шифрования** нажмите на кнопку **Исключения**.

   Откроется окно **Исключения**.
4. Выполните одно из следующих действий:
   - Если вы хотите добавить IP-адрес или имя компьютера в список исключений, нажмите на кнопку **Добавить**.
   - Если вы хотите изменить IP-адрес или имя компьютера, выберите его в списке исключений и нажмите на кнопку **Изменить**.

   Откроется окно **Компьютеры**.
5. Введите IP-адрес компьютера или имя компьютера, попытки внешнего шифрования с которого не должны обрабатываться.
6. Нажмите на кнопку **ОК** в окне **Компьютеры**.
7. Нажмите на кнопку **ОК** в окне **Исключения**.
8. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Защита от эксплойтов

Этот раздел содержит информацию о Защите от эксплойтов и инструкции о том, как настроить параметры компонента.

В этом разделе

О Защите от эксплойтов

Компонент Защита от эксплойтов отслеживает исполняемые файлы, запускаемые уязвимыми программами. Если попытка запустить исполняемый файл из уязвимой программы не была произведена пользователем, то Kaspersky Endpoint Security блокирует запуск этого файла. Информация о запрете запуска исполняемого файла сохраняется в отчете о работе Защиты от эксплойтов.

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. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 46).
2. В левой части окна в разделе **Продвинутая защита** выберите подраздел **Защита от эксплойтов**.

   В правой части окна отобразятся параметры компонента Защита от эксплойтов.
3. Выполните одно из следующих действий:
   - Установите флажок **Включить Защиту от эксплойтов**, если вы хотите, чтобы Kaspersky Endpoint Security отслеживал 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 действие, выбранное в раскрывающемся списке **При обнаружении эксплойта**.
   - Снимите флажок **Включить Защиту от эксплойтов**, если вы не хотите, чтобы Kaspersky Endpoint Security отслеживал исполняемые файлы, запускаемые уязвимыми программами.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Настройка Защиты от эксплойтов

Вы можете выполнить следующие действия для настройки работы компонента Защита от эксплойтов:

- выбрать действие при обнаружении эксплойта;
- включить или выключить защиту памяти системных процессов.

В этом разделе

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. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 46).
2. В левой части окна в разделе **Продвинутая защита** выберите подраздел **Защита от эксплойтов**.

   В правой части окна отобразятся параметры компонента Защита от эксплойтов.
3. В раскрывающемся списке **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. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Включение и выключение защиты памяти системных процессов

По умолчанию защита памяти системных процессов включена.

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

1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 46).
2. В левой части окна в разделе **Продвинутая защита** выберите подраздел **Защита от эксплойтов**.

В правой части окна отобразятся параметры компонента Защита от эксплойтов.

3. Выполните одно из следующих действий:

   - В блоке **Защита памяти системных процессов** установите флажок **Включить защиту памяти системных процессов**, если вы хотите, чтобы Kaspersky Endpoint Security блокировал сторонние процессы, осуществляющие попытки доступа к системным процессам.
   - В блоке **Защита памяти системных процессов** снимите флажок **Включить защиту памяти системных процессов**, если вы не хотите, чтобы Kaspersky Endpoint Security блокировал сторонние процессы, осуществляющие попытки доступа к системным процессам.

4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Предотвращение вторжений

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

Этот раздел содержит информацию о Предотвращении вторжений и инструкции о том, как настроить параметры компонента.

В этом разделе

О Предотвращении вторжений

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

Компонент не следует путать с системой обнаружения вторжений.

Компонент контролирует работу программ, в том числе доступ программ к защищаемым ресурсам (например, к файлам и папкам, ключам реестра), с помощью *правил контроля программ*. Правила контроля активности программ представляют собой набор ограничений для различных действий программ в операционной системе и прав доступа к ресурсам компьютера.

Во время первого запуска программы на компьютере компонент Предотвращение вторжений проверяет безопасность программы и помещает программу в одну из групп доверия. Группа доверия определяет правила, которые Kaspersky Endpoint Security применяет для контроля активности программ.

Для более эффективной работы компонента Предотвращение вторжений вам рекомендуется принять участие в Kaspersky Security Network (см. раздел "Участие в Kaspersky Security Network" на стр. 60). Данные, полученные с помощью Kaspersky Security Network, позволяют точнее относить программы к той или иной группе доверия, а также применять оптимальные правила контроля активности программ.

Во время повторного запуска программы Предотвращение вторжений проверяет целостность программы. Если программа не была изменена, компонент применяет к ней текущие правила контроля активности программ. Если программа была изменена, Предотвращение вторжений исследует программу как при первом запуске.

Ограничения контроля аудио- и видеоустройств

О защите аудиосигнала

Функциональность защиты аудиосигнала имеет следующие особенности:

- Для работы функциональности необходимо, чтобы был включен компонент Предотвращение вторжений.
- 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 в окне параметров Предотвращение вторжений) 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.

Особенности работы аудио и видео устройств во время установки и обновления Kaspersky Endpoint Security

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.

О доступе 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** (Imaging Device).

Поддерживаемые веб-камеры

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.

Включение и выключение Предотвращения вторжений

По умолчанию компонент Предотвращение вторжений включен и работает в рекомендованном специалистами "Лаборатории Касперского" режиме. Вы можете выключить компонент Предотвращение вторжений при необходимости.

► *Чтобы включить или выключить компонент Предотвращение вторжений выполните следующие действия:*

1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 46).
2. В левой части окна в разделе **Продвинутая защита** выберите подраздел **Предотвращение вторжений**.

   В правой части окна отобразятся параметры компонента Предотвращение вторжений.
3. В правой части окна выполните одно из следующих действий:
   - Установите флажок **Включить Предотвращение вторжений**, если вы хотите включить компонент Предотвращение вторжений.
   - Снимите флажок **Включить Предотвращение вторжений**, если вы хотите выключить компонент Предотвращение вторжений.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

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.

Вы можете выбрать группу доверия, в которую Kaspersky Endpoint Security должен автоматически помещать все неизвестные программы. Программы, которые были запущены до Kaspersky Endpoint Security, автоматически помещаются в группу доверия, указанную в окне **Выбор группы доверия** (см. раздел "**Выбор группы доверия для программ, запускаемых до Kaspersky Endpoint Security**" на стр. 80).

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".

  Такие программы имеют значительные ограничения на работу с ресурсами операционной системы.

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 (см. раздел "Участие в Kaspersky Security Network" на стр. 60) (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. Программы, которые были запущены до Kaspersky Endpoint Security, автоматически помещаются в группу доверия, указанную в окне **Выбор группы доверия** (см. раздел "**Выбор группы доверия для программ, запускаемых до Kaspersky Endpoint Security**" на стр. 80).

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

В этом разделе

Настройка параметров распределения программ по группам доверия

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

► *Чтобы настроить параметры распределения программ по группам доверия, выполните следующие действия:*

1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 46).
2. В левой части окна в разделе **Продвинутая защита** выберите подраздел **Предотвращение вторжений**.

   В правой части окна отобразятся параметры компонента **Предотвращение вторжений**.
3. Если вы хотите автоматически помещать программы с цифровой подписью в группу доверия "Доверенные", установите флажок **Доверять программам, имеющим цифровую подпись**.
4. Чтобы помещать все неизвестные программы в указанную группу доверия, выберите нужную группу доверия из раскрывающегося списка **Программы, для которых не удалось определить группу доверия, автоматически помещать в**.

   В целях безопасности группа **Доверенные** не включена в значения параметра **Программы, для которых не удалось определить группу доверия, автоматически помещать в**.

5. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Изменение группы доверия

Во время первого запуска программы Kaspersky Endpoint Security автоматически помещает программу в ту или иную группу доверия. При необходимости вы можете вручную переместить программу в другую группу доверия.

Специалисты "Лаборатории Касперского" не рекомендуют перемещать программы из группы доверия, определенной автоматически, в другую группу доверия. Вместо этого при необходимости измените правила контроля активности отдельной программы (см. раздел "Изменение правила контроля программы" на стр. 82).

► *Чтобы изменить группу доверия, в которую Kaspersky Endpoint Security автоматически поместил программу при первом ее запуске, выполните следующие действия:*

1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 46).
2. В левой части окна в разделе **Продвинутая защита** выберите подраздел **Предотвращение вторжений**.

   В правой части окна отобразятся параметры компонента Предотвращение вторжений.
3. Нажмите на кнопку **Программы**.

   Откроется закладка **Контроль активности программ** окна **Программы**.
4. На закладке **Контроль активности программ** выберите нужную программу.
5. Выполните одно из следующих действий:
   - По правой клавише мыши откройте контекстное меню программы. В контекстном меню программы выберите пункт **Переместить в группу** → **<название группы>**.
   - По ссылке **Доверенные** / **Слабые ограничения** / **Сильные ограничения** / **Недоверенные** откройте контекстное меню. В контекстном меню выберите нужную группу доверия.
6. Нажмите на кнопку **OK**.
7. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

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.

► *Чтобы выбрать группу доверия для программ, запускаемых до Kaspersky Endpoint Security,*

выполните следующие действия:

1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 46).
2. В левой части окна в разделе **Продвинутая защита** выберите подраздел **Предотвращение вторжений**.

   В правой части окна отобразятся параметры компонента Предотвращение вторжений.
3. Нажмите на кнопку **Изменить**.

   Откроется окно **Выбор группы доверия**.
4. Выберите нужную группу доверия.
5. Нажмите на кнопку **ОК**.
6. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Работа с правилами контроля программ

По умолчанию для контроля работы программы применяются правила контроля активности программ, определенные для той группы доверия, в которую Kaspersky Endpoint Security поместил программу при первом ее запуске. При необходимости вы можете изменить правила контроля активности программ для всей группы доверия, для отдельной программы или группы программ внутри группы доверия.

Правила контроля активности программ, определенные для отдельных программ или групп программ внутри группы доверия, имеют более высокий приоритет, чем правила контроля активности программ, определенные для группы доверия. То есть, если параметры правил контроля программ, определенные для отдельной программы или группы программ внутри группы доверия, отличны от параметров правил контроля программ, определенных для группы доверия, то компонент Предотвращение вторжений контролирует работу программы или группы программ внутри группы доверия в соответствии с правилами контроля программ, определенными для программы или группы программ.

В этом разделе

Изменение правил контроля программ для групп доверия и для групп программ

По умолчанию для разных групп доверия созданы оптимальные правила контроля активности программ. Параметры правил контроля групп программ, входящих в группу доверия, наследуют значения параметров правил контроля групп доверия. Вы можете изменить предустановленные правила контроля групп доверия

и правила контроля групп программ.

► *Чтобы изменить правила контроля группы доверия или правила контроля группы программ, выполните следующие действия:*

1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 46).
2. В левой части окна в разделе **Продвинутая защита** выберите подраздел **Предотвращение вторжений**.

   В правой части окна отобразятся параметры компонента Предотвращение вторжений.
3. Нажмите на кнопку **Программы**.

   Откроется закладка **Контроль активности программ** окна **Предотвращение вторжений**.
4. Выберите нужную группу доверия или группу программ.
5. В контекстном меню группы доверия или группы программ выберите пункт **Правила группы**.

   Откроется окно **Правила контроля группы программ**.
6. В окне **Правила контроля группы программ** выполните одно из следующих действий:
   - Выберите закладку **Файлы и системный реестр**, если вы хотите изменить правила контроля группы доверия или правила контроля группы программ, регулирующие права группы доверия или группы программ на операции с реестром операционной системы, файлами пользователя и параметрами программ.
   - Выберите закладку **Права**, если вы хотите изменить правила контроля группы доверия или правила контроля группы программ, регулирующие права группы доверия или группы программ на доступ к процессам и объектам операционной системы.
7. Для нужного ресурса в графе соответствующего действия по правой клавише мыши откройте контекстное меню.
8. В контекстном меню выберите нужный пункт:
   - **Наследовать**.
   - **Разрешать**.
   - **Запрещать**.
   - **Записывать в отчет**.

   Если вы изменяете правила контроля группы доверия, то пункт **Наследовать** недоступен для выбора.
9. Нажмите на кнопку **OK**.
10. В окне **Программы** нажмите на кнопку **OK**.
11. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Изменение правила контроля программы

По умолчанию параметры правил контроля программ, входящих в группу программ или в группу доверия, наследуют значения параметров правил контроля группы доверия. Вы можете изменить параметры правил

контроля программ.

► *Чтобы изменить правило контроля программы, выполните следующие действия:*

1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 46).
2. В левой части окна в разделе **Продвинутая защита** выберите подраздел **Предотвращение вторжений**.

   В правой части окна отобразятся параметры компонента Предотвращение вторжений.
3. Нажмите на кнопку **Программы**.

   Откроется закладка **Контроль активности программ** окна **Предотвращение вторжений**.
4. Выберите нужную программу.
5. Выполните одно из следующих действий:
   - В контекстном меню программы выберите пункт **Правила программы**.
   - Нажмите на кнопку **Дополнительно** в правом нижнем углу закладки **Контроль активности программ**.

   Откроется окно **Правила контроля программы**.
6. В окне **Правила контроля программы** выполните одно из следующих действий:
   - Выберите закладку **Файлы и системный реестр**, если вы хотите изменить правила контроля программы, регулирующие права программы на операции с реестром операционной системы, файлами пользователя и параметрами программ.
   - Выберите закладку **Права**, если вы хотите изменить правила контроля программы, регулирующие права программы на доступ к процессам и объектам операционной системы.
7. Для нужного ресурса в графе соответствующего действия по правой клавише мыши откройте контекстное меню.
8. В контекстном меню выберите нужный пункт:
   - **Наследовать**.
   - **Разрешать**.
   - **Запрещать**.
   - **Записывать в отчет**.
9. Нажмите на кнопку **OK**.
10. В окне **Программы** нажмите на кнопку **OK**.
11. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Выключение загрузки и обновления правил контроля программ из базы Kaspersky Security Network

По умолчанию при обнаружении в базе Kaspersky Security Network новой информации о программе Kaspersky Endpoint Security применяет для этой программы правила контроля, загруженные из базы KSN. После этого вы можете изменить правила контроля для программы вручную.

Если на момент первого своего запуска программа отсутствовала в базе Kaspersky Security Network, но

затем информация о ней была добавлена в базу Kaspersky Security Network, то по умолчанию Kaspersky Endpoint Security автоматически обновляет правила контроля этой программы.

Вы можете выключить загрузку правил контроля программ из базы Kaspersky Security Network и автоматическое обновление правил контроля для ранее неизвестных программ.

► *Чтобы выключить загрузку и обновление правил контроля программ из базы Kaspersky Security Network, выполните следующие действия:*

1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 46).
2. В левой части окна в разделе **Продвинутая защита** выберите подраздел **Предотвращение вторжений**.

   В правой части окна отобразятся параметры компонента Предотвращение вторжений.
3. Снимите флажок **Обновлять правила контроля ранее неизвестных программ из базы KSN**.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Выключение наследования ограничений родительского процесса

Инициатором запуска программы может быть как пользователь, так и другая запущенная программа. Если инициатором запуска программы является другая программа, образуется последовательность запуска, состоящая из родительских и дочерних процессов.

Когда программа пытается получить доступ к защищаемому ресурсу, компонент Предотвращение вторжений анализирует права всех родительских процессов этой программы на доступ к защищаемому ресурсу. При этом выполняется правило минимального приоритета: при сравнении прав доступа программы и родительского процесса к активности программы применяются права доступа с минимальным приоритетом.

Приоритет прав доступа следующий:

1. **Разрешать**. Это право доступа имеет высший приоритет.
2. **Запрещать**. Это право доступа имеет низший приоритет.

Этот механизм предотвращает использование доверенных программ недоверенными или ограниченными в правах программами с целью выполнения привилегированных действий.

Если действие программы блокируется по причине недостатка прав у одного из родительских процессов, вы можете изменить эти права или выключить наследование ограничений родительского процесса.

► *Чтобы выключить наследование ограничений родительского процесса, выполните следующие действия:*

1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 46).
2. В левой части окна в разделе **Продвинутая защита** выберите подраздел **Предотвращение вторжений**.

   В правой части окна отобразятся параметры компонента Предотвращение вторжений.
3. Нажмите на кнопку **Программы**.

Откроется закладка **Правила контроля программ** окна **Предотвращение вторжений**.

4. Выберите нужную программу.
5. В контекстном меню программы выберите пункт **Правила программы**.

   Откроется окно **Правила контроля программы**.
6. В окне **Правила контроля программы** выберите закладку **Исключения**.
7. Установите флажок **Не наследовать ограничения родительского процесса (программы)**.
8. Нажмите на кнопку **OK**.
9. В окне **Программы** нажмите на кнопку **OK**.
10. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Исключение некоторых действий программ из правил контроля программ

► *Чтобы исключить некоторые действия программы из правил контроля программы, выполните следующие действия:*

1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 46).
2. В левой части окна в разделе **Продвинутая защита** выберите подраздел **Предотвращение вторжений**.

   В правой части окна отобразятся параметры компонента Предотвращение вторжений.
3. Нажмите на кнопку **Программы**.

   Откроется закладка **Правила контроля программ** окна **Предотвращение вторжений**.
4. Выберите нужную программу.
5. В контекстном меню программы выберите пункт **Правила программы**.

   Откроется окно **Правила контроля программы**.
6. Выберите закладку **Исключения**.
7. Установите флажки напротив действий программы, которые не нужно контролировать.
8. Нажмите на кнопку **OK**.
9. В окне **Программы** нажмите на кнопку **OK**.
10. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Удаление устаревших правил контроля программ

По умолчанию правила контроля программ, которые не запускались в течение 60 дней, автоматически удаляются. Вы можете изменить время хранения правил контроля неиспользуемых программ или выключить их автоматическое удаление.

► *Чтобы удалить устаревшие правила контроля программ, выполните следующие действия:*

1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров

программы" на стр. 46).

2. В левой части окна в разделе **Продвинутая защита** выберите подраздел **Предотвращение вторжений**.

   В правой части окна отобразятся параметры компонента Предотвращение вторжений.

3. Выполните одно из следующих действий:

   - Установите флажок **Удалять правила контроля программ, не запускавшихся более** и укажите нужное количество дней, если вы хотите, чтобы Kaspersky Endpoint Security удалял правила контроля неиспользуемых программ.
   - Снимите флажок **Удалять правила контроля программ, не запускавшихся более**, если вы хотите выключить автоматическое удаление правил контроля неиспользуемых программ.

4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Защита ресурсов операционной системы 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. Вы не можете изменять или удалять предустановленные категории защищаемых ресурсов и относящиеся к ним защищаемые ресурсы.

Вы можете выполнить следующие действия:

- добавить новую категорию защищаемых ресурсов;
- добавить новый защищаемый ресурс;
- выключить защиту ресурса.

В этом разделе

Добавление категории защищаемых ресурсов

► *Чтобы добавить новую категорию защищаемых ресурсов, выполните следующие действия:*

1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 46).
2. В левой части окна в разделе **Продвинутая защита** выберите подраздел **Предотвращение вторжений**.

В правой части окна отобразятся параметры компонента Предотвращение вторжений.

3. Нажмите на кнопку **Ресурсы**.

   Откроется закладка **Защищаемые ресурсы** окна **Предотвращение вторжений**.

4. В левой части закладки **Защищаемые ресурсы** выберите раздел или категорию защищаемых ресурсов, в которые вы хотите добавить новую категорию защищаемых ресурсов.

5. Нажмите на кнопку **Добавить** и в раскрывающемся списке выберите элемент **Категорию**.

   Откроется окно **Категория защищаемых ресурсов**.

6. В окне **Категория защищаемых ресурсов** введите название новой категории защищаемых ресурсов.

7. Нажмите на кнопку **OK**.

   В списке категорий защищаемых ресурсов появится новый элемент.

8. В окне **Предотвращение вторжений** нажмите на кнопку **OK**.

9. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

После того как вы добавили категорию защищаемых ресурсов, вы можете изменить или удалить ее с помощью кнопок **Изменить** и **Удалить** в верхней левой части закладки **Защищаемые ресурсы**.

Добавление защищаемого ресурса

► *Чтобы добавить защищаемый ресурс, выполните следующие действия:*

1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 46).

2. В левой части окна в разделе **Продвинутая защита** выберите подраздел **Предотвращение вторжений**.

   В правой части окна отобразятся параметры компонента Предотвращение вторжений.

3. Нажмите на кнопку **Ресурсы**.

   Откроется закладка **Защищаемые ресурсы** окна **Предотвращение вторжений**.

4. В левой части закладки **Защищаемые ресурсы** выберите категорию защищаемых ресурсов, в которую вы хотите добавить новый защищаемый ресурс.

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

   - **Файл или папку**.
   - **Ключ реестра**.

   Откроется окно **Защищаемый ресурс**.

6. В окне **Защищаемый ресурс** в поле **Название** введите название защищаемого ресурса.

7. Нажмите на кнопку **Обзор**.

8. В открывшемся окне задайте необходимые параметры в зависимости от типа добавляемого

защищаемого ресурса и нажмите на кнопку **OK**.

9. В окне **Защищаемый ресурс** нажмите на кнопку **OK**.

   На закладке **Защищаемые ресурсы** в списке защищаемых ресурсов выбранной категории появится новый элемент.

10. В окне **Предотвращение вторжений** нажмите на кнопку **OK**.
11. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

После того как вы добавили защищаемый ресурс, вы можете его изменить или удалить с помощью кнопок **Изменить** и **Удалить** в верхней левой части закладки **Защищаемые ресурсы**.

Выключение защиты ресурса

► *Чтобы выключить защиту ресурса, выполните следующие действия:*

1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 46).
2. В левой части окна в разделе **Продвинутая защита** выберите подраздел **Предотвращение вторжений**.

   В правой части окна отобразятся параметры компонента Предотвращение вторжений.

3. В правой части окна нажмите на кнопку **Ресурсы**.

   Откроется закладка **Защищаемые ресурсы** окна **Предотвращение вторжений**.

4. Выполните одно из следующих действий:

   - В левой части закладки в списке защищаемых ресурсов выберите ресурс, защиту которого вы хотите выключить, и снимите флажок рядом с его названием.
   - Нажмите на кнопку **Исключения** и выполните следующие действия:

     a. В окне **Исключения** нажмите на кнопку **Добавить** и в раскрывающемся списке выберите тип ресурса, который вы хотите добавить в список исключений из защиты компонента Предотвращение вторжений: **Файл или папку** или **Ключ реестра**.

        Откроется окно **Защищаемый ресурс**.

     b. В окне **Защищаемый ресурс** в поле **Название** введите название защищаемого ресурса.

     c. Нажмите на кнопку **Обзор**.

     d. В открывшемся окне задайте необходимые параметры в зависимости от типа защищаемого ресурса, который вы хотите добавить в список исключений из защиты компонентом Предотвращение вторжений.

     e. Нажмите на кнопку **OK**.

     f. В окне **Защищаемый ресурс** нажмите на кнопку **OK**.

        В списке ресурсов, исключенных из защиты компонента Предотвращение вторжений, появится новый элемент.

После того как вы добавили ресурс в список исключений из защиты компонентом Предотвращение вторжений, вы можете его изменить или удалить с помощью кнопок **Изменить** и **Удалить** в верхней части окна **Исключения**.

g. В окне **Исключения** нажмите на кнопку **OK**.

5. В окне **Предотвращение вторжений** нажмите на кнопку **OK**.
6. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Откат вредоносных действий

Этот раздел содержит информацию об Откате вредоносных действий и инструкции о том, как настроить параметры компонента.

В этом разделе

Об Откате 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 удаляет созданные вредоносной программой исполняемые файлы, которые располагаются на любых носителях, кроме сетевых.

  Kaspersky Endpoint Security удаляет исполняемые файлы, созданные программой, в которую внедрялась вредоносная программа.

  Kaspersky Endpoint Security не восстанавливает измененные или удаленные файлы.

- Реестровая активность.

  Kaspersky Endpoint Security удаляет созданные вредоносной программой разделы и ключи реестра.

  Kaspersky Endpoint Security не восстанавливает измененные или удаленные разделы и ключи реестра.

- Системная активность.

  Kaspersky Endpoint Security завершает процессы, которые запускала вредоносная программа.

  Kaspersky Endpoint Security завершает процессы, в которые внедрялась вредоносная программа.

  Kaspersky Endpoint Security не возобновляет процессы, которые остановила вредоносная программа.

- Сетевая активность.

  Kaspersky Endpoint Security запрещает сетевую активность вредоносной программы.

  Kaspersky Endpoint Security запрещает сетевую активность тех процессов, в которые внедрялась вредоносная программа.

Откат действий вредоносной программы может быть запущен компонентом Защита от файловых угроз (см. стр. 92) или при антивирусной проверке (см. раздел «Проверка компьютера» на стр. 186).

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

Включение и выключение Отката вредоносных действий

► *Чтобы включить или выключить Откат вредоносных действий, выполните следующие действия:*

1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 46).
2. В левой части окна в разделе **Продвинутая защита** выберите подраздел **Откат вредоносных действий**.
3. Выполните одно из следующих действий:
   - Установите флажок **Включить Откат вредоносных действий** в правой части окна, если вы хотите, чтобы при обнаружении вредоносных программ, Kaspersky Endpoint Security выполнял откат действий, которые эти программы совершили в операционной системе.
   - Снимите флажок **Включить Откат вредоносных действий** в правой части окна, если вы хотите, чтобы при обнаружении вредоносных программ, Kaspersky Endpoint Security не выполнял откат действий, которые эти программы совершили в операционной системе.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Защита от файловых угроз

Этот раздел содержит информацию о компоненте Защита от файловых угроз и инструкции о том, как настроить параметры этого компонента.

В этом разделе

О Защите от файловых угроз

Компонент Защита от файловых угроз позволяет избежать заражения файловой системы компьютера. По умолчанию компонент Защита от файловых угроз запускается при старте Kaspersky Endpoint Security, постоянно находится в оперативной памяти компьютера и проверяет открываемые и запускаемые файлы на компьютере и на присоединенных дисках на наличие в них вирусов и других программ, которые могут предоставлять угрозу. Проверка выполняется в соответствии с параметрами программы.

При обнаружении угрозы в файле Kaspersky Endpoint Security выполняет следующие действия:

1. Определяет тип обнаруженного в файле объекта (например, *вирус*, *троянская программа*).
2. Выводит на экран уведомление (см. стр. 209) о вредоносном объекте, обнаруженном в файле (если настроены уведомления) и выполняет над файлом действие (см. раздел "Изменение действия над зараженными файлами" на стр. 190), заданное в параметрах компонента Защита от файловых угроз.

Включение и выключение Защиты от файловых угроз

По умолчанию компонент Защита от файловых угроз включен и работает в рекомендованном специалистами "Лаборатории Касперского" режиме. Вы можете выключить Защиту от файловых угроз при необходимости.

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

1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 46).
2. В левой части окна в разделе **Базовая защита** выберите подраздел **Защита от файловых угроз**.

   В правой части окна отобразятся параметры компонента Защита от файловых угроз.
3. Выполните одно из следующих действий:
   - Установите флажок **Включить Защиту от файловых угроз**, если вы хотите включить Защиту

от файловых угроз.

- Снимите флажок **Включить Защиту от файловых угроз**, если вы хотите выключить Защиту от файловых угроз.

4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

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. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 46).
2. В левой части окна в разделе **Базовая защита** выберите подраздел **Защита от файловых угроз**.

   В правой части окна отобразятся параметры компонента **Защита от файловых угроз**.
3. В блоке **Уровень безопасности** нажмите на кнопку **Настройка**.

   Откроется окно **Защита от файловых угроз**.
4. В окне **Защита от файловых угроз** выберите закладку **Дополнительно**.
5. В блоке **Приостановка задачи** выполните следующие действия:

   - Установите флажок **По расписанию** и нажмите на кнопку **Расписание**, если вы хотите настроить автоматическую приостановку работы Защиты от файловых угроз в указанное время.

     Откроется окно **Приостановка задачи**.
   - Установите флажок **При запуске программ** и нажмите на кнопку **Выбрать**, если вы хотите настроить автоматическую приостановку Защиты от файловых угроз при запуске указанных программ.

     Откроется окно **Программы**.
6. Выполните одно из следующих действий:

   - Если вы настраиваете автоматическую приостановку Защиты от файловых угроз в указанное время, то в окне **Приостановка задачи** в полях **Приостановить в** и **Возобновить в** укажите время (в формате ЧЧ:ММ), в течение которого Защиту от файловых угроз следует приостанавливать. Нажмите на кнопку **ОК**.
   - Если вы настраиваете автоматическую приостановку Защиты от файловых угроз при запуске

указанных программ, то в окне **Программы** с помощью кнопок **Добавить**, **Изменить** и **Удалить** сформируйте список программ, во время работы которых Защиту от файловых угроз следует приостанавливать. Нажмите на кнопку **OK**.

7. В окне **Защита от файловых угроз** нажмите на кнопку **OK**.
8. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Настройка Защиты от файловых угроз

Вы можете выполнить следующие действия для настройки работы компонента Защита от файловых угроз:

- Изменить уровень безопасности.

  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.

- Изменить действие, которое компонент Защита от файловых угроз выполняет при обнаружении зараженного файла.

- Сформировать область защиты компонента Защита от файловых угроз.

  Вы можете расширить или сузить область защиты, добавив или удалив объекты проверки или изменив тип проверяемых файлов.

- Настроить использование эвристического анализа.

  Во время своей работы компонент Защита от файловых угроз использует метод проверки Машинное обучение и сигнатурный анализ. В процессе сигнатурного анализа компонент Защита от файловых угроз сравнивает найденный объект с записями в антивирусных 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. В процессе эвристического анализа компонент Защита от файловых угроз анализирует активность, которую объекты производят в системе. Эвристический анализ позволяет обнаруживать вредоносные объекты, записей о которых еще нет в антивирусных базах программы.

- Оптимизировать проверку.

  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, которые позволяют оптимизировать скорость проверки файлов за счет исключения из проверки файлов, не измененных с момента их последней проверки.

- Настроить проверку составных файлов.

- Изменить режим проверки файлов.

В этом разделе

Изменение уровня безопасности

Для защиты файловой системы компьютера компонент Защита от файловых угроз применяет разные наборы параметров. Такие наборы параметров называют *уровнями безопасности*. Предустановлены три уровня безопасности: **Высокий**, **Рекомендуемый**, **Низкий**. Параметры уровня безопасности **Рекомендуемый** считаются оптимальными, они рекомендованы специалистами "Лаборатории Касперского".

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

1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 46).
2. В левой части окна в разделе **Базовая защита** выберите подраздел **Защита от файловых угроз**.

   В правой части окна отобразятся параметры компонента Защита от файловых угроз.
3. В блоке **Уровень безопасности** выполните одно из следующих действий:
   - Если вы хотите установить один из предустановленных уровней безопасности (**Высокий**, **Рекомендуемый**, **Низкий**), выберите его при помощи ползунка.
   - Если вы хотите настроить уровень безопасности самостоятельно, нажмите на кнопку **Настройка** и задайте параметры в открывшемся окне **Защита от файловых угроз**.

     После того как вы самостоятельно настроили уровень безопасности, название уровня безопасности в блоке **Уровень безопасности** изменится на **Другой**.
   - Если вы хотите изменить уровень безопасности на **Рекомендуемый**, нажмите на кнопку **По умолчанию**.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить 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. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 46).
2. В левой части окна в разделе **Базовая защита** выберите подраздел **Защита от файловых угроз**.

   В правой части окна отобразятся параметры компонента 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 компонент Защита от файловых угроз автоматически пытается вылечить все обнаруженные зараженные файлы. Если лечение невозможно, то компонент Защита от файловых угроз удаляет эти файлы.
   - **Лечить, блокировать, если лечение невозможно**.

     Если выбран этот вариант действия, то компонент Защита от файловых угроз автоматически пытается вылечить все обнаруженные зараженные файлы. Если лечение невозможно, то компонент Защита от файловых угроз блокирует эти файлы.
   - **Блокировать**.

     Если выбран этот вариант действия, то компонент Защита от файловых угроз автоматически блокирует зараженные файлы без попытки их вылечить.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить 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.

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

1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 46).
2. В левой части окна в разделе **Базовая защита** выберите подраздел **Защита от файловых угроз**.

   В правой части окна отобразятся параметры компонента Защита от файловых угроз.
3. В блоке **Уровень безопасности** нажмите на кнопку **Настройка**.

   Откроется окно **Защита от файловых угроз**.
4. В окне **Защита от файловых угроз** выберите закладку **Общие**.
5. В блоке **Типы файлов** укажите тип файлов, которые вы хотите проверять компонентом Защита от файловых угроз:

- Выберите **Все файлы**, если вы хотите проверять все файлы.
- Выберите **Файлы, проверяемые по формату**, если вы хотите проверять файлы тех форматов, которые наиболее подвержены заражению.
- Выберите **Файлы, проверяемые по расширению**, если вы хотите проверять файлы с расширениями, наиболее подверженными заражению.

Выбирая тип проверяемых файлов, нужно помнить следующее:

- Вероятность внедрения вредоносного кода в файлы некоторых форматов (например, TXT) и его последующей активации достаточно низка. В то же время существуют файловые форматы, которые содержат или могут содержать исполняемый код (например, форматы EXE, DLL, DOC). Риск внедрения в такие файлы вредоносного кода и его активации весьма высок.
- 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 такой файл пропускается. Если же выбрана проверка файлов по формату, то вне зависимости от расширения компонент Защита от файловых угроз проанализирует заголовок файла, в результате чего может выясниться, что файл имеет формат EXE. Такой файл тщательно проверяется на вирусы и другие программы, представляющие угрозу.

6. В списке **Область защиты** выполните одно из следующих действий:
   - Нажмите на кнопку **Добавить**, если вы хотите добавить новый объект в область проверки.
   - Если вы хотите изменить местоположение объекта, выберите объект из области проверки и нажмите на кнопку **Изменить**.

   Откроется окно **Выбор области проверки**.
   - Если вы хотите удалить объект из списка проверяемых объектов, выберите объект в списке проверяемых объектов и нажмите на кнопку **Удалить**.

     Откроется окно подтверждения удаления.
7. Выполните одно из следующих действий:
   - Если вы хотите добавить новый объект или изменить местоположение объекта из списка проверяемых объектов, в окне **Выбор области проверки** выберите объект и нажмите на кнопку **Добавить**.

     Все объекты, выбранные в окне **Выбор области проверки**, отобразятся в списке **Область защиты** в окне **Защита от файловых угроз**.

     Нажмите на кнопку **ОК**.
   - Если вы хотите удалить объект, нажмите на кнопку **Да** в окне подтверждения удаления.
8. При необходимости повторите пункты 6-7 для добавления, изменения местоположения или удаления объектов из списка проверяемых объектов.
9. Чтобы исключить объект из списка проверяемых объектов, в списке **Область защиты** снимите флажок рядом с ним. Объект при этом остается в списке проверяемых объектов, но исключается из проверки компонентом Защита от файловых угроз.
10. В окне **Защита от файловых угроз** нажмите на кнопку **ОК**.
11. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Использование эвристического анализа в работе компонента Защита от файловых угроз

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

1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 46).
2. В левой части окна в разделе **Базовая защита** выберите подраздел **Защита от файловых угроз**.

   В правой части окна отобразятся параметры компонента Защита от файловых угроз.
3. В блоке **Уровень безопасности** нажмите на кнопку **Настройка**.

   Откроется окно **Защита от файловых угроз**.
4. В окне **Защита от файловых угроз** выберите закладку **Производительность**.
5. В блоке **Методы проверки** выполните следующие действия:
   - Если вы хотите, чтобы компонент Защита от файловых угроз использовал эвристический анализ, установите флажок **Эвристический анализ** и при помощи ползунка задайте уровень эвристического анализа: **поверхностный**, **средний** или **глубокий**.
   - Если вы хотите, чтобы компонент Защита от файловых угроз не использовал эвристический анализ, снимите флажок **Эвристический анализ**.
6. Нажмите на кнопку **OK**.
7. Нажмите на кнопку **Сохранить**, чтобы сохранить 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. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 46).
2. В левой части окна в разделе **Базовая защита** выберите подраздел **Защита от файловых угроз**.

   В правой части окна отобразятся параметры компонента Защита от файловых угроз.
3. В блоке **Уровень безопасности** нажмите на кнопку **Настройка**.

   Откроется окно **Защита от файловых угроз**.
4. В окне **Защита от файловых угроз** выберите закладку **Дополнительно**.
5. В блоке **Технологии проверки** выполните следующие действия:
   - Установите флажки около названий тех технологий, которые вы хотите использовать в работе компонента Защита от файловых угроз.
   - Снимите флажки около названий тех технологий, которые вы не хотите использовать в работе компонента Защита от файловых угроз.
6. Нажмите на кнопку **OK**.

7. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Оптимизация проверки файлов

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

1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 46).
2. В левой части окна в разделе **Базовая защита** выберите подраздел **Защита от файловых угроз**.

   В правой части окна отобразятся параметры компонента Защита от файловых угроз.
3. Нажмите на кнопку **Настройка**.

   Откроется окно **Защита от файловых угроз**.
4. В окне **Защита от файловых угроз** выберите закладку **Производительность**.
5. В блоке **Оптимизация проверки** установите флажок **Проверять только новые и измененные файлы**.
6. Нажмите на кнопку **ОК**.
7. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Проверка составных файлов

Распространенной практикой сокрытия вирусов и других программ, представляющих угрозу, является внедрение их в составные файлы, например, архивы или почтовые базы. 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 круг 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. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 46).
2. В левой части окна в разделе **Базовая защита** выберите подраздел **Защита от файловых угроз**.

   В правой части окна отобразятся параметры компонента Защита от файловых угроз.
3. В блоке **Уровень безопасности** нажмите на кнопку **Настройка**.

   Откроется окно **Защита от файловых угроз**.
4. В окне **Защита от файловых угроз** выберите закладку **Производительность**.
5. В блоке **Проверка составных файлов** укажите, какие составные файлы вы хотите проверять: архивы, установочные пакеты или файлы офисных форматов.

6. Чтобы проверять только новые и измененные составные файлы, установите флажок **Проверять только новые и измененные файлы**.

   Компонент Защита от файловых угроз будет проверять только новые и измененные составные файлы всех типов.

7. Нажмите на кнопку **Дополнительно**.

   Откроется окно **Составные файлы**.

8. В блоке **Фоновая проверка** выполните одно из следующих действий:

   - Чтобы запретить компоненту Защита от файловых угроз распаковывать составные файлы в фоновом режиме, снимите флажок **Распаковывать составные файлы в фоновом режиме**.
   - Чтобы разрешить компоненту Защита от файловых угроз распаковывать составные файлы при проверке в фоновом режиме, установите флажок **Распаковывать составные файлы в фоновом режиме** и в поле **Минимальный размер файла** укажите нужное значение.

9. В блоке **Ограничение по размеру** выполните одно из следующих действий:

   - Чтобы запретить компоненту Защита от файловых угроз распаковывать составные файлы большого размера, установите флажок **Не распаковывать составные файлы большого размера** и в поле **Максимальный размер файла** укажите нужное значение. Компонент Защита от файловых угроз не будет распаковывать составные файлы больше указанного размера.
   - Чтобы разрешить компоненту Защита от файловых угроз распаковывать составные файлы большого размера, снимите флажок **Не распаковывать составные файлы большого размера**.

     Файлом большого размера считается файл, размер которого больше значения в поле **Максимальный размер файла**.

   Компонент Защита от файловых угроз проверяет файлы больших размеров, извлеченные из архивов, независимо от того, установлен ли флажок **Не распаковывать составные файлы большого размера**.

10. Нажмите на кнопку **OK**.
11. В окне **Защита от файловых угроз** нажмите на кнопку **OK**.
12. Нажмите на кнопку **Сохранить**, чтобы сохранить 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. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров

программы" на стр. 46).

2. В левой части окна в разделе **Базовая защита** выберите подраздел **Защита от файловых угроз**.

   В правой части окна отобразятся параметры компонента Защита от файловых угроз.

3. В блоке **Уровень безопасности** нажмите на кнопку **Настройка**.

   Откроется окно **Защита от файловых угроз**.

4. В окне **Защита от файловых угроз** выберите закладку **Дополнительно**.

5. В блоке **Режим проверки** выберите нужный режим:

   - **Интеллектуальный**.
   - **При доступе и изменении**.
   - **При доступе**.
   - **При выполнении**.

6. Нажмите на кнопку **ОК**.

7. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Защита от веб-угроз

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

Этот раздел содержит информацию о компоненте Защита от веб-угроз и инструкции о том, как настроить параметры компонента.

В этом разделе

О Защите от веб-угроз

Каждый раз при работе в интернете пользователь подвергает информацию, хранящуюся на компьютере, риску заражения вирусами и другими программами, представляющими угрозу. Они могут проникать на компьютер, когда пользователь загружает бесплатные программы или просматривает информацию на веб-сайтах, которые до посещения пользователем подверглись атаке злоумышленников. Сетевые черви могут проникать на компьютер пользователя до открытия веб-страницы или скачивания файла, непосредственно в момент установки соединения с интернетом.

Компонент Защита от веб-угроз защищает информацию, поступающую на компьютер пользователя и отправляемую с него по протоколам HTTP и FTP, а также устанавливает принадлежность ссылок к вредоносным или фишинговым веб-адресам.

Каждую веб-страницу или файл, к которому обращаются пользователь или некоторая программа по протоколу HTTP или FTP, компонент Защита от веб-угроз перехватывает и анализирует на присутствие вирусов и других программ, представляющих угрозу. Далее происходит следующее:

- Если на веб-странице или в файле не обнаружен вредоносный код, они сразу же становятся доступными для пользователя.
- Если веб-страница или файл, к которым обращается пользователь, содержат вредоносный код, программа выполняет заданное в параметрах компонента Защита от веб-угроз действие.

Включение и выключение Защиты от веб-угроз

По умолчанию компонент Защита от веб-угроз включен и работает в рекомендованном специалистами "Лаборатории Касперского" режиме. Вы можете выключить компонент Защита от веб-угроз при необходимости.

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

1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 46).
2. В левой части окна в разделе **Базовая защита** выберите подраздел **Защита от веб-угроз**.

   В правой части окна отобразятся параметры компонента Защита от веб-угроз.
3. Выполните одно из следующих действий:
   - Установите флажок **Включить Защиту от веб-угроз**, если вы хотите включить компонент Защита от веб-угроз.
   - Снимите флажок **Включить Защиту от веб-угроз**, если вы хотите выключить компонент Защита от веб-угроз.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Настройка Защиты от веб-угроз

Вы можете выполнить следующие действия для настройки работы компонента Защита от веб-угроз:

- Изменить уровень безопасности веб-трафика.

  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.
- Изменить действие, которое Kaspersky Endpoint Security выполняет над вредоносными объектами веб-трафика.

  Если в результате проверки веб-трафика компонентом Защита от веб-угроз объекта выясняется, что объект содержит вредоносный код, дальнейшие операции компонента Защита от веб-угроз с этим объектом зависят от указанного вами действия.
- Настроить проверку ссылок компонентом Защита от веб-угроз по базам фишинговых и вредоносных веб-адресов.
- Настроить использование эвристического анализа при проверке веб-трафика на наличие вирусов и других программ, представляющих угрозу.

  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.
- Настроить использование эвристического анализа при проверке веб-страниц на наличие фишинговых ссылок.
- Оптимизировать проверку веб-трафика компонентом Защита от веб-угроз, исходящего и поступающего по протоколам HTTP и FTP.
- Сформировать список 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.

В этом разделе

Изменение уровня безопасности веб-трафика

Для защиты данных, получаемых и передаваемых по протоколам HTTP и FTP, компонент Защита от веб-угроз применяет разные наборы параметров. Такие наборы параметров называются *уровнями безопасности веб-трафика*. Предустановлены три уровня безопасности веб-трафика: **Высокий**, **Рекомендуемый**, **Низкий**. Параметры уровня безопасности веб-трафика **Рекомендуемый** считаются оптимальными, они рекомендованы специалистами "Лаборатории Касперского".

► *Чтобы изменить уровень безопасности веб-трафика, выполните следующие действия:*

1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 46).
2. В левой части окна в разделе **Базовая защита** выберите подраздел **Защита от веб-угроз**.

   В правой части окна отобразятся параметры компонента Защита от веб-угроз.
3. В блоке **Уровень безопасности** выполните одно из следующих действий:
   - Если вы хотите установить один из предустановленных уровней безопасности веб-трафика (**Высокий**, **Рекомендуемый**, **Низкий**), выберите его при помощи ползунка.
   - Если вы хотите настроить уровень безопасности веб-трафика самостоятельно, нажмите на кнопку **Настройка** и задайте параметры в открывшемся окне **Защита от веб-угроз**.

     После того как вы самостоятельно настроили уровень безопасности веб-трафика, название уровня безопасности веб-трафика в блоке **Уровень безопасности** изменится на **Другой**.
   - Если вы хотите изменить настроенный самостоятельно уровень безопасности веб-трафика на **Рекомендуемый**, нажмите на кнопку **По умолчанию**.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

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. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 46).
2. В левой части окна в разделе **Базовая защита** выберите подраздел **Защита от веб-угроз**.

   В правой части окна отобразятся параметры компонента 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 выводит на экран окно уведомления о блокировке, создает в журнале запись, содержащую информацию о зараженном объекте.
   - **Информировать**.

     Если выбран этот вариант, то в случае обнаружения в веб-трафике зараженного объекта компонент Защита от веб-угроз разрешает загрузку этого объекта на компьютер и Kaspersky Endpoint Security создает в журнале запись, содержащую информацию о зараженном объекте, добавляет информацию о зараженном объекте в список активных угроз.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Проверка компонентом Защита от веб-угроз 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. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 46).
2. В левой части окна в разделе **Базовая защита** выберите подраздел **Защита от веб-угроз**.

В правой части окна отобразятся параметры компонента Защита от веб-угроз.

3. Нажмите на кнопку **Настройка**.

   Откроется окно **Защита от веб-угроз**.

4. В окне **Защита от веб-угроз** выберите закладку **Общие**.

5. Выполните следующие действия:

   - В блоке **Методы проверки** установите флажок **Проверять ссылки по базе вредоносных веб-адресов**, если вы хотите, чтобы компонент Защита от веб-угроз проверял ссылки по базам вредоносных веб-адресов.
   - В блоке **Параметры антифишинга** установите флажок **Проверять ссылки по базе фишинговых веб-адресов**, если вы хотите, чтобы компонент Защита от веб-угроз проверял ссылки по базам фишинговых веб-адресов.

   Для проверки ссылок вы также можете использовать репутационные базы Kaspersky Security Network (см. раздел "Участие в Kaspersky Security Network" на стр. 60).

6. Нажмите на кнопку **OK**.

7. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Использование эвристического анализа в работе компонента Защита от веб-угроз

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

1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 46).

2. В левой части окна в разделе **Базовая защита** выберите подраздел **Защита от веб-угроз**.

   В правой части окна отобразятся параметры компонента Защита от веб-угроз.

3. В блоке **Уровень безопасности** нажмите на кнопку **Настройка**.

   Откроется окно **Защита от веб-угроз**.

4. Выберите закладку **Общие**.

5. Если вы хотите, чтобы компонент Защита от веб-угроз использовал эвристический анализ при проверке веб-трафика на наличие вирусов и других программ, представляющих угрозу, в блоке **Методы проверки** установите флажок **Эвристический анализ для обнаружения вирусов** и при помощи ползунка задайте уровень эвристического анализа: **поверхностный**, **средний** или **глубокий**.

6. Если вы хотите, чтобы компонент Защита от веб-угроз использовал эвристический анализ при проверке веб-страниц на наличие фишинговых ссылок, в блоке **Параметры антифишинга** установите флажок **Эвристический анализ для обнаружения фишинговых ссылок**.

7. Нажмите на кнопку **OK**.

8. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Формирование списка доверенных веб-адресов

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

1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 46).
2. В левой части окна в разделе **Базовая защита** выберите подраздел **Защита от веб-угроз**.

   В правой части окна отобразятся параметры компонента Защита от веб-угроз.
3. Нажмите на кнопку **Настройка**.

   Откроется окно **Защита от веб-угроз**.
4. Выберите закладку **Доверенные веб-адреса**.
5. Установите флажок **Не проверять веб-трафик с доверенных веб-адресов**.
6. Сформируйте список адресов веб-сайтов / веб-страниц, содержимому которых вы доверяете. Для пополнения списка выполните следующие действия:
   a. Нажмите на кнопку **Добавить**.

      Откроется окно **Веб-адрес / Маска веб-адреса**.
   b. Введите адрес веб-сайта / веб-страницы или маску адреса веб-сайта / веб-страницы.
   c. Нажмите на кнопку **OK**.

      В списке доверенных веб-адресов появится новая запись.
7. Нажмите на кнопку **OK**.
8. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Защита от почтовых угроз

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

Этот раздел содержит информацию о компоненте Защита от почтовых угроз и инструкции о том, как настроить параметры компонента.

В этом разделе

О Защите от почтовых угроз

Компонент Защита от почтовых угроз проверяет входящие и исходящие сообщения электронной почты на наличие в них вирусов и других программ, представляющих угрозу. Он запускается при старте Kaspersky Endpoint Security, постоянно находится в оперативной памяти компьютера и проверяет все сообщения, получаемые или отправляемые по протоколам POP3, SMTP, IMAP, MAPI и NNTP. Если угрозы в сообщении электронной почты не обнаружены, оно становится доступным и / или обрабатывается.

При обнаружении угрозы в сообщении электронной почты компонент Защита от почтовых угроз выполняет следующие действия:

1. Присваивает сообщению электронной почты статус *Заражен*.

   Этот статус присваивается сообщению электронной почты в следующих случаях:

   - Если в результате проверки в сообщении электронной почты найден участок кода известного вируса, информация о котором содержится в антивирусных базах Kaspersky Endpoint Security.
   - Если в сообщении электронной почты присутствует участок кода, свойственный вирусам и другим программам, представляющим угрозу, или модифицированный код известного вируса.
2. Определяет тип объекта, обнаруженного в сообщении электронной почты (например, *троянская программа*).
3. Блокирует сообщение электронной почты.
4. Выводит на экран уведомление (см. стр. 209) об обнаруженном объекте (если это указано в параметрах уведомлений).
5. Выполняет действие, заданное в параметрах компонента Защита от почтовых угроз.

Компонент взаимодействует с почтовыми клиентами, установленными на компьютере. Для почтового

клиента Microsoft Office Outlook® предусмотрено встраиваемое расширение, позволяющее производить более тонкую настройку проверки сообщений. Расширение компонента Защита от почтовых угроз встраивается в почтовый клиент Microsoft Office Outlook во время установки Kaspersky Endpoint Security.

Включение и выключение Защиты от почтовых угроз

По умолчанию компонент Защита от почтовых угроз включен и работает в рекомендованном специалистами "Лаборатории Касперского" режиме. Вы можете выключить компонент Защита от почтовых угроз при необходимости.

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

1. Откройте окно окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 46).
2. В левой части окна в разделе **Базовая защита** выберите подраздел **Защита от почтовых угроз**.

   В правой части окна отобразятся параметры компонента Защита от почтовых угроз.
3. Выполните одно из следующих действий:
   - Установите флажок **Включить Защиту от почтовых угроз**, если вы хотите включить компонент Защита от почтовых угроз.
   - Снимите флажок **Включить Защиту от почтовых угроз**, если вы хотите выключить компонент Защита от почтовых угроз.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Настройка Защиты от почтовых угроз

Вы можете выполнить следующие действия для настройки работы компонента Защиты от почтовых угроз:

- Изменить уровень безопасности почты.

  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.
- Изменить действие, которое Kaspersky Endpoint Security выполняет над зараженными сообщениями.
- Сформировать область защиты компонент Защита от почтовых угроз.
- Настроить проверку 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.
- Настроить фильтрацию по типу вложений в сообщениях электронной почты.

  Фильтрация по типу вложений в сообщениях позволяет автоматически переименовывать или удалять файлы указанных типов.

- Настроить использование эвристического анализа.

  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 в сообщениях угрозы, записей о которых еще нет в базах Kaspersky Endpoint Security.

- Настроить параметры проверки почты в программе Microsoft Office Outlook.

  Для почтового клиента Microsoft Office Outlook предусмотрено встраиваемое расширение, позволяющее удобно настраивать параметры проверки почты.

  Работая с остальными почтовыми клиентами (в том числе с Microsoft Outlook Express®, Windows Mail и Mozilla™ Thunderbird™), компонент Защита от почтовых угроз проверяет трафик почтовых протоколов SMTP, POP3, IMAP и NNTP.

  > Работая с почтовым клиентом Mozilla Thunderbird, компонент Защита от почтовых угроз не проверяет на вирусы и другие программы, представляющие угрозу, сообщения, передаваемые по протоколу IMAP, в случае если используются фильтры, перемещающие сообщения из папки **Входящие**.

В этом разделе

Изменение уровня безопасности почты

Для защиты почты компонент Защита от почтовых угроз применяет разные наборы параметров. Такие наборы параметров называют *уровнями безопасности почты*. Установлены три уровня безопасности почты: **Высокий**, **Рекомендуемый**, **Низкий**. Параметры уровня безопасности почты **Рекомендуемый** считаются оптимальными, они рекомендованы специалистами "Лаборатории Касперского".

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

1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 46).
2. В левой части окна в разделе **Базовая защита** выберите подраздел **Защита от почтовых угроз**.

   В правой части окна отобразятся параметры компонента Защита от почтовых угроз.
3. В блоке **Уровень безопасности** выполните одно из следующих действий:
   - Если вы хотите установить один из предустановленных уровней безопасности почты (**Высокий**, **Рекомендуемый**, **Низкий**), выберите его при помощи ползунка.
   - Если вы хотите настроить уровень безопасности почты самостоятельно, нажмите на кнопку

Настройка и задайте параметры в открывшемся окне **Защита от почтовых угроз**.

После того как вы самостоятельно настроили уровень безопасности почты, название уровня безопасности почты в блоке **Уровень безопасности** изменится на **Другой**.

- Если вы хотите изменить настроенный самостоятельно уровень безопасности почты на **Рекомендуемый**, нажмите на кнопку **По умолчанию**.

4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

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. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 46).
2. В левой части окна в разделе **Базовая защита** выберите подраздел **Защита от почтовых угроз**.

   В правой части окна отобразятся параметры компонента 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**.

     Если выбран этот вариант действия, то 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.

   - **Лечить, блокировать, если лечение невозможно**.

     Если выбран этот вариант действия, то компонент Защита от почтовых угроз автоматически пытается вылечить все обнаруженные зараженные сообщения электронной почты. Если лечение невозможно, то компонент Защита от почтовых угроз блокирует зараженные сообщения электронной почты.

   - **Блокировать**.

     Если выбран этот вариант действия, то компонент Защита от почтовых угроз автоматически блокирует зараженные сообщения электронной почты без попытки их вылечить.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить 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. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 46).
2. В левой части окна в разделе **Базовая защита** выберите подраздел **Защита от почтовых угроз**.

   В правой части окна отобразятся параметры компонента Защита от почтовых угроз.
3. Нажмите на кнопку **Настройка**.

   Откроется окно **Защита от почтовых угроз**.
4. Выберите закладку **Общие**.
5. В блоке **Область защиты** выполните одно из следующих действий:
   - Выберите вариант **Входящие и исходящие сообщения**, если вы хотите, чтобы компонент Защита от почтовых угроз проверял все входящие и исходящие сообщения на вашем компьютере.
   - Выберите вариант **Только входящие сообщения**, если вы хотите, чтобы компонент Защита от почтовых угроз проверял только входящие сообщения на вашем компьютере.

     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.
6. В блоке **Встраивание в систему** выполните следующие действия:
   - Установите флажок **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 **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 **Дополнительно: расширение в Microsoft Office Outlook**.

     Если вы используете почтовый клиент, отличный от Microsoft Office Outlook, то при снятом флажке **Трафик POP3 / SMTP / NNTP / IMAP** компонент Защита от почтовых угроз не проверяет сообщения, передающиеся по почтовым протоколам POP3, SMTP, NNTP и IMAP.
   - Установите флажок **Дополнительно: расширение в Microsoft Office 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 **Дополнительно: расширение в Microsoft Office 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.

7. Нажмите на кнопку **OK**.
8. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Проверка составных файлов, вложенных в сообщения электронной почты

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

1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 46).
2. В левой части окна в разделе **Базовая защита** выберите подраздел **Защита от почтовых угроз**.

   В правой части окна отобразятся параметры компонента Защита от почтовых угроз.
3. Нажмите на кнопку **Настройка**.

   Откроется окно **Защита от почтовых угроз**.
4. Выберите закладку **Общие**.
5. В блоке **Проверка составных файлов** выполните следующие действия:
   - Снимите флажок **Проверять вложенные архивы**, если вы хотите, чтобы компонент Защита от почтовых угроз не выполнял проверку вложенных в сообщения архивов.
   - Снимите флажок **Проверять вложенные файлы офисных форматов**, если вы хотите, чтобы компонент Защита от почтовых угроз не выполнял проверку вложенных в сообщения файлов офисных форматов.
   - Установите флажок **Не проверять архивы размером более N МБ**, если вы хотите, чтобы компонент Защита от почтовых угроз не проверял вложенные в сообщения архивы размером более N мегабайт. Если вы установили этот флажок, укажите максимальный размер архивов в поле рядом с названием флажка.
   - Снимите флажок **Не проверять архивы более N с**, если вы хотите, чтобы компонент Защита от почтовых угроз проверял вложенные в сообщения архивы, если на их проверку затрачивается более N секунд.
6. Нажмите на кнопку **OK**.
7. Нажмите на кнопку **Сохранить**, чтобы сохранить 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. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 46).
2. В левой части окна в разделе **Базовая защита** выберите подраздел **Защита от почтовых угроз**.

   В правой части окна отобразятся параметры компонента Защита от почтовых угроз.
3. В блоке **Уровень безопасности** нажмите на кнопку **Настройка**.

   Откроется окно **Защита от почтовых угроз**.
4. В окне **Защита от почтовых угроз** выберите закладку **Фильтр вложений**.
5. 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.
   - Выберите вариант **Удалять вложения указанных типов**, если вы хотите, чтобы компонент Защита от почтовых угроз удалял вложенные в сообщения файлы указанных типов.
6. Если на предыдущем шаге инструкции вы выбрали вариант **Переименовывать вложения указанных типов** или вариант **Удалять вложения указанных типов**, установите флажки напротив нужных типов файлов.

   Вы можете изменить список типов файлов с помощью кнопок **Добавить**, **Изменить**, **Удалить**.
7. Нажмите на кнопку **ОК**.
8. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Проверка почты в Microsoft Office Outlook

Во время установки Kaspersky Endpoint Security в программу Microsoft Office Outlook (далее также "Outlook") встраивается расширение компонента Защита от почтовых угроз. Оно позволяет перейти к настройке параметров компонента Защита от почтовых угроз из программы Outlook, а также указать, в какой момент проверять сообщения электронной почты на присутствие вирусов и других программ, представляющих угрозу. Расширение компонента Защита от почтовых угроз для Outlook может проверять входящие и исходящие сообщения, переданные по протоколам POP3, SMTP, NNTP, IMAP и MAPI.

Настройка параметров компонента Защита от почтовых угроз из программы Outlook доступна в том случае, если в интерфейсе программы Kaspersky Endpoint Security установлен флажок **Дополнительно: расширение в Microsoft Office Outlook**.

В программе Outlook входящие сообщения сначала проверяет компонент Защита от почтовых угроз (если в интерфейсе программы Kaspersky Endpoint Security установлен флажок **Трафик POP3 / SMTP / NNTP / IMAP**), затем входящие сообщения проверяет расширение компонента Защита от почтовых угроз для Outlook. Если компонент Защита от почтовых угроз обнаруживает в сообщении вредоносный объект, он уведомляет вас об этом.

Исходящие сообщения сначала проверяет расширение компонента Защита от почтовых угроз для Outlook, а затем проверяет компонент Защита от почтовых угроз.

Настройка проверки почты в программе Outlook

► *Чтобы перейти к настройке проверки почты в программе Outlook 2007, выполните следующие действия:*

1. Откройте главное окно Outlook 2007.
2. В меню программы выберите пункт **Сервис → Параметры**.

   Откроется окно **Параметры**.
3. В окне **Параметры** выберите закладку **Защита почты**.

► *Чтобы перейти к настройке проверки почты в программе Outlook 2010 / 2013 / 2016, выполните следующие действия:*

1. Откройте главное окно Outlook.

   В верхнем левом углу выберите закладку **Файл**.
2. Нажмите на кнопку **Параметры**.

   Откроется окно **Параметры Outlook**.
3. Выберите раздел **Надстройки**.

   В правой части окна отобразятся параметры встроенных в Outlook плагинов.
4. Нажмите на кнопку **Параметры надстроек**.

Настройка проверки почты с помощью Kaspersky Security Center

В случае проверки почты с помощью расширения компонента Защита от почтовых угроз для Outlook рекомендуется использовать режим кеширования сервера Exchange (Use Cached Exchange Mode). Более подробную информацию о режиме кеширования Exchange и рекомендациях по его использованию вы можете найти в базе знаний Майкрософт: https://technet.microsoft.com/ru-ru/library/cc179175.aspx.

► *Чтобы настроить режим работы расширения компонента Защита от почтовых угроз для Outlook с помощью Kaspersky Security Center, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева Консоли администрирования откройте папку с названием группы администрирования, для которой вы хотите настроить проверку почты.
3. В рабочей области выберите закладку **Политики**.
4. Выберите нужную политику.
5. Откройте окно **Свойства: <Название политики>** одним из следующих способов:
   - В контекстном меню политики выберите пункт **Свойства**.
   - Перейдите по ссылке **Настроить параметры политики**, которая находится в правой части рабочей области Консоли администрирования.
6. В разделе **Базовая защита** выберите подраздел **Защита от почтовых угроз**.
7. В блоке **Уровень безопасности** нажмите на кнопку **Настройка**.

   Откроется окно **Защита от почтовых угроз**.
8. В блоке **Встраивание в систему** нажмите на кнопку **Настройка**.

   Откроется окно **Защита почты**.
9. В окне **Защита почты** выполните следующие действия:
   - Установите флажок **Проверять при получении**, если вы хотите, чтобы расширение компонента Защита от почтовых угроз для Outlook проверяло входящие сообщения в момент их поступления в почтовый ящик.
   - Установите флажок **Проверять при прочтении**, если вы хотите, чтобы расширение компонента Защита от почтовых угроз для Outlook проверяло входящие сообщения в тот момент, когда пользователь открывает их для чтения.
   - Установите флажок **Проверять при отправке**, если вы хотите, чтобы расширение компонента Защита от почтовых угроз для Outlook проверяло исходящие сообщения в момент их отправки.
10. Нажмите на кнопку **ОК** в окне **Защита почты**.
11. Нажмите на кнопку **ОК** в окне **Защита от почтовых угроз**.
12. Примените политику.

    Подробнее о применении политики Kaspersky Security Center вы можете прочитать в *Руководстве администратора для Kaspersky Security Center.*

Защита от сетевых угроз

Этот раздел содержит информацию о Защите от сетевых угроз и инструкции о том, как настроить параметры компонента.

В этом разделе

О Защите от сетевых угроз

Компонент Защита от сетевых угроз отслеживает во входящем сетевом трафике активность, характерную для сетевых атак. Обнаружив попытку сетевой атаки на компьютер пользователя, Kaspersky Endpoint Security блокирует сетевую активность атакующего компьютера. После этого на экран выводится уведомление о том, что была попытка сетевой атаки, с указанием информации об атакующем компьютере.

Сетевая активность атакующего компьютера блокируется на один час. Вы можете изменить параметры блокирования атакующего компьютера (см. раздел "Изменение параметров блокирования атакующего компьютера" на стр. 118).

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

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. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 46).
2. В левой части окна в разделе **Базовая защита** выберите подраздел **Защита от сетевых угроз**.

   В правой части окна отобразятся параметры компонента Защита от сетевых угроз.
3. Выполните следующие действия:
   - Установите флажок **Включить Защиту от сетевых угроз**, если вы хотите включить Защиту от сетевых угроз.
   - Снимите флажок **Включить Защиту от сетевых угроз**, если вы хотите выключить Защиту от сетевых угроз.

4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Настройка Защиты от сетевых угроз

Вы можете выполнить следующие действия для настройки работы Защиты от сетевых угроз:

- настроить параметры блокирования атакующего компьютера;
- сформировать список адресов для исключения из блокирования.

В этом разделе

Изменение параметров блокирования атакующего компьютера

► *Чтобы изменить параметры блокирования атакующего компьютера, выполните следующие действия:*

1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 46).
2. В левой части окна в разделе **Базовая защита** выберите подраздел **Защита от сетевых угроз**.

   В правой части окна отобразятся параметры компонента Защита от сетевых угроз.
3. Установите флажок **Добавить атакующий компьютер в список блокирования на**.

   Если этот флажок установлен, то, обнаружив попытку сетевой атаки, компонент Защита от сетевых угроз блокирует сетевую активность атакующего компьютера в течение заданного времени, чтобы автоматически защитить компьютер от возможных будущих сетевых атак с этого адреса.

   Если этот флажок снят, то, обнаружив попытку сетевой атаки, компонент Защита от сетевых угроз не включает автоматическую защиту от возможных будущих сетевых атак с этого адреса.
4. Измените время блокирования атакующего компьютера в поле, расположенном справа от флажка **Добавить атакующий компьютер в список блокирования на**.
5. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Настройка адресов исключений из блокирования

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

1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 46).
2. В левой части окна в разделе **Базовая защита** выберите подраздел **Защита от сетевых угроз**.

   В правой части окна отобразятся параметры компонента Защита от сетевых угроз.

3. Нажмите на кнопку **Исключения**.

   Откроется окно **Исключения**.

4. Выполните одно из следующих действий:

   - Если хотите добавить новый IP-адрес, нажмите на кнопку **Добавить**.
   - Если хотите изменить добавленный ранее IP-адрес, выберите его в списке адресов и нажмите на кнопку **Изменить**.

   Откроется окно **IP-адрес**.

5. Введите IP-адрес компьютера, сетевые атаки с которого не должны блокироваться.
6. Нажмите на кнопку **ОК** в окне **IP-адрес**.
7. Нажмите на кнопку **ОК** в окне **Исключения**.
8. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Сетевой экран

Компонент Сетевой экран в сертифицируемой версии программы Kaspersky Endpoint Security должен быть выключен. Включение Сетевого экрана приводит к выходу программы из сертифицируемого состояния.

Защита от атак BadUSB

Этот раздел содержит информацию о компоненте Защита от атак BadUSB.

В этом разделе

О Защите от атак BadUSB

Некоторые вирусы изменяют встроенное программное обеспечение USB-устройств так, чтобы операционная система определяла USB-устройство как клавиатуру.

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) цифровой код, сформированный программой. Эта процедура называется авторизацией клавиатуры. Программа разрешает использование авторизованной клавиатуры и блокирует использование клавиатуры, не прошедшей авторизацию.

Защита от атак BadUSB работает в фоновом режиме сразу после установки компонента. Если к компьютеру с установленной программой Kaspersky Endpoint Security не применена политика Kaspersky Security Center, вы можете включать и выключать Защиту от атак BadUSB с помощью временной приостановки и возобновления защиты и контроля компьютера (см. раздел "Приостановка и возобновление защиты и контроля компьютера" на стр. 58).

Установка компонента Защита от атак BadUSB

Если во время установки Kaspersky Endpoint Security вы выбрали базовый или стандартный тип установки (см. раздел "Шаг 4. Выбор типа установки" на стр. 21), компонент Защита от атак BadUSB не будет доступен. Для его установки требуется изменить состав компонентов программы.

► *Чтобы установить компонент Защита от атак BadUSB, 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 / 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**.
5. В окне мастера установки программы **Изменение, восстановление или удаление программы** нажмите на кнопку **Изменение**.

   Откроется окно **Выборочная установка** мастера установки программы.
6. В группе компонентов **Базовая защита** в контекстном меню значка рядом с названием компонента **Защита от атак BadUSB** выберите пункт **Компонент будет установлен на локальный жесткий диск**.
7. Нажмите на кнопку **Далее**.
8. Следуйте указаниям мастера установки программы.

Включение и выключение Защиты от атак BadUSB

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

1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 46).
2. В левой части окна в разделе **Базовая защита** выберите подраздел **Защита от атак BadUSB**.

   В правой части окна отобразятся параметры компонента Защита от атак BadUSB.
3. Выполните одно из следующих действий:
   - Установите флажок **Включить Защиту от атак BadUSB**, если вы хотите включить Защиту от атак BadUSB.
   - Снимите флажок **Включить Защиту от атак BadUSB**, если вы хотите выключить Защиту от атак BadUSB.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Разрешение и запрещение использования экранной клавиатуры при авторизации

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. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров

программы" на стр. 46).

2. В левой части окна в разделе **Базовая защита** выберите подраздел **Защита от атак BadUSB**.

   В правой части окна отобразятся параметры компонента.

3. Выполните одно из следующих действий:

   - Установите флажок **Запретить использование экранной клавиатуры для авторизации USB-устройств**, если вы хотите запретить использование экранной клавиатуры для авторизации.
   - Снимите флажок **Запретить использование экранной клавиатуры для авторизации USB-устройств**, если вы хотите разрешить использование экранной клавиатуры для авторизации.

4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Авторизация клавиатуры

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

Программа требует авторизацию подключенного USB-устройства, определенного операционной системой как клавиатура, если включен запрос авторизации USB-клавиатур. Пользователь не может использовать неавторизованную клавиатуру до тех пор, пока она не будет авторизована.

Если запрос авторизации USB-клавиатур выключен, пользователь может использовать все подключенные клавиатуры. Сразу после включения запроса авторизации USB-клавиатур программа запрашивает авторизацию для каждой подключенной неавторизованной клавиатуры.

► *Чтобы авторизовать клавиатуру, выполните следующие действия:*

1. При включенной авторизации USB-клавиатур подключите клавиатуру к USB-порту.

   Откроется окно **Авторизация клавиатуры <Название клавиатуры>** с информацией о подключенной клавиатуре и цифровым кодом для ее авторизации.

2. С подключенной или экранной клавиатуры, если она доступна, последовательно введите случайно сформированной в окне авторизации цифровой код.

3. Нажмите на кнопку **OK**.

   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.

Контроль программ

Этот раздел содержит информацию о Контроле программ и инструкции о том, как настроить параметры компонента.

В этом разделе

О Контроле программ

Компонент Контроль программ отслеживает попытки запуска программ пользователями и регулирует запуск программ с помощью *правил Контроля программ* (см. раздел "*О правилах Контроля программ*" на стр. 126).

Запуск программ, параметры которых не удовлетворяют ни одному из правил Контроля программ, регулируется выбранным режимом работы компонента. По умолчанию выбран режим *Черный список* (см. раздел "*О режимах работы Контроля программ*" на стр. 135). Этот режим разрешает любым пользователям запускать любые программы.

Все попытки запуска программ пользователями фиксируются в отчетах (см. раздел "Работа с отчетами" на стр. 203).

Включение и выключение Контроля программ

По умолчанию Контроль программ включен, вы можете выключить Контроль программ при необходимости.

► *Чтобы включить или выключить Контроль программ выполните следующие действия:*

1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 46).
2. В левой части окна в разделе **Контроль безопасности** выберите подраздел **Контроль программ**.

В правой части окна отобразятся параметры компонента Контроль программ.

3. Выполните одно из следующих действий:
   - Установите флажок **Включить Контроль программ**, если вы хотите включить Контроль программ.
   - Снимите флажок **Включить Контроль программ**, если вы хотите выключить Контроль программ.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

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 Kaspersky Endpoint Security 10 Service Pack 2 для Windows до Kaspersky Endpoint Security 11 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.

- 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.

О правилах Контроля программ

Kaspersky Endpoint Security контролирует запуск программ пользователями с помощью правил. В правиле Контроля программ содержатся условия срабатывания и действие 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" (см. рис. ниже). На основании условий срабатывания правила Kaspersky Endpoint Security применяет (или не применяет) правило к программе.

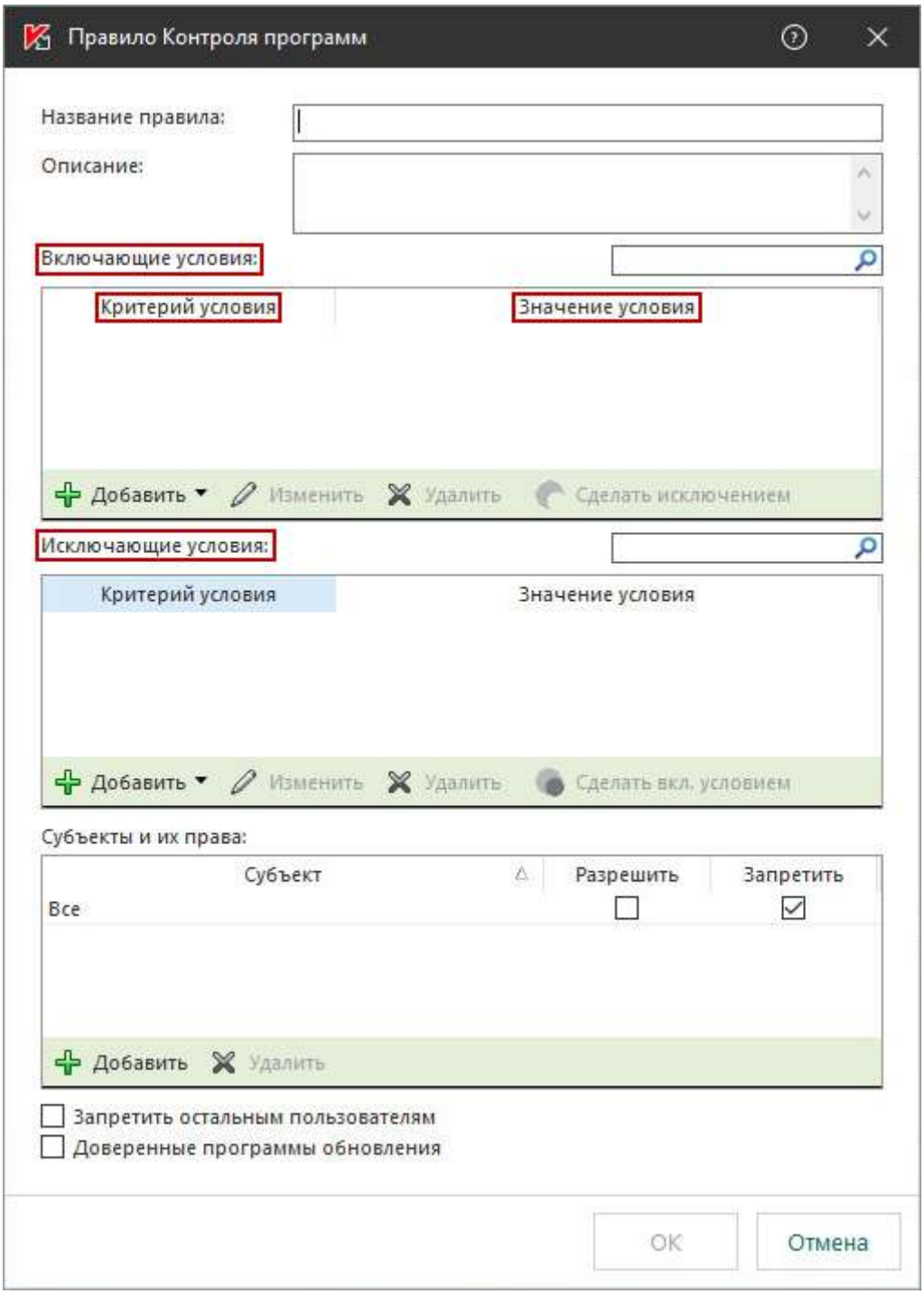


Figure 1: Правило контроля запуска программ. Параметры условия срабатывания правила

В правилах используются включающие и исключающие условия:

- *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.

Правила Контроля программ по умолчанию

По умолчанию Контроль программ работает в режиме Черный список. Компонент разрешает запуск всех программ всем пользователям. При попытке пользователя запустить программу, запрещенную правилами

Контроля программ, Kaspersky Endpoint Security блокирует запуск этой программы (если выбрано действие **Блокировать**) или сохраняет информацию о запуске программы в отчет (если выбрано действие **Уведомлять**).

Действия с правилами Контроля программ

Вы можете выполнить следующие действия с правилами Контроля программ:

- Добавить новое правило.
- Сформировать или изменить условия срабатывания правила.
- Изменить статус работы правила.

  Правило Контроля программ может быть включено, выключено или переведено в тестовый режим. По умолчанию после создания правило Контроля программ включено.
- Удалить правило.

В этом разделе

Добавление и изменение правила Контроля программ

► *Чтобы добавить или изменить правило Контроля программ, выполните следующие действия:*

1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 46).
2. В левой части окна в разделе **Контроль безопасности** выберите подраздел **Контроль программ**.

   В правой части окна отобразятся параметры компонента Контроль программ.
3. Установите флажок **Включить Контроль программ**, чтобы параметры компонента стали доступными для изменения.
4. Выполните одно из следующих действий:
   - Если вы хотите добавить правило, нажмите на кнопку **Добавить**.
   - Если вы хотите изменить существующее правило, выберите правило в списке и нажмите на кнопку **Изменить**.

   Откроется окно **Правило Контроля программ**.
5. Задайте или измените параметры правила:
   a. В поле **Название правила** введите или измените название правила.

b. В таблице **Включающие условия** сформируйте (см. раздел "Добавление условия срабатывания в правило Контроля программ" на стр. 131) или измените список включающих условий срабатывания правила с помощью кнопок **Добавить**, **Изменить**, **Удалить**, **Сделать исключением**.

c. В таблице **Исключающие условия** сформируйте или измените список исключающих условий срабатывания правила с помощью кнопок **Добавить**, **Изменить**, **Удалить**, **Сделать вкл. условием**.

d. Если требуется, измените тип условия срабатывания правила:

- Чтобы сменить тип условия с включающего на исключающее, выберите условие в таблице **Включающие условия** и нажмите на кнопку **Сделать исключением**.
- Чтобы сменить тип условия с исключающего на включающее, выберите условие в таблице **Исключающие условия** и нажмите на кнопку **Сделать вкл. условием**.

e. 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**.

Откроется окно Microsoft Windows **Выбор пользователей или групп**. В этом окне вы можете выбрать пользователей и / или группы пользователей.

По умолчанию в список пользователей добавлено значение **Everyone**. Действие правила распространяется на всех пользователей.

> Если в таблице не указан ни один пользователь, правило не может быть сохранено.

f. В таблице **Субъекты и их права** установите флажки **Разрешить** или **Запретить** напротив пользователей и / или групп пользователей, чтобы определить их право на запуск программ.

Флажок, установленный по умолчанию зависит от режима работы Контроля программ (см. раздел "О режимах работы Контроля программ" на стр. 135).

g. 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**.

h. 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. Нажмите на кнопку **OK**.
7. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Добавление условия срабатывания в правило Контроля программ

► *Чтобы добавить новое условие срабатывания в правило Контроля программ, выполните следующие действия:*

1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 46).
2. В левой части окна в разделе **Контроль безопасности** выберите подраздел Контроль программ.

   В правой части окна отобразятся параметры компонента Контроль программ.
3. Установите флажок **Включить Контроль программ**, чтобы параметры компонента стали доступными для изменения.
4. Выполните одно из следующих действий:
   - Если вы хотите создать новое правило и добавить в него условие срабатывания, нажмите на кнопку **Добавить**.
   - Если вы хотите добавить условие срабатывания в существующее правило, выберите его в списке правил и нажмите на кнопку **Изменить**.

   Откроется окно **Правило Контроля программ**.
5. В таблице **Включающие условия** или **Исключающие условия** нажмите на кнопку **Добавить**.

С помощью раскрывающегося списка кнопки **Добавить** вы можете добавлять в правило различные условия срабатывания (см. инструкции ниже).

► *Чтобы добавить условие срабатывания правила на основе свойств файлов в указанной папке, выполните следующие действия:*

1. В раскрывающемся списке кнопки **Добавить** выберите пункт **Условие(я) из свойств файлов указанной папки**.

   Откроется стандартное окно Microsoft Windows **Выбор папки**.
2. В окне **Выбор папки** выберите папку с исполняемыми файлами программ, на основе свойств которых вы хотите сформировать одно или несколько условий срабатывания правила.
3. Нажмите на кнопку **OK**.

   Откроется окно **Добавление условий**.
4. В раскрывающемся списке **Показать критерий** выберите критерий, на основе которого вы хотите создать одно или несколько условий срабатывания правила: **Хеш файла**, **Сертификат**, **KL-категория**, **Метаданные** или **Путь к папке**.

   Kaspersky Endpoint Security не поддерживает MD5-хеш файла и не контролирует запуск приложений на основе MD5-хеша. В качестве условия срабабатывания правила используется SHA256-хеш.
5. Если в раскрывающемся списке **Показать критерий** вы выбрали элемент **Метаданные**, установите флажки напротив тех свойств исполняемых файлов программы, которые вы хотите использовать в условии срабатывании правила: **Название файла**, **Версия файла**, **Название программы**, **Версия программы**, **Производитель**.

Если не выбрано ни одно из указанных свойств, правило не может быть сохранено.

6. Если в раскрывающемся списке **Показать критерий** вы выбрали элемент **Сертификат**, установите флажки напротив тех параметров, которые вы хотите использовать в условии срабатывании правила: **Издатель**, **Субъект**, **Отпечаток**.

   Если не выбран ни один из указанных параметров, правило не может быть сохранено.

   > Не рекомендуется использовать в качестве условий срабатывания правил только критерии **Издатель** и **Субъект**. Использование этих критериев является ненадежным.

7. Установите флажки напротив названий исполняемых файлов программ, свойства которых вы хотите включить в условия срабатывания правила.
8. Нажмите на кнопку **Далее**.

   Отобразится список сформированных условий срабатывания правила.

9. В списке сформированных условий срабатывания правила установите флажки около тех условий срабатывания правила, которые вы хотите добавить в правило Контроля программ.
10. Нажмите на кнопку **Завершить**.

► *Чтобы добавить условие срабатывания правила на основе свойств программ, запускавшихся на компьютере, выполните следующие действия:*

1. В раскрывающемся списке кнопки **Добавить** выберите пункт **Условие(я) из свойств запускавшихся программ**.
2. В окне **Добавление условий** в раскрывающемся списке **Показать критерий** выберите критерий, на основе которого вы хотите создать одно или несколько условий срабатывания правила: **Хеш файла**, **Сертификат**, **KL-категория**, **Метаданные** или **Путь к папке**.
3. Если в раскрывающемся списке **Показать критерий** вы выбрали элемент **Метаданные**, установите флажки напротив тех свойств исполняемых файлов программы, которые вы хотите использовать в условии срабатывании правила: **Название файла**, **Версия файла**, **Название программы**, **Версия программы**, **Производитель**.

   Если не выбрано ни одно из указанных свойств, правило не может быть сохранено.

4. Если в раскрывающемся списке **Показать критерий** вы выбрали элемент **Сертификат**, установите флажки напротив тех параметров, которые вы хотите использовать в условии срабатывании правила: **Издатель**, **Субъект**, **Отпечаток**.

   Если не выбран ни один из указанных параметров, правило не может быть сохранено.

   > Не рекомендуется использовать в качестве условий срабатывания правил только критерии **Издатель** и **Субъект**. Использование этих критериев является ненадежным.

5. Установите флажки напротив названий исполняемых файлов программ, свойства которых вы хотите включить в условия срабатывания правила.
6. Нажмите на кнопку **Далее**.

   Отобразится список сформированных условий срабатывания правила.

7. В списке сформированных условий срабатывания правила установите флажки около тех условий срабатывания правила, которые вы хотите добавить в правило Контроля программ.

8. Нажмите на кнопку **Завершить**.

► *Чтобы добавить условие срабатывания правила на основе KL-категории, выполните следующие действия:*

1. В раскрывающемся списке кнопки **Добавить** выберите пункт **Условие(я) "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.

2. В окне **Условие(я) "KL-категория"** установите флажки около названий тех KL-категорий, на основе которых вы хотите создать условия срабатывания правила.

   Вы можете нажать на кнопку ⊞ слева от названия KL-категории, чтобы просмотреть вложенные KL-категории.

3. Нажмите на кнопку **OK**.

► *Чтобы добавить условие срабатывания правила, сформированное вручную, выполните следующие действия:*

1. В раскрывающемся списке под кнопкой **Добавить** выберите пункт **Условие вручную**.
2. Нажмите на кнопку **Выбрать** в окне **Пользовательское условие** и укажите путь к исполняемому файлу программы.
3. Выберите критерий, на основе которого вы хотите создать условие срабатывания правила: **Хеш файла**, **Сертификат**, **Метаданные** или **Путь к файлу или папке**.

   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**.

4. Если требуется, настройте параметры выбранного критерия.
5. Нажмите на кнопку **OK**.

► *Чтобы добавить условие срабатывания на основе информации о носителе исполняемого файла программы, выполните следующие действия:*

1. В раскрывающемся списке под кнопкой **Добавить** выберите пункт **Условие по носителю файла**.
2. В окне **Условие по носителю файла** в раскрывающемся списке **Носитель** выберите тип носителя, запуск программ с которого будет условием срабатывания правила.
3. Нажмите на кнопку **OK**.

Изменение статуса правила Контроля программ

► *Чтобы изменить статус правила Контроля программ, выполните следующие действия:*

1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров

программы" на стр. 46).

2. В левой части окна в разделе **Контроль безопасности** выберите подраздел **Контроль программ**.

   В правой части окна отобразятся параметры компонента Контроль программ.

3. Установите флажок **Включить Контроль программ**, чтобы параметры компонента стали доступными для изменения.
4. Выберите правило, статус которого вы хотите изменить.
5. В графе **Статус** по левой клавише мыши откройте контекстное меню и выберите один из следующих пунктов:

   - **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 всегда разрешает запуск программ, на которые распространяется действие этого правила, но заносит информацию о запуске этих программ в отчет.

   > С помощью статуса **Тест** вы можете назначить действие **Уведомлять (см. раздел "Тестирование правил Контроля программ" на стр.** 134**)** для части правил, при выбранном варианте **Блокировать** в раскрывающемся списке **Действие**.

6. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Тестирование правил Контроля программ

Чтобы убедиться, что правила Контроля программ не блокируют программы, необходимые для работы, рекомендуется после создания правил перевести их в тестовый режим и проанализировать их работу.

Для анализа работы правил Контроля программ требуется изучить события о работе компонента Контроль программ, приходящие на Kaspersky Security Center. Если разрешен запуск всех программ, которые необходимы для работы пользователю компьютера, то созданы верные правила. В противном случае рекомендуется уточнить параметры созданных вами правил.

По умолчанию тестовый режим для правил Контроля программ выключен.

► *Чтобы включить тестовый режим для правил Контроля программ, выполните следующие действия:*

1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 46).
2. В левой части окна в разделе **Контроль безопасности** выберите подраздел **Контроль программ**.

   В правой части окна отобразятся параметры компонента Контроль программ.

3. Установите флажок **Включить Контроль программ**, чтобы параметры компонента стали доступными для изменения.
4. В раскрывающемся списке **Режим Контроля программ** выберите один из следующих элементов:

   - **Черный список**, если вы хотите разрешать запуск всех программ, кроме программ, указанных в

запрещающих правилах.

- **Белый список**, если вы хотите запрещать запуск всех программ, кроме программ, указанных в разрешающих правилах.

5. В раскрывающемся списке **Действие** выберите элемент **Уведомлять**.
6. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Kaspersky Endpoint Security не будет блокировать программы, запуск которых запрещен правилами Контроля программ, но будет отправлять уведомления об их запуске на Сервер администрирования.

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. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 46).
2. В левой части окна в разделе **Контроль безопасности** выберите подраздел **Контроль программ**.

   В правой части окна отобразятся параметры компонента Контроль программ.
3. Установите флажок **Включить Контроль программ**, чтобы параметры компонента стали доступными для изменения.
4. Нажмите на кнопку **Шаблоны**.

   Откроется окно **Шаблоны сообщений**.
5. Выполните одно из следующих действий:
   - Если вы хотите изменить шаблон сообщения о блокировке запуска программы, выберите закладку **Блокировка**.
   - Если вы хотите изменить шаблон сообщения для администратора локальной сети организации, выберите закладку **Сообщение администратору**.
6. Измените шаблон сообщения о блокировке или сообщения администратору. Для этого используйте кнопки **По умолчанию** и **Переменная**.
7. Нажмите на кнопку **ОК**.
8. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

О режимах работы Контроля программ

Компонент Контроль программ может работать в двух режимах:

- **Черный список**. Режим, при котором Контроль программ разрешает всем пользователям запуск

любых программ, кроме тех, которые указаны в запрещающих правилах Контроля программ (см. раздел "О правилах Контроля программ" на стр. 126).

Этот режим работы Контроля программ установлен по умолчанию.

- **Белый список**. Режим, при котором Контроль программ запрещает всем пользователям запуск любых программ, кроме тех, которые указаны в разрешающих 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 белого списка (см. раздел "Лучшие практики по внедрению режима белого списка" на стр. 150).

В каждом режиме доступно два действия над запускаемыми программами: Kaspersky Endpoint Security может блокировать запуск программ или уведомлять пользователя о запуске программы, соответствующей условиям правил Контроля 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 (на стр. 139).

  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 (см. раздел "Получение информации о программах, которые установлены на компьютерах пользователей" на стр. 138).

Поэтому настройку работы компонента Контроль программ рекомендуется выполнять с помощью Kaspersky Security Center.

Выбор режима Контроля программ

► *Чтобы выбрать режим Контроля программ, выполните следующие действия:*

1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 46).
2. В левой части окна в разделе **Контроль безопасности** выберите подраздел **Контроль программ**.

   В правой части окна отобразятся параметры компонента Контроль программ.
3. Установите флажок **Включить Контроль программ**, чтобы параметры компонента стали доступными для изменения.
4. В раскрывающемся списке **Режим Контроля программ** выберите один из следующих элементов:
   - **Черный список**, если вы хотите разрешать запуск всех программ, кроме программ, указанных в запрещающих правилах;
   - **Белый список**, если вы хотите запрещать запуск всех программ, кроме программ, указанных в

разрешающих правилах.

Для режима белого списка изначально задано правило **Операционная система и ее компоненты**, которое разрешает запуск программ, входящих в KL-категорию Золотая категория, и правило **Доверенные программы обновления**, которое разрешает запуск программ, входящих в KL-категорию Доверенные программы обновления. В KL-категорию Золотая категория 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 **Операционная система и ее компоненты** 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 в раскрывающемся списке **Режим Контроля программ**.

5. В раскрывающемся списке **Действие** выберите, какое действие компонент должен выполнять при попытке пользователя запустить программу, запрещенную правилами Контроля программ.
6. Установите флажок **Контролировать DLL и драйверы**, если вы хотите, чтобы Kaspersky Endpoint Security контролировал 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 **Контролировать DLL и драйверы**. Перезагрузите компьютер после установки флажка **Контролировать DLL и драйверы**, если вы хотите, чтобы Kaspersky Endpoint Security контролировал 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 разделе **Контроль программ** включено правило по умолчанию **Операционная система и ее компоненты** 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 **Операционная система и ее компоненты** может привести к нестабильности операционной системы.

   Правила Контроля программ, созданные на основе других KL-категорий (за исключением KL-категории Доверенные сертификаты), не применяются при контроле загрузки DLL-модулей и драйверов.

   Рекомендуется включить защиту паролем 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.

7. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Управление правилами Контроля программ с помощью Kaspersky Security Center

Этот раздел содержит информацию о настройке Контроля программ с помощью Kaspersky Security Center и рекомендации по оптимальному использованию Контроля программ.

В этом разделе

Получение информации о программах, которые установлены на компьютерах пользователей

Для создания оптимальных правил Контроля программ рекомендуется получить представление о программах, используемых на компьютерах локальной сети организации. Для этого вы можете получить следующую информацию:

- производители, версии и локализации программ, которые используются в локальной сети организации;
- регулярность обновлений программ;
- политики использования программ, принятые в организации (это могут быть политики безопасности или административные политики);
- расположение хранилища дистрибутивов программ.

Чтобы получить информацию о программах, которые используются на компьютерах локальной сети организации, вы можете использовать данные, представленные в папках **Реестр программ** и **Исполняемые файлы**. Папки **Реестр программ** и **Исполняемые файлы** входят в состав папки **Управление программами** дерева Консоли администрирования Kaspersky Security Center.

Папка **Реестр программ** содержит список программ, которые обнаружил на клиентских компьютерах установленный на них Агент администрирования.

Папка **Исполняемые файлы** содержит список исполняемых файлов, которые когда-либо запускались на

клиентских компьютерах или были обнаружены в процессе работы задачи инвентаризации для Kaspersky Endpoint Security.

Открыв окно свойств выбранной программы в папке **Реестр программ** или **Исполняемые файлы**, вы можете получить общую информацию о программе и о ее исполняемых файлах, а также просмотреть список компьютеров, на которых установлена эта программа.

Получение информации о программах, запускаемых на компьютерах пользователей

► *Чтобы включить отправку информации о программах, запускаемых на компьютерах с установленной программой Kaspersky Endpoint Security, на Сервер администрирования, 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.
5. Откройте окно **Свойства: <Название политики>** одним из следующих способов:
   - В контекстном меню политики выберите пункт **Свойства**.
   - Перейдите по ссылке **Настроить параметры политики**, которая находится в правой части рабочей области Консоли администрирования.
6. В разделе **Общие параметры** выберите подраздел **Отчеты и хранение**.
7. В правой части окна в блоке **Передача данных на Сервер администрирования** нажмите на кнопку **Настройка**

   Откроется окно **Информировать**.
8. Установите флажок **О запускаемых программах**.
9. Нажмите на кнопку **ОК** в окне **Информировать**.
10. Нажмите на кнопку **ОК** в окне **Свойства: <Название политики>**.

Создание категорий программ

Для удобства формирования правил Контроля программ вы можете создать категории программ.

Рекомендуется создать категорию "Программы для работы", которая включает в себя стандартный набор программ, используемых в организации. Если различные группы пользователей используют различные наборы программ для работы, вы можете создать отдельную категорию программ для работы каждой группы пользователей.

► *Чтобы создать категорию программ, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве Консоли администрирования выберите папку **Дополнительно** → **Управление**

программами → Категории программ.

3. В рабочей области нажмите на кнопку **Создать категорию**.

   Запустится мастер создания пользовательской категории.

4. Следуйте указаниям мастера создания пользовательской категории.

Шаг 1. Выбор типа категории

На этом шаге выберите один из следующих типов категорий программ:

- **Пополняемая вручную категория**. Если вы выбрали этот тип категории, то на шаге "Настройка условий для включения программ в категорию" и шаге "Настройка условий для исключения программ из категории" вы сможете задать критерии, по которым исполняемые файлы будут попадать в создаваемую категорию.
- **Категория, в которую входят исполняемые файлы с выбранных устройств**. Если вы выбрали этот тип категории, то на шаге "Параметры" вы сможете указать устройство, исполняемые файлы с которого должны попадать в категорию.
- **Автоматически пополняемая категория**. Укажите папку, исполняемые файлы из которой будут автоматически попадать в создаваемую категорию.

  При создании автоматически пополняемой категории Kaspersky Security Center выполняет инвентаризацию файлов следующих форматов: EXE, COM, DLL, SYS, BAT, PS1, CMD, JS, VBS, REG, MSI, MSC, CPL, HTML, HTM, DRV, OCX, SCR.

Шаг 2. Ввод названия пользовательской категории

На этом шаге укажите название категории программ.

Чтобы продолжить работу мастера установки программы, нажмите на кнопку **Далее**.

Шаг 3. Настройка условий для включения программ в категорию

Этот шаг доступен, если вы выбрали тип категории **Пополняемая вручную категория**.

На этом шаге в раскрывающемся списке **Добавить** выберите один или несколько из следующих критериев добавления условий для включения программ в категорию:

- **Из списка исполняемых файлов**. Добавьте программы из списка исполняемых файлов на клиентском устройстве в пользовательскую категорию.
- **Из свойств файла**. Укажите детальные данные исполняемых файлов в качестве условия добавления программ в пользовательскую категорию.
- **Метаданные файлов папки**. Выберите папку на клиентском устройстве, которая содержит исполняемые файлы. Kaspersky Security Center укажет метаданные этих исполняемых файлов в качестве условия добавления программ в пользовательскую категорию.
- **Хеши файлов папки**. Выберите выбрать папку на клиентском устройстве, которая содержит исполняемые файлы. Kaspersky Security Center укажет хеши этих исполняемых файлов в качестве

условия добавления программ в пользовательскую категорию.

- **Сертификаты файлов из папки**. Выберите папку на клиентском устройстве, которая содержит исполняемые файлы, подписанные сертификатами. Kaspersky Security Center укажет сертификаты этих исполняемых файлов в качестве условия добавления программ в пользовательскую категорию.

  Не рекомендуется использовать условия, в свойствах которых не указывается параметр **Отпечаток сертификата**.

- **Метаданные файлов установщика MSI**. Выберите установочный пакет MSI. Kaspersky Security Center укажет метаданные исполняемых файлов, упакованных в этот установочный пакет MSI, в качестве условия добавления программ в пользовательскую категорию.
- **Контрольные суммы файлов msi-инсталлятора программы**. Выберите установочный пакет MSI. Kaspersky Security Center укажет хеши исполняемых файлов, упакованных в этот установочный пакет MSI, в качестве условия добавления программ в пользовательскую категорию.
- **KL-категория**. Укажите KL-категорию в качестве условия добавления программ в пользовательскую категорию.

  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.

  Вы можете выбрать все KL-категории, чтобы сформировать расширенный список доверенных программ.
- **Папка программы**. Выберите папку на клиентском устройстве. Kaspersky Security Center добавит исполняемые файлы из этой папки в пользовательскую категорию.
- **Сертификаты из хранилища сертификатов**. Выберите сертификат из хранилища сертификатов в качестве условия добавления программ в пользовательскую категорию.

  Не рекомендуется использовать условия, в свойствах которых не указывается параметр **Отпечаток сертификата**.

- **Тип носителя**. Укажите тип носителя (все жесткие и съемные диски, или только съемные диски) в качестве условия добавления программ в пользовательскую категорию.

Чтобы продолжить работу мастера установки программы, нажмите на кнопку **Далее**.

Шаг 4. Настройка условий для исключения программ из категории

Этот шаг доступен, если вы выбрали тип категории **Пополняемая вручную категория**.
Программы, указанные на этом шаге, исключаются из категории, даже если эти программы были указаны на шаге "Настройка условий для включения программ в категорию".

На этом шаге в раскрывающемся списке **Добавить** выберите один из следующих критериев добавления условий для исключения программ из категории:

- **Из списка исполняемых файлов**. Добавьте программы из списка исполняемых файлов на клиентском устройстве в пользовательскую категорию.

- **Из свойств файла**. Укажите детальные данные исполняемых файлов в качестве условия добавления программ в пользовательскую категорию.
- **Метаданные файлов папки**. Выберите папку на клиентском устройстве, которая содержит исполняемые файлы. Kaspersky Security Center укажет метаданные этих исполняемых файлов в качестве условия добавления программ в пользовательскую категорию.
- **Хеши файлов папки**. Выберите выбрать папку на клиентском устройстве, которая содержит исполняемые файлы. Kaspersky Security Center укажет хеши этих исполняемых файлов в качестве условия добавления программ в пользовательскую категорию.
- **Сертификаты файлов из папки**. Выберите папку на клиентском устройстве, которая содержит исполняемые файлы, подписанные сертификатами. Kaspersky Security Center укажет сертификаты этих исполняемых файлов в качестве условия добавления программ в пользовательскую категорию.
- **Метаданные файлов установщика MSI**. Выберите установочный пакет MSI. Kaspersky Security Center укажет метаданные исполняемых файлов, упакованных в этот установочный пакет MSI, в качестве условия добавления программ в пользовательскую категорию.
- **Контрольные суммы файлов msi-инсталлятора программы**. Выберите установочный пакет MSI. Kaspersky Security Center укажет хеши исполняемых файлов, упакованных в этот установочный пакет MSI, в качестве условия добавления программ в пользовательскую категорию.
- **KL-категория**. Укажите KL-категорию в качестве условия добавления программ в пользовательскую категорию.
- **Папка программы**. Выберите папку на клиентском устройстве. Kaspersky Security Center добавит исполняемые файлы из этой папки в пользовательскую категорию программ.
- **Сертификаты из хранилища сертификатов**. Выберите сертификат из хранилища сертификатов в качестве условия добавления программ в пользовательскую категорию.
- **Тип носителя**. Укажите тип носителя (все жесткие и съемные диски, или только съемные диски) в качестве условия добавления программ в пользовательскую категорию.

Чтобы продолжить работу мастера установки программы, нажмите на кнопку **Далее**.

Шаг 5. Параметры

Этот шаг доступен, если вы выбрали тип категории **Категория, в которую входят исполняемые файлы с выбранных устройств**.

На этом шаге нажмите на кнопку **Добавить** и укажите компьютеры, исполняемые файлы с которых Kaspersky Security Centerдобавит в категорию программ. Kaspersky Security Center добавит в категорию программ все исполняемые файлы с указанных компьютеров, представленные в папке **Исполняемые файлы** (см. раздел "**Получение информации о программах, которые установлены на компьютерах пользователей**" на стр. 138).

Также на этом шаге вы можете настроить следующие параметры:

- Алгоритм вычисления хеш-функции программой Kaspersky Security Center. Для выбора алгоритма необходимо установить один из следующих флажков:
  - Флажок **Вычислять SHA-256 для файлов в категории (поддерживается для Kaspersky Endpoint Security 10 Service Pack 2 для Windows и выше)**.
  - Флажок **Вычислять MD5 для файлов в категории (поддерживается для версий ниже**

Kaspersky Endpoint Security 10 Service Pack 2 для Windows).

- Флажок **Синхронизировать с хранилищем Сервера администрирования**. Установите этот флажок, если вы хотите, чтобы Kaspersky Security Center периодически очищал категорию программ и добавлял в нее все исполняемые файлы с указанных компьютеров, представленные в папке **Исполняемые файлы**.

  Если флажок **Синхронизировать с хранилищем Сервера администрирования** снят, то после создания категории программ Kaspersky Security Center не будет вносить в нее изменения.

- Поле **Период проверки (ч)**. В поле вы можете указать период времени в часах, по истечении которого Kaspersky Security Center очищает категорию программ и добавляет в нее все исполняемые файлы с указанных компьютеров, представленные в папке **Исполняемые файлы**.

  Поле доступно, если установлен флажок **Синхронизировать с хранилищем Сервера администрирования**.

Чтобы продолжить работу мастера установки программы, нажмите на кнопку **Далее**.

Шаг 6. Папка хранилища

Этот шаг доступен, если вы выбрали тип категории **Автоматически пополняемая категория**.

На этом шаге нажмите на кнопку **Обзор** и укажите папку, в которой Kaspersky Security Center будет выполнять поиск исполняемых файлов для автоматического добавления в категорию программ.

Также на этом шаге вы можете настроить следующие параметры:

- Флажок **Включать в категорию динамически подключаемые библиотеки (DLL)**. Установите этот флажок, если вы хотите, чтобы в категорию программ включались динамически подключаемые библиотеки (файлы формата DLL) и компонент Контроль программ регистрировал действия таких библиотек, запущенных в системе.

  При включении файлов формата DLL в категорию программ возможно снижение производительности работы Kaspersky Security Center.

- Флажок **Включать в категорию данные о скриптах**. Установите этот флажок, если вы хотите, чтобы в категорию программ включались данные о скриптах и скрипты не блокировались компонентом Защита от веб-угроз.

  При включении данных о скриптах в категорию программ возможно снижение производительности работы Kaspersky Security Center.

- Алгоритм вычисления хеш-функции программой Kaspersky Security Center. Для выбора алгоритма необходимо установить один из следующих флажков:

  - Флажок **Вычислять SHA-256 для файлов в категории (поддерживается для Kaspersky Endpoint Security 10 Service Pack 2 для Windows и выше)**.

  - Флажок **Вычислять MD5 для файлов в категории (поддерживается для версий ниже Kaspersky Endpoint Security 10 Service Pack 2 для Windows)**.

- Флажок **Принудительно проверять папку на наличие изменений**. Установите этот флажок, если

вы хотите, чтобы Kaspersky Security Center периодически выполнял поиск исполняемых файлов в папке автоматического пополнения категории программ.

Если флажок **Принудительно проверять папку на наличие изменений** снят, Kaspersky Security Center выполняет поиск исполняемых файлов в папке автоматического пополнения категории программ, только если в этой папке были изменены, добавлены или удалены файлы.

- Поле **Период проверки (ч)**. В поле вы можете указать период времени в часах, по истечении которого Kaspersky Security Center проверяет на наличие изменений папку автоматического пополнения категории программ.

  Поле доступно, если установлен флажок **Принудительно проверять папку на наличие изменений**.

Чтобы продолжить работу мастера установки программы, нажмите на кнопку **Далее**.

Шаг 7. Создание пользовательской категории

Чтобы завершить работу мастера установки программы, нажмите на кнопку **Готово**.

Добавление в категорию программ исполняемых файлов из папки Исполняемые файлы

Чтобы добавить в категорию программ исполняемые файлы из папки Исполняемые файлы, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Дополнительно** дерева Консоли администрирования в папке **Управление программами** выберите папку **Исполняемые файлы**.
3. В папке **Исполняемые файлы** выберите исполняемые файл, которые вы хотите добавить в категорию программ.
4. По правой клавише мыши откройте контекстное меню для выбранных событий и выберите пункт **Добавить в категорию**.

   Откроется окно **Выберите пользовательскую категорию**.
5. В окне **Выберите пользовательскую категорию** выполните следующие действия:
   - В верхней части окна выберите один из следующих вариантов:
     - **Создать категорию программ**. Выберите этот вариант, если вы хотите создать новую категорию программ и добавить в нее исполняемые файлы.
     - **Добавить правила в указанную категорию**. Выберите этот вариант, если вы хотите выбрать существующую категорию программ и добавить в нее исполняемые файлы.
   - В блоке **Тип правила** выберите один из следующих вариантов:
     - **Добавить правила включения**. Выберите этот вариант, если вы хотите создать условие, добавляющее исполнительные файлы в категорию программ.
     - **Добавить правила исключения**. Выберите этот вариант, если вы хотите создать условие, исключающие исполнительные файлы из категории программ.
   - В блоке **Тип информации о файле** выберите один из следующих вариантов:

- **Данные сертификата или SHA-256 для файлов без сертификата**.
- **Данные сертификата (файлы без сертификата пропускаются)**.
- **Только SHA-256 (файлы без SHA-256 пропускаются)**.
- **MD5 (устаревший режим, только для версий Kaspersky Endpoint Security 10 Service Pack 1)**.

6. Нажмите на кнопку **ОК**.

Добавление в категорию программ исполняемых файлов, связанных с событиями

Чтобы добавить в категорию программ исполняемые файлы, связанные с событиями о работе компонента Контроль программ, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В узле **Сервер администрирования** дерева Консоли администрирования выберите закладку **События**.
3. Выберите выборку в раскрывающемся списке **События выборки**.
4. Нажмите на кнопку **Запустить выборку**.
5. Выберите события, исполняемые файл связанные с которыми вы хотите добавить в категорию программ.
6. По правой клавише мыши откройте контекстное меню для выбранных событий и выберите пункт **Добавить в категорию**.

   Откроется окно **Выберите пользовательскую категорию**.
7. В окне **Выберите пользовательскую категорию** выполните следующие действия:
   - В верхней части окна выберите один из следующих вариантов:
     - **Создать категорию программ**. Выберите этот вариант, если вы хотите создать новую категорию программ и добавить в нее исполняемые файлы.
     - **Добавить правила в указанную категорию**. Выберите этот вариант, если вы хотите выбрать существующую категорию программ и добавить в нее исполняемые файлы.
   - В блоке **Тип правила** выберите один из следующих вариантов:
     - **Добавить правила включения**. Выберите этот вариант, если вы хотите создать условие, добавляющее исполнительные файлы в категорию программ.
     - **Добавить правила исключения**. Выберите этот вариант, если вы хотите создать условие, исключающие исполнительные файлы из категории программ.
   - В блоке **Тип информации о файле** выберите один из следующих вариантов:
     - **Данные сертификата или SHA-256 для файлов без сертификата**.
     - **Данные сертификата (файлы без сертификата пропускаются)**.
     - **Только SHA-256 (файлы без SHA-256 пропускаются)**.
     - **MD5 (устаревший режим, только для версий Kaspersky Endpoint Security 10 Service Pack 1)**.

8. Нажмите на кнопку **ОК**.

Добавление и изменение правила Контроля программ с помощью Kaspersky Security Center

► *Чтобы добавить или изменить правило Контроля программ с помощью Kaspersky Security Center, 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.
5. Откройте окно **Свойства: <Название политики>** одним из следующих способов:
   - В контекстном меню политики выберите пункт **Свойства**.
   - Перейдите по ссылке **Настроить параметры политики**, которая находится в правой части рабочей области Консоли администрирования.
6. В разделе **Контроль безопасности** выберите подраздел **Контроль программ**.

   В правой части окна отобразятся параметры компонента Контроль программ.
7. Выполните одно из следующих действий:
   - Если вы хотите добавить правило, нажмите на кнопку **Добавить**.
   - Если вы хотите изменить существующее правило, выберите правило в списке и нажмите на кнопку **Изменить**.

   Откроется окно **Правило Контроля программ**.
8. Из раскрывающегося списка **Категория** выберите созданную категорию программ, на основе которой вы хотите создать правило.
9. В таблице **Субъекты и их права** нажмите на кнопку **Добавить**.

   Откроется стандартное окно Microsoft Windows **Выбор: "Пользователи" или "Группы"**.
10. В окне **Выбор: "Пользователи" или "Группы"** задайте список пользователей и / или групп пользователей, для которых вы хотите настроить возможность запускать программы, принадлежащие к выбранной категории.
11. В таблице **Субъекты и их права** выполните следующие действия:
    - Если вы хотите разрешить пользователям и / или группам пользователей запуск программ, принадлежащих к выбранной категории, установите флажок **Разрешить** в нужных строках.
    - Если вы хотите запретить пользователям и / или группам пользователей запуск программ, принадлежащих к выбранной категории, установите флажок **Запретить** в нужных строках.
12. Установите флажок **Запретить остальным пользователям**, если вы хотите, чтобы программа запрещала запуск программ, принадлежащих к выбранной категории, всем пользователям, которые не указаны в графе **Субъект** и не входят в группы пользователей, указанные в графе **Субъект**.
13. 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.

14. Нажмите на кнопку **OK**.
15. Нажмите на кнопку **Применить** в разделе **Контроль программ** окна свойств политики.

Изменение статуса правила Контроля программ с помощью Kaspersky Security Center

► *Чтобы изменить статус правила Контроля программ, 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.
5. Откройте окно **Свойства: <Название политики>** одним из следующих способов:
   - В контекстном меню политики выберите пункт **Свойства**.
   - Перейдите по ссылке **Настроить параметры политики**, которая находится в правой части рабочей области Консоли администрирования.
6. В разделе **Контроль безопасности** выберите подраздел **Контроль программ**.

   В правой части окна отобразятся параметры компонента Контроль программ.
7. Выберите правило Контроля программ, статус которого вы хотите изменить.
8. В графе **Статус** по левой клавише мыши откройте контекстное меню и выберите один из следующих пунктов:
   - **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 всегда разрешает запуск программ, на которые распространяется действие правила, но заносит информацию о запуске этих программ в отчет.

     С помощью статуса **Тест** вы можете назначить действие **Уведомлять** **(см. раздел "Тестирование правил Контроля программ" на стр. 134)** для части правил, при выбранном варианте **Блокировать** в раскрывающемся списке **Действие**.
9. Нажмите на кнопку **Применить**.

Тестирование правил Контроля программ с помощью Kaspersky Security Center

Чтобы убедиться, что правила Контроля программ не блокируют программы, необходимые для работы,

рекомендуется после создания правил включить для них тестовый режим и проанализировать их работу. При включении тестового режима Kaspersky Endpoint Security не будет блокировать программы, запуск которых запрещен правилами Контроля программ, но будет отправлять уведомления об их запуске на Сервер администрирования.

Для анализа работы правил Контроля программ требуется изучить события по результатам работы компонента Контроль программ, приходящие на Kaspersky Security Center. Если успешно запущены все программы, которые необходимы для работы пользователю компьютера, то созданы верные правила. В противном случае рекомендуется уточнить параметры созданных вами правил.

По умолчанию включен блокирующий режим для правил Контроля программ.

► *Чтобы включить тестовый режим или блокирующий режим для правил Контроля программ в Kaspersky Security Center, 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.
5. Откройте окно **Свойства: <Название политики>** одним из следующих способов:
   - В контекстном меню политики выберите пункт **Свойства**.
   - Перейдите по ссылке **Настроить параметры политики**, которая находится в правой части рабочей области Консоли администрирования.
6. В разделе **Контроль безопасности** выберите подраздел **Контроль программ**.

   В правой части окна отобразятся параметры компонента Контроль программ.
7. В раскрывающемся списке **Режим Контроля программ** выберите один из следующих элементов:
   - **Черный список**, если вы хотите разрешать запуск всех программ, кроме программ, указанных в запрещающих правилах.
   - **Белый список**, если вы хотите запрещать запуск всех программ, кроме программ, указанных в разрешающих правилах.
8. В раскрывающемся списке **Действие** выберите один из следующих элементов:
   - **Уведомлять**. Включение тестового режима для правил Контроля программ.
   - **Блокировать**. Включение блокирующего режима для правил Контроля программ.
9. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Просмотр событий о работе компонента Контроля программ в тестовом режиме

► *Чтобы просмотреть приходящие на Kaspersky Security Center события по результату работы компонента Контроль программ в тестовом режиме, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.

2. В узле **Сервер администрирования** дерева Консоли администрирования выберите закладку **События**.
3. Нажмите на кнопку **Создать выборку**.

   Откроется окно **Свойства: <Название выборки>**.
4. Откройте раздел **События**.
5. Нажмите на кнопку **Сбросить все**.
6. В таблице **События** установите флажки **Запуск программы запрещен в тестовом режиме** и **Запуск программы разрешен в тестовом режиме**.
7. Нажмите на кнопку **ОК**.
8. В раскрывающемся списке **События выборки** выберите созданную выборку.
9. Нажмите на кнопку **Запустить выборку**.

Просмотр отчета о тестовых запрещенных запусках

► *Чтобы просмотреть отчет о тестовых запрещенных запусках, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В узле **Сервер администрирования** дерева Консоли администрирования выберите закладку **Отчеты**.
3. Нажмите на кнопку **Создать шаблон отчета**.

   Запустится мастер создания шаблона отчета.
4. Следуйте указаниям мастера создания шаблона отчета. На шаге **Выбор типа шаблона отчета** в разделе **Прочее** выберите пункт **Отчет о тестовых запрещенных запусках**.

   После завершения работы мастера создания шаблона отчета в таблице на закладке **Отчеты** появится новый шаблон отчета.
5. Выберите шаблон отчета, созданный на предыдущих шагах инструкции.
6. В контекстном меню шаблона выберите пункт **Показать отчет**.

Запустится процесс формирования отчета. Отчет отобразится в новом окне.

Просмотр событий о работе компонента Контроль программ

► *Чтобы просмотреть приходящие на Kaspersky Security Center события по результату работы компонента Контроль программ, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В узле **Сервер администрирования** дерева Консоли администрирования выберите закладку **События**.
3. Нажмите на кнопку **Создать выборку**.

   Откроется окно **Свойства: <Название выборки>**.

4. Откройте раздел **События**.
5. Нажмите на кнопку **Сбросить все**.
6. В таблице **События** установите флажок **Запуск программы запрещен**.
7. Нажмите на кнопку **ОК**.
8. В раскрывающемся списке **События выборки** выберите созданную выборку.
9. Нажмите на кнопку **Запустить выборку**.

Просмотр отчета о запрещенных запусках

► *Чтобы просмотреть отчет о запрещенных запусках, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В узле **Сервер администрирования** дерева Консоли администрирования выберите закладку **Отчеты**.
3. Нажмите на кнопку **Создать шаблон отчета**.

   Запустится мастер создания шаблона отчета.
4. Следуйте указаниям мастера создания шаблона отчета. На шаге **Выбор типа шаблона отчета** в разделе **Прочее** выберите пункт **Отчет о запрещенных запусках**.

   После завершения работы мастера создания шаблона отчета в таблице на закладке **Отчеты** появится новый шаблон отчета.
5. Выберите шаблон отчета, созданный на предыдущих шагах инструкции.
6. В контекстном меню шаблона выберите пункт **Показать отчет**.

Запустится процесс формирования отчета. Отчет отобразится в новом окне.

Лучшие практики по внедрению режима белого списка

Этот раздел содержит рекомендации по внедрению режима белого списка (см. раздел "О режимах работы Контроля программ" на стр. 135).

Планирование внедрения режима белого списка

При планировании внедрения режима белого списка рекомендуется выполнить следующие действия:

1. Определить состав следующих категорий:
   - Группы пользователей. Группы пользователей, для которых необходимо разрешить использование различных наборов программ.
   - Группы администрирования. Одна или несколько групп компьютеров, к которым Kaspersky Security Center будет применять режим белого списка. Создание нескольких групп компьютеров необходимо, если для этих групп используются различные настройки режима белого списка.
2. Составить список программ, запуск которых необходимо разрешить.

   Перед составлением списка рекомендуется выполнить задачу инвентаризации и включить отправку

на Сервер администрирования информации о запускаемых на компьютере программах (см. раздел "Получение информации о программах, запускаемых на компьютерах пользователей" на стр. 139). После выполнения задачи инвентаризации вы можете просмотреть список исполняемых файлов (см. раздел "Получение информации о программах, которые установлены на компьютерах пользователей" на стр. 138). Информация о создании, изменении параметров и запуске задачи инвентаризации доступна в разделе Управление задачами (на стр. 246).

Настройка режима белого списка

При настройке режима белого списка рекомендуется выполнить следующие действия:

1. Создать категории программ (см. раздел "Создание категорий программ" на стр. 139), содержащие те программы, запуск которых необходимо разрешить.

   Вы можете выбрать один из следующих типов категорий программ:

   - **Пополняемая вручную категория** (см. раздел "**Шаг 3. Настройка условий для включения программ в категорию**" на стр. 140). Вы можете вручную пополнять эту категорию, используя следующие условия:
     - Метаданные файла. Если используется это условие, Kaspersky Security Center добавляет в категорию программ все исполняемые файлы, имеющие указанные метаданные.
     - Хеш файла. Если используется это условие, Kaspersky Security Center добавляет в категорию программ все исполняемые файлы, имеющие указанный хеш.

       Использование этого условия исключает возможность автоматической установки обновлений, поскольку файлы различных версий будут иметь различный хеш.

     - Сертификат файла. Если используется это условие, Kaspersky Security Center добавляет в категорию программ все исполняемые файлы, подписанные указанным сертификатом.
     - KL-категория. Если используется это условие, Kaspersky Security Center добавляет в категорию программ все программы, входящие в указанную KL-категорию.
     - Папка программы. Если используется это условие, Kaspersky Security Center добавляет в категорию программ все исполняемые файлы из этой папки.

     Использование условия Папка программы небезопасно, поскольку запуск любой программы из указанной папки будет разрешен. Правила, использующие категории программ с условием Папка программы, рекомендуется применять только к тем пользователям, для которых необходимо разрешить автоматическую установку обновлений.

   - **Автоматически пополняемая категория** (см. раздел "**Шаг 6. Папка хранилища**" на стр. 143). Вы можете указать папку, исполняемые файлы из которой будут автоматически попадать в создаваемую категорию программ.

     В категории программ этого типа хранится только одна версия файла – либо старая, либо обновленная, что исключает возможность автоматической установки обновлений, поскольку обновления устанавливаются на компьютерах неодновременно.

   - **Категория, в которую входят исполняемые файлы с выбранных устройств** (см. раздел

"**Шаг 5. Параметры**" на стр. 142). Вы можете указать компьютер, все исполняемые файлы которого будут автоматически попадать в создаваемую категорию программ.

> При использовании этого типа категорий программ Kaspersky Security Center получает информацию о программах на компьютере из списка исполняемых файлов (см. раздел "Получение информации о программах, которые установлены на компьютерах пользователей" на стр. 138).

Вы можете добавить в категорию программ исполняемые файлы из папки **Исполняемые файлы** (см. раздел "**Добавление в категорию программ исполняемых файлов из папки Исполняемые файлы**" на стр. 144) или исполняемые файлы, связанные с событиями о работе компонента Контроль программ (см. раздел "Добавление в категорию программ исполняемых файлов, связанных с событиями" на стр. 145).

2. Выбрать режим белого списка (см. раздел "Выбор режима Контроля программ" на стр. 136) для компонента Контроль программ.
3. Создать правила Контроля программ (см. раздел "Добавление и изменение правила Контроля программ с помощью Kaspersky Security Center" на стр. 146) с использованием созданных категорий программ.

> Для режима белого списка изначально задано правило Операционная система и ее компоненты, которое разрешает запуск программ, входящих в KL-категорию Золотая категория, и правило Доверенные программы обновления, которое разрешает запуск программ, входящих в KL-категорию Доверенные программы обновления. В KL-категорию Золотая категория 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 Операционная система и ее компоненты включено, а правило Доверенные программы обновления выключено. Запуск программ, соответствующих условиям срабатывания этих правил, разрешен всем пользователям.

4. Определить те программы, для которых необходимо разрешить автоматическую установку обновлений.

   Вы можете разрешить автоматическую установку обновлений одним из следующих способов:

   - Указать расширенный список разрешенных программ, разрешив запуск все программ, входящих в KL-категорию, или разрешив запуск всех программ, подписанных сертификатами.

     Чтобы разрешить запуск всех программ, подписанных сертификатами, вы можете создать категорию с условием на основе сертификата, в котором используется только параметр **Субъект** со значением *.

   - Для правила Контроля программ установить параметр **Доверенные программы обновления**. Если этот флажок установлен, то Kaspersky Endpoint Security будет считать программы, принадлежащие к указанной в правиле категории программ, доверенными программами обновления. Kaspersky Endpoint Security разрешает запуск программ, которые были установлены или обновлены программами, указанными в правиле категории, если для них не определены запрещающие правила.
   - Создать категорию программ на основе условия Папка программы. При использовании этого способа все исполняемые файлы, находящиеся в указанной папке, будут добавлены в

категорию программ.

Использование условия Папка программы небезопасно, поскольку запуск любой программы из указанной папки будет разрешен. Правила, использующие категории программ с условием Папка программы, рекомендуется применять только к тем пользователям, для которых необходимо разрешить автоматическую установку обновлений.

Тестирование режима белого списка

Чтобы убедиться, что правила Контроля программ не блокируют программы, необходимые для работы, рекомендуется после создания правил включить для них тестовый режим и проанализировать их работу. При включении тестового режима Kaspersky Endpoint Security не будет блокировать программы, запуск которых запрещен правилами Контроля программ, но будет отправлять уведомления об их запуске на Сервер администрирования.

При тестировании режима белого списка рекомендуется выполнить следующие действия:

1. Определить период тестирования (от нескольких дней до двух месяцев).
2. Включить тестовый режим для правил Контроля программ (см. раздел "Тестирование правил Контроля программ с помощью Kaspersky Security Center" на стр. 147).
3. Проанализировать результаты тестирования, используя события и отчеты о работе компонента Контроль программ в тестовом режиме (см. раздел "Просмотр событий о работе компонента Контроля программ в тестовом режиме" на стр. 148, "Просмотр отчета о тестовых запрещенных запусках" на стр. 149).
4. По результатам анализа внести изменения в настройки режима белого списка.

Поддержка режима белого списка

После включения блокирующего режима для правил Контроля программ рекомендуется продолжать поддержку режима белого списка, выполняя следующие действия:

- Анализировать работу правил Контроля программ, используя события и отчеты о работе компонента Контроль программ (см. раздел "Просмотр отчета о запрещенных запусках" на стр. 150, "Просмотр событий о работе компонента Контроль программ" на стр. 149), а также запросы доступа к программам, получаемые от пользователей (см. раздел "Просмотр сообщений пользователей в хранилище событий Kaspersky Security Center" на стр. 259).
- Анализировать незнакомые файлы, проверяя их репутацию в Kaspersky Security Network (см. раздел "Проверка репутации файла в Kaspersky Security Network" на стр. 64) или на портале Kaspersky Whitelist http://whitelist.kaspersky.com/.
- Добавлять необходимые программы в категории программ.

Веб-Контроль

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

Этот раздел содержит информацию о Веб-Контроле и инструкции о том, как настроить параметры компонента.

В этом разделе

О Веб-Контроле

Компонент Веб-Контроль позволяет контролировать действия пользователей локальной сети организации: ограничивать или запрещать доступ к веб-ресурсам.

Под веб-ресурсом подразумевается как отдельная веб-страница или несколько веб-страниц, так и веб-сайт или несколько веб-сайтов, сгруппированных по общему признаку.

Веб-Контроль предоставляет следующие возможности:

- Экономия трафика.

  Расход трафика контролируется путем ограничения или запрета загрузок мультимедийных файлов и ограничения или запрета доступа на не связанные с работой веб-ресурсы.

- Разграничение доступа по категориям содержания веб-ресурсов.

  Для уменьшения расхода трафика и потенциальных потерь из-за нецелевого использования рабочего времени вы можете ограничить или запретить доступ к веб-ресурсам определенных

категорий (например, запретить доступ к веб-ресурсам категории "Общение в сети").

- Централизованное управление доступом к веб-ресурсам.

  При использовании Kaspersky Security Center доступны персональные и групповые настройки доступа к веб-ресурсам.

Все ограничения и запреты на доступ к веб-ресурсам реализуются в виде правил доступа к веб-ресурсам (см. раздел "О правилах доступа к веб-ресурсам" на стр. 161).

Включение и выключение Веб-Контроля

По умолчанию Веб-Контроль включен. Вы можете выключить Веб-Контроль при необходимости.

► *Чтобы включить или выключить Веб-Контроль, выполните следующие действия:*

1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 46).
2. В левой части окна в разделе **Контроль безопасности** выберите подраздел **Веб-Контроль**.

   В правой части окна отобразятся параметры компонента Веб-Контроль.
3. Выполните одно из следующих действий:
   - Установите флажок **Включить Веб-Контроль**, если вы хотите включить Веб-Контроль.
   - Снимите флажок **Включить Веб-Контроль**, если вы хотите выключить Веб-Контроль.

   Если Веб-Контроль выключен, Kaspersky Endpoint Security не контролирует доступ к веб-ресурсам.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Категории содержания веб-ресурсов

Категории содержания веб-ресурсов (далее также "категории") в приведенном ниже списке подобраны таким образом, чтобы максимально полно описать блоки информации, размещенные на веб-ресурсах, с учетом их функциональных и тематических особенностей. Порядок категорий в списке не отражает относительной важности или распространенности категорий в сети Интернет. Названия категорий являются условными и используются лишь для целей программ и веб-сайтов "Лаборатории Касперского". Названия не обязательно соответствуют значению, которое им придает применимое законодательство. Один веб-ресурс может относиться к нескольким категориям одновременно.

Для взрослых

Категория включает следующие типы веб-ресурсов:

- Содержащие любые фото- или видеоматериалы с изображением половых органов людей или человекоподобных существ, полового акта или самоудовлетворения, совершенного людьми или человекоподобными существами.
- Содержащие любые текстовые, в том числе литературные и художественные материалы с описанием половых органов людей или человекоподобных существ, полового акта или самоудовлетворения, совершенного людьми или человекоподобными существами.
- Посвященные обсуждению сексуальной стороны человеческих взаимоотношений.

- Содержащие эротические материалы, произведения, натуралистично освещающие половую жизнь человека, или произведения искусства, рассчитанные на стимулирование сексуального возбуждения.
- Веб-ресурсы официальных СМИ, интернет-сообществ, имеющих устоявшуюся целевую аудиторию, содержащие специальный раздел и / или отдельные статьи, посвященные сексуальной стороне человеческих взаимоотношений.
- Посвященные половым извращениям.
- Посвященные рекламе и реализации предметов, предназначенных для секса и стимулирования сексуального возбуждения, сексуальных услуг и услуг интимных знакомств, в том числе оказываемых в сети Интернет посредством эротических видеочатов, "секса по телефону", "секса по переписке" ("виртуального секса").
- Веб-ресурсы, содержимое которых:
  - Статьи и блоги на тему полового воспитания, как научные, так и популярные.
  - Медицинские энциклопедии, их разделы о половом размножении.
  - Ресурсы медицинских учреждений, их разделы про лечение половых органов.

Программное обеспечение, аудио, видео

Категория включает следующие подкатегории, которые вы можете выбрать отдельно:

- **Аудио и видео**.

  Подкатегория включает веб-ресурсы, распространяющие аудио- и видеоматериалы: фильмы, записи спортивных трансляций, записи концертов, песни, клипы, видеоролики, учебные аудио- и видеозаписи и прочее.

- **Торренты**.

  Подкатегория включает веб-сайты торрент-трекеров, предназначенных для обмена файлами неограниченного размера.

- **Файловые обменники**.

  Подкатегория включает веб-сайты файлообмена вне зависимости от физического нахождения распространяемых файлов.

Алкоголь, табак, наркотические и психотропные вещества

Категория включает веб-ресурсы, содержание которых прямым или косвенным образом связано с алкогольной и спиртосодержащей продукцией, табачными изделиями и наркотическими, психотропными и / или одурманивающими веществами:

- Посвященные рекламе и реализации указанных средств, а также предметов, предназначенных для их употребления.
- Содержащие инструкции по употреблению или изготовлению наркотических, психотропных и/или одурманивающих веществ.

> К этой категории относятся веб-ресурсы с научной и медицинской тематикой.

Насилие

Категория включает веб-ресурсы, содержащие любые фото-, видео- и текстовые материалы, описывающие

акты физического или психического насилия над людьми, а также жестокого отношения к животным:

- Содержащие изображение / описание сцен казней, пыток и истязаний, а также предназначенных для них инструментов.

  Пересекается с категорией "Оружие, взрывчатые вещества, пиротехника".

- Содержащие изображение / описание сцен убийств, драк, избиений и изнасилований, сцен издевательств и глумления над людьми, животными или вымышленными существами.
- Содержащие информацию, побуждающую к совершению действий, представляющих угрозу жизни и / или здоровью, в том числе к причинению вреда своему здоровью, самоубийству.
- Содержащие информацию, обосновывающую или оправдывающую допустимость насилия и / или жестокости либо побуждающую осуществлять насильственные действия по отношению к людям или животным.
- Содержащие особо натуралистичное изображение / описание жертв и ужасов войны, вооруженных конфликтов и боевых столкновений, аварий, катастроф, стихийных бедствий, технологических и общественных катаклизмов, страданий людей.
- Браузерные компьютерные игры, в которых присутствуют сцены насилия и жестокости, в том числе называемые "шутеры / стрелялки", "файтинги", "слэшеры" и так далее.

  Пересекается с категорией "Компьютерные игры".

Оружие, взрывчатые вещества, пиротехника

Категория включает веб-ресурсы, содержащие информацию об оружии, взрывчатых веществах и пиротехнической продукции:

- Веб-сайты производителей и магазинов оружия, взрывчатых веществ и пиротехнической продукции.
- Веб-ресурсы, посвященные изготовлению и использованию оружия, взрывчатых веществ и пиротехнической продукции.
- Веб-ресурсы, содержащие аналитические, исторические, производственные и энциклопедические материалы на тему оружия, взрывчатых веществ и пиротехнической продукции.

Под "оружием" понимаются устройства, предметы и средства, конструктивно предназначенные для нанесения вреда жизни и здоровью людей и животных и / или выведения из строя техники и сооружений.

Нецензурная лексика

Категория включает веб-ресурсы, на которых обнаружены элементы нецензурной брани.

Пересекается с категорией "Для взрослых".

К этой категории относятся также веб-ресурсы с лингвистическими и филологическими материалами, содержащими нецензурную лексику в качестве предмета рассмотрения.

Общение в сети

Категория включает веб-ресурсы, позволяющие тем или иным пользователям, зарегистрированным или нет, отправлять персональные сообщения другим пользователям соответствующих веб-ресурсов или других интернет-сервисов и / или на определенных условиях участвовать в пополнении содержимого, общедоступного или частично доступного, соответствующих веб-ресурсов. Вы можете отдельно выбрать следующие подкатегории:

- **Чаты и форумы**.

  Подкатегория включает веб-ресурсы, предназначенные для публичного обсуждения различных тем с помощью специальных веб-приложений, а также веб-ресурсы, предназначенные для распространения и поддержки приложений для мгновенного обмена сообщениями, предоставляющих возможность коммуникации в реальном времени.

- **Блоги**.

  Подкатегория включает блог-платформы - веб-сайты, предоставляющие платные или бесплатные услуги по созданию и обслуживанию блогов.

- **Социальные сети**.

  Подкатегория включает веб-сайты, предназначенные для построения, отражения и организации контактов между людьми, организациями, государством, требующие в качестве условия участия регистрацию учетной записи пользователя.

- **Сайты знакомств**.

  Подкатегория включает веб-ресурсы, являющиеся разновидностью социальных сетей, которые предоставляют платные или бесплатные услуги.

  Пересекается с категориями "Для взрослых".

- **Веб-почта**.

  Подкатегория включает исключительно страницы авторизации в почтовом сервисе и страницы почтового ящика, содержащего сообщения электронной почты и сопутствующие данные (например, личные контакты). Остальные веб-страницы интернет-провайдера, предлагающего почтовый сервис, к этой категории не относятся.

Азартные игры, лотереи, тотализаторы

Категория включает веб-ресурсы, предлагающие пользователям финансовое участие в игровой деятельности, даже если это не является обязательным условием использования веб-ресурса. Категория охватывает веб-ресурсы, содержащие:

- Азартные игры, предусматривающие денежные взносы за участие.

  Пересекается с категорией "Компьютерные игры".

- Тотализаторы, предусматривающие денежные ставки.

- Лотереи, предусматривающие приобретение лотерейных билетов / номеров.
- Информацию, способную вызвать желание участвовать в азартных играх, тотализаторах и лотереях.

К этой категории относятся игры, предлагающие бесплатное участие в качестве отдельного режима, а также веб-ресурсы, которые активно рекламируют пользователям посещение веб-ресурсов типов, перечисленных в этой категории.

Интернет-магазины, банки, платежные системы

Категория включает веб-ресурсы, предназначенные для проведения любых операций с безналичными денежными средствами в режиме онлайн с помощью специальных веб-приложений. Вы можете отдельно выбрать следующие подкатегории:

- **Интернет-магазины**.

  Подкатегория включает интернет-магазины и интернет-аукционы, предназначенные для реализации любых товаров, работ или услуг физическим и/или юридическим лицам, в том числе как веб-сайты магазинов, осуществляющих реализацию исключительно в интернете, так и интернет-представительства обычных магазинов, характерной особенностью которых является возможность оплаты в режиме онлайн.

- **Банки**.

  Подкатегория включает специальные веб-страницы банков, предусматривающие услуги интернет-банкинга, включающие безналичные (электронные) переводы между банковскими счетами, открытие банковских вкладов, конвертацию денежных средств, оплату услуг сторонних организаций и так далее.

- **Платежные системы**.

  Подкатегория включает веб-страницы электронных платежных систем, предоставляющие доступ к персональной учетной записи пользователя.

В техническом аспекте средством проведения платежей могут служить как банковские карты любых типов (пластиковые и виртуальные, дебетовые и кредитные, локальные и международные), так и электронные деньги. Для определения категории веб-ресурса несущественно наличие таких технических аспектов, как передача данных по протоколу SSL, использование средства проверки подлинности "3D Secure" и так далее.

Поиск работы

Категория включает веб-ресурсы, предназначенные для установления контактов между работодателем и соискателем работы:

- Веб-сайты кадровых агентств (агентств по трудоустройству и / или агентств по подбору персонала).
- Веб-страницы работодателей, содержащие описание имеющихся вакансий и их преимуществ.
- Независимые порталы, содержащие предложения трудоустройства от работодателей и кадровых агентств.
- Социальные сети профессионального характера, которые в том числе позволяют

размещать / находить данные о специалистах, которые не находятся в активном поиске работы.

Средства анонимного доступа

Категория включает веб-ресурсы, выступающие в роли посредника для загрузки содержимого других веб-ресурсов с помощью специальных веб-приложений со следующими целями:

- Обход ограничений администратора локальной сети на доступ к веб-адресам или IP-адресам.
- Анонимный доступ к веб-ресурсам, в том числе к веб-ресурсам, которые преднамеренно не принимают HTTP-запросы с определенных IP-адресов или их групп (например, по стране происхождения).

К этой категории относятся как веб-ресурсы, исключительно предназначенные для вышеуказанных целей ("анонимайзеры"), так и веб-ресурсы, имеющие технически схожую функциональность.

Компьютерные игры

Категория включает веб-ресурсы, посвященные компьютерным играм разнообразных жанров:

- Веб-сайты разработчиков компьютерных игр.
- Веб-ресурсы, посвященные обсуждению компьютерных игр.
- Веб-ресурсы, предоставляющие техническую возможность игрового участия в режиме онлайн, во взаимодействии с другими участниками или без него, с условием локальной установки приложений или без него ("браузерные").
- Веб-ресурсы, предназначенные для рекламы, распространения и поддержки игрового программного обеспечения.

Религии, религиозные объединения

Категория включает веб-ресурсы, содержащие материалы об общественных течениях (движениях), объединениях (сообществах) и организациях, подразумевающих наличие религиозной идеологии и / или культа в любых проявлениях:

- Веб-сайты официальных религиозных организаций разного уровня, начиная с межнациональных конфессий и заканчивая местными религиозными общинами.
- Веб-сайты незарегистрированных религиозных объединений и сообществ, исторически появившихся в результате отделения от господствующего религиозного объединения или сообщества.
- Веб-сайты религиозных объединений и сообществ, появившихся независимо от традиционных религиозных течений / движений, в том числе по инициативе конкретного основателя.
- Веб-сайты межконфессиональных организаций, служащих для взаимодействия представителей разных традиционных религий.
- Веб-ресурсы, содержащие научные, исторические и энциклопедические материалы на тему религий.
- Веб-ресурсы, содержащие подробное изображение / описание отправления религиозных культов, в том числе обрядов и ритуалов, связанных с почитанием Бога, существ и / или предметов, наделяемых сверхъестественными свойствами.

Новостные ресурсы

Категория включает веб-ресурсы, содержащие публично-новостной контент, формируемый СМИ или интернет-издательствами, предусматривающими добавление новостей пользователями:

- Веб-сайты официальных средств массовой информации.
- Веб-сайты, предоставляющие сервисы информирования со ссылкой на официальные источники информации.
- Веб-сайты, предоставляющие сервисы агрегирования, то есть сбора новостной информации из различных официальных или неофициальных источников.
- Веб-сайты, новостной контент которых формируется самими пользователями ("сайты социальных новостей").

Баннеры

Категория включает веб-ресурсы, содержащие баннеры. Рекламная информация на баннерах может отвлекать пользователей от дел, а загрузка баннеров увеличивает объем трафика.

Региональные ограничения законодательства

Категория включает подкатегорию **Заблокировано по требованию законодательства РФ**, которая включает веб-ресурсы, заблокированные в соответствии с требованиями законодательства Российской Федерации.

О правилах 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 (см. раздел "Категории содержания веб-ресурсов" на стр. 155) 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. 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", которое разрешает всем пользователям в любое время доступ к любым веб-ресурсам.

Действия с правилами доступа к веб-ресурсам

Вы можете выполнить следующие действия с правилами доступа к веб-ресурсам:

- Добавить новое правило.
- Изменить правило.
- Назначить правилу приоритет.

  Приоритет правила определяется положением строки с кратким описанием правила в таблице правил доступа в окне настроек компонента Веб-Контроль. То есть правило, расположенное выше других правил в таблице правил доступа, имеет более высокий приоритет.

  Если веб-ресурс, к которому пользователь пытается получить доступ, соответствует параметрам нескольких правил, то действие Kaspersky Endpoint Security определяет правило с более высоким приоритетом.
- Проверить работу правила.

  Вы можете проверить согласованность работы правил с помощью функции "Диагностика правил".
- Включить и выключить правило.

  Правило доступа к веб-ресурсам может быть включено (статус работы *Вкл*) или выключено (статус работы *Выкл*). По умолчанию после создания правило включено (имеет статус работы *Вкл)*. Вы можете выключить правило.
- Удалить правило.

В этом разделе

Добавление и изменение правила доступа к веб-ресурсам

► *Чтобы добавить или изменить правило доступа к веб-ресурсам, выполните следующие действия:*

1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 46).
2. В левой части окна в разделе **Контроль безопасности** выберите подраздел **Веб-Контроль**.

   В правой части окна отобразятся параметры компонента Веб-Контроль.
3. Выполните одно из следующих действий:
   - Если вы хотите добавить правило, нажмите на кнопку **Добавить**.
   - Если вы хотите изменить правило, выберите правило в таблице и нажмите на кнопку **Изменить**.

   Откроется окно **Правило доступа к веб-ресурсам**.
4. Задайте или измените параметры правила. Для этого выполните следующие действия:
   a. В поле **Название** введите или измените название правила.
   b. В раскрывающемся списке **Фильтровать содержание** выберите нужный элемент:
      - **Любое содержание**.
      - **По категориям содержания**.
      - **По типам данных**.
      - **По категориям содержания и типам данных**.
   c. Если выбран элемент, отличный от **Любое содержание**, откроются блоки для выбора категорий содержания и / или типов данных. 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.
   d. В раскрывающемся списке **Применять к адресам** выберите нужный элемент:
      - **Ко всем адресам**.
      - **К отдельным адресам**.
   e. Если выбран элемент **К отдельным адресам**, откроется блок, в котором требуется создать список адресов веб-ресурсов. Вы можете добавлять или изменять адреса и / или группы

адресов веб-ресурсов, используя кнопки **Добавить**, **Изменить**, **Удалить**.

f. Установите флажок **Укажите пользователей и / или группы**.

g. Нажмите на кнопку **Выбрать**.

Откроется окно Microsoft Windows **Выбор пользователей или групп**.

h. Задайте или измените список пользователей и / или групп пользователей, для которых разрешен или ограничен доступ к веб-ресурсам, описанным в правиле.

i. Из раскрывающегося списка **Действие** выберите нужный элемент:

- **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.

j. 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:

1. Нажмите на кнопку **Настройка** напротив раскрывающегося списка **Расписание работы правила**.

   Откроется окно **Расписание работы правила**.

2. Чтобы добавить в расписание работы правила интервал времени, в течение которого правило не работает, в таблице с изображением расписания работы правила левой клавишей мыши выберите ячейки таблицы, соответствующие нужному вам времени и дню недели.

   Цвет ячеек изменится на серый.

3. Чтобы в расписании работы правила изменить интервал времени, в течение которого правило работает, на интервал времени, в течение которого правило не работает, левой клавишей мыши выберите серые ячейки таблицы, соответствующие нужному вам времени и дню недели.

   Цвет ячеек изменится на зеленый.

4. Нажмите на кнопку **Сохранить как**.

   Откроется окно **Название расписания работы правила**.

5. Введите название расписания работы правила или оставьте название, предложенное по умолчанию.

6. Нажмите на кнопку **ОК**.

5. В окне **Правило доступа к веб-ресурсам** нажмите на кнопку **ОК**.

6. Нажмите на кнопку **Сохранить**, чтобы сохранить 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. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 46).
2. В левой части окна в разделе **Контроль безопасности** выберите подраздел **Веб-Контроль**.

   В правой части окна отобразятся параметры компонента Веб-Контроль.
3. В правой части окна выберите правило, приоритет которого вы хотите изменить.
4. С помощью кнопок **Вверх** и **Вниз** переместите правило на желаемую позицию в списке правил.
5. Повторите действие пунктов инструкции 3-4 для тех правил, приоритет которых вы хотите изменить.
6. Нажмите на кнопку **Сохранить**, чтобы сохранить 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. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 46).
2. В левой части окна в разделе **Контроль безопасности** выберите подраздел **Веб-Контроль**.

   В правой части окна отобразятся параметры компонента Веб-Контроль.
3. В правой части окна нажмите на кнопку **Диагностика**.

   Откроется окно **Диагностика правил**.
4. Заполните поля в блоке **Условия**:
   a. 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.
   b. 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.
   c. Из раскрывающегося списка **Фильтровать содержание** 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.
   d. 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.
5. 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.

Включение и выключение правила доступа к веб-ресурсам

► *Чтобы включить или выключить правило доступа к веб-ресурсам, выполните следующие действия:*

1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 46).
2. В левой части окна в разделе **Контроль безопасности** выберите подраздел **Веб-Контроль**.

   В правой части окна отобразятся параметры компонента Веб-Контроль.
3. В правой части окна выберите правило, которое вы хотите включить или выключить.
4. В графе **Статус** выполните следующие действия:
   - Если вы хотите включить использование правила, выберите значение *Вкл*.
   - Если вы хотите выключить использование правила, выберите значение *Выкл*.
5. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Миграция правил доступа к веб-ресурсам из предыдущих версий программы

При обновлении программы с версии Kaspersky Endpoint Security 10 Service Pack 2 для Windows и с более ранних версий до Kaspersky Endpoint Security 11 для Windows правила доступа к веб-ресурсам, основанные на категориях содержания веб-ресурсов, мигрируют по следующим правилам:

- Правила доступа к веб-ресурсам, основанные на одной или нескольких категориях содержания веб-ресурсов из списка "Чаты и форумы", "Веб-почта", "Социальные сети", становятся основанными на категории содержания веб-ресурсов "Общение в сети".
- Правила доступа к веб-ресурсам, основанные на одной или нескольких категориях содержания веб-ресурсов из списка "Интернет-магазины" и "Платежные системы", становятся основанными на категории содержания веб-ресурсов "Интернет-магазины, банки, платежные системы".
- Правила доступа к веб-ресурсам, основанные на категории содержания веб-ресурсов "Азартные игры", становятся основанными на категории содержания веб-ресурсов "Азартные игры, лотереи, тотализаторы".
- Правила доступа к веб-ресурсам, основанные на категории содержания веб-ресурсов "Браузерные игры", становятся основанными на категории содержания веб-ресурсов "Компьютерные игры".
- Правила доступа к веб-ресурсам, основанные на категориях содержания веб-ресурсов, не перечисленных в предыдущих пунктах списка, мигрируют без изменений.

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 экспортировать список адресов веб-ресурсов в файл, выполните следующие действия:*

1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 46).
2. В левой части окна в разделе **Контроль безопасности** выберите подраздел **Веб-Контроль**.

   В правой части окна отобразятся параметры компонента Веб-Контроль.
3. Выберите правило, список адресов веб-ресурсов которого вы хотите экспортировать в файл.
4. Нажмите на кнопку **Изменить**.

   Откроется окно **Правило доступа к веб-ресурсам**.
5. Если вы хотите экспортировать не весь список адресов веб-ресурсов, а только его часть, выделите нужные вам адреса веб-ресурсов.
6. Нажмите на кнопку  справа от поля со списком адресов веб-ресурсов.

   Откроется окно подтверждения действия.
7. Выполните одно из следующих действий:
   - Если вы хотите экспортировать только выделенные элементы списка адресов веб-ресурсов, в окне подтверждения действия нажмите на кнопку **Да**.
   - Если вы хотите экспортировать все элементы списка адресов веб-ресурсов, в окне подтверждения действия нажмите на кнопку **Нет**.

     Откроется стандартное окно Microsoft Windows **Сохранить как**.
8. В окне Microsoft Windows **Сохранить как** выберите файл, в который вы хотите экспортировать список адресов веб-ресурсов, и нажмите на кнопку **Сохранить**.

► *Чтобы импортировать в правило список адресов веб-ресурсов из файла, выполните следующие действия:*

1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 46).
2. В левой части окна в разделе **Контроль безопасности** выберите подраздел **Веб-Контроль**.

   В правой части окна отобразятся параметры компонента Веб-Контроль.
3. Выполните одно из следующих действий:
   - Нажмите на кнопку **Добавить**, если вы хотите создать новое правило доступа к веб-ресурсам.
   - Выберите правило доступа к веб-ресурсам, которое вы хотите изменить. Далее нажмите на кнопку **Изменить**.

Откроется окно **Правило доступа к веб-ресурсам**.

4. Выполните одно из следующих действий:
   - Если вы создаете новое правило доступа к веб-ресурсам, в раскрывающемся списке **Применять к адресам** выберите элемент **К отдельным адресам**.
   - Если вы изменяете правило доступа к веб-ресурсам, перейдите к пункту 5 инструкции.
5. Нажмите на кнопку  справа от поля со списком адресов веб-ресурсов.

   Если вы создаете новое правило, откроется стандартное окно Microsoft Windows **Открыть файл**.

   Если вы изменяете правило, откроется окно подтверждения действия.
6. Выполните одно из следующих действий:
   - Если вы создаете новое правило доступа к веб-ресурсам, перейдите к пункту 7 инструкции.
   - Если вы изменяете правило доступа к веб-ресурсам, в окне подтверждения действия выполните одно из следующих действий:
     - Если вы хотите добавить к существующим импортируемые элементы списка адресов веб-ресурсов, нажмите на кнопку **Да**.
     - Если вы хотите удалить существующие элементы списка адресов веб-ресурсов и добавить импортируемые, нажмите на кнопку **Нет**.

   Откроется стандартное окно Microsoft Windows **Открыть файл**.
7. В окне Microsoft Windows **Открыть файл** выберите файл со списком адресов веб-ресурсов для импорта.
8. Нажмите на кнопку **Открыть**.
9. В окне **Правило доступа к веб-ресурсам** нажмите на кнопку **OK**.

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.

   Для включения символа `*` в состав маски адреса требуется вводить два символа `*`.
2. Последовательность символов `www.` в начале маски адреса трактуется как последовательность `*.`.

   Пример: маска адреса www.example.com трактуется как *.example.com.
3. Если маска адреса начинается не с символа `*`, то содержание маски адреса эквивалентно тому же содержанию с префиксом `*.`.

4. Последовательность символов `*.` в начале маски трактуется как `*.` или пустая строка.

   Пример: под действие маски адреса http://www.*.example.com попадает адрес http://www2.example.com.

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 2. 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 1.
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 2, 1.
7	www.example.com	https://www.example.com	Да	См. правила 2, 1.

№	Маска адреса	Проверяемый адрес веб-ресурса	Удовлетворяет ли проверяемый адрес маске адреса	Комментарий
8	http://www.*.example.com	http://123.example.com	Да	См. правила 2, 4, 1.
9	www.example.com	http://www.example.com/abc	Да	См. правила 2, 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.

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.

При обработке веб-трафика, получаемого по протоколу HTTPS, Kaspersky Endpoint Security блокирует веб-ресурсы, доступ к которым запрещен, но сообщения Веб-Контроля не выводятся.

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. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 46).
2. В левой части окна в разделе **Контроль безопасности** выберите подраздел **Веб-Контроль**.

   В правой части окна отобразятся параметры компонента Веб-Контроль.
3. В правой части окна нажмите на кнопку **Шаблоны**.

   Откроется окно **Шаблоны сообщений**.
4. Выполните одно из следующих действий:
   - Если вы хотите изменить шаблон сообщения для пользователя о том, что веб-ресурс не рекомендован для посещения, выберите закладку **Предупреждение**.
   - Если вы хотите изменить шаблон сообщения о блокировке доступа к веб-ресурсу, выберите закладку **Блокировка**.
   - Если вы хотите изменить шаблон сообщения администратору, выберите закладку **Сообщение администратору**.
5. Измените шаблон сообщения. При этом вы можете использовать раскрывающийся список **Переменная**, а также кнопки **По умолчанию** и **Ссылка** (кнопка не доступна на закладке **Сообщение администратору**).
6. Нажмите на кнопку **ОК**.
7. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Endpoint Sensor

Параметры компонента Endpoint Sensor доступны только в Консоли администрирования Kaspersky Security Center. Для использования компонента требуется установить плагин управления.

Этот раздел содержит информацию о Endpoint Sensor и инструкцию о том, как включить или выключить компонент.

В этом разделе

О Endpoint Sensor

Endpoint Sensor является компонентом Kaspersky Anti Targeted Attack Platform. Это решение предназначено для своевременного обнаружения таких угроз, как целевые атаки.

Компонент устанавливается на клиентских компьютерах. На этих компьютерах компонент постоянно наблюдает за процессами, открытыми сетевыми соединениями и изменяемыми файлами и передает эту информацию в Kaspersky Anti Targeted Attack Platform.

Функциональность компонента доступна для следующих операционных систем:

- Microsoft Windows 7 Professional / Enterprise / Ultimate x86 Edition SP1, Microsoft Windows 7 Professional / Enterprise / Ultimate x64 Edition SP1.
- Microsoft Windows 8.1 Enterprise x86 Edition, Microsoft Windows 8.1 Enterprise x64 Edition.
- Microsoft Windows 10 Pro / Enterprise x86 Edition, Microsoft Windows 10 Pro / Enterprise x64 Edition.
- Microsoft Windows Server 2012 Standard / Foundation / Essentials x64 Edition, Microsoft Windows Server 2012 R2 Standard / Foundation / Essentials x64 Edition.
- Microsoft Windows Server 2016.

Вы можете найти информацию о Kaspersky Anti Targeted Attack Platform, не указанную в этой справке, в справке для Kaspersky Anti Targeted Attack Platform.

На компьютерах с компонентом Endpoint Sensor необходимо разрешить входящее соединение с сервером Kaspersky Anti Targeted Attack Platform напрямую, без использования прокси-сервера.

Включение и выключение компонента Endpoint Sensor

► *Чтобы включить или выключить компонент Endpoint Sensor, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева Консоли администрирования откройте папку с названием нужной группы администрирования, для которой вы хотите изменить параметры политики.
3. В рабочей области выберите закладку **Политики**.
4. Выберите нужную политику.
5. Откройте окно **Свойства: <Название политики>** одним из следующих способов:
   - В контекстном меню политики выберите пункт **Свойства**.
   - Перейдите по ссылке **Настроить параметры политики**, которая находится в правой части рабочей области Консоли администрирования.
6. Выберите раздел **Endpoint Sensor**.
7. Выполните одно из следующих действий:
   - Если вы хотите включить Endpoint Sensor, установите флажок **Endpoint Sensor**.
   - Если вы хотите выключить Endpoint Sensor, снимите флажок **Endpoint Sensor**.
8. Если на предыдущем шаге вы установили флажок, выполните следующие действия:
   a. В поле **Адрес сервера** укажите адрес сервера Kaspersky Anti Targeted Attack Platform, состоящий из следующих частей:
      1. название протокола;
      2. IP-адрес или полное доменное имя (FQDN) сервера;
      3. путь к Сборщику событий Windows на сервере.
   b. В поле **Порт** укажите номера порта, используемого для соединения с сервером Kaspersky Anti Targeted Attack Platform.
9. Нажмите на кнопку **OK**.
10. Примените политику.

    Подробнее о применении политики Kaspersky Security Center вы можете прочитать в *Руководстве администратора для Kaspersky Security Center.*

Обновление баз программы

Этот раздел содержит информацию об обновлении баз программы (далее также "обновления") и инструкции о том, как настроить параметры обновления.

Об обновлении баз программы

Обновление баз 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 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.

В процессе обновления на ваш компьютер загружаются 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.

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

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. 203).

Об источниках обновлений

Источник обновлений - это ресурс, содержащий обновления баз программы Kaspersky Endpoint Security.

Источником обновлений может быть FTP-, HTTP-сервер (например, Kaspersky Security Center, серверы обновлений "Лаборатории Касперского"), сетевая или локальная папка.

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

Настройка параметров обновления

Вы можете выполнить следующие действия для настройки параметров обновления:

- Добавить новые источники обновлений.

  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 в качестве источника обновлений выбран ресурс, расположенный вне локальной сети организации, для обновления требуется соединение с интернетом.

- Выбрать регион сервера обновлений "Лаборатории Касперского".

  Если в качестве источника обновлений вы используете серверы "Лаборатории Касперского", вы можете выбрать местоположение сервера обновлений "Лаборатории Касперского" для загрузки пакета обновлений. Серверы обновлений "Лаборатории Касперского" расположены в нескольких странах мира. Использование географически ближайшего к вам сервера обновлений "Лаборатории Касперского" поможет сократить время получения пакета обновлений.

  По умолчанию в параметрах обновления используется информация о текущем регионе из реестра операционной системы.

- Настроить обновление Kaspersky Endpoint Security из папки общего доступа.

  Для экономии интернет-трафика вы можете настроить обновление Kaspersky Endpoint Security на компьютерах локальной сети организации из папки общего доступа. Для этого один из компьютеров локальной сети организации должен получать актуальный пакет обновлений с сервера Kaspersky Security Center или серверов обновлений "Лаборатории Касперского" и копировать полученный пакет обновлений в папку общего доступа. Тогда остальные компьютеры локальной сети организации смогут получать пакет обновлений из папки общего доступа.

- Выбрать режим запуска 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.

- Настроить запуск задачи обновления с правами другого пользователя.

В этом разделе

Добавление источника обновлений

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

1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 46).
2. В левой части окна в разделе **Задачи** выберите подраздел **Обновление**.

   В правой части окна отобразятся параметры обновления антивирусных баз программы.
3. В блоке **Режим запуска и источник обновлений** нажмите на кнопку **Источник обновлений**.

   Откроется закладка **Источник** окна **Обновление**.
4. На закладке **Источник** нажмите на кнопку **Добавить**.

   Откроется окно **Выбор источника обновлений**.
5. В окне **Выбор источника обновлений** выберите папку, которая содержит пакет обновлений, или введите полный путь к папке в поле **Источник**.
6. Нажмите на кнопку **ОК**.
7. В окне **Обновление** нажмите на кнопку **ОК**.
8. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Выбор региона сервера обновлений

► *Чтобы выбрать регион сервера обновлений, выполните следующие действия:*

1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 46).
2. В левой части окна в разделе **Задачи** выберите подраздел **Обновление**.

В правой части окна отобразятся параметры обновления баз программы.

3. В блоке **Режим запуска и источник обновлений** нажмите на кнопку **Источник обновлений**.

   Откроется закладка **Источник** окна **Обновление**.

4. На закладке **Источник** в блоке **Региональные параметры** выберите **Выбрать из списка**.
5. В раскрывающемся списке выберите ближайшую к вашему текущему местонахождению страну.
6. Нажмите на кнопку **ОК**.
7. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Настройка обновления из папки общего доступа

Настройка обновления Kaspersky Endpoint Security 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 Kaspersky Endpoint Security 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. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 46).
2. В левой части окна в разделе **Задачи** выберите подраздел **Обновление**.

   В правой части окна отобразятся параметры обновления баз программы.

3. В блоке **Дополнительно** установите флажок **Копировать обновления в папку**.
4. Укажите путь к папке общего доступа, в которую следует помещать полученный пакет обновлений. Вы можете это сделать одним из следующих способов:
   - Введите путь к папке общего доступа в поле под флажком **Копировать обновления в папку**.
   - Нажмите на кнопку **Обзор**. Далее в открывшемся окне **Выбор папки** выберите нужную папку и нажмите на кнопку **ОК**.
5. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

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

1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 46).
2. В левой части окна в разделе **Задачи** выберите подраздел **Обновление**.

   В правой части окна отобразятся параметры обновления баз программы.

3. В блоке **Режим запуска и источник обновлений** нажмите на кнопку **Источник обновлений**.

   Откроется закладка **Источник** окна **Обновление**.

4. На закладке **Источник** нажмите на кнопку **Добавить**.

Откроется окно **Выбор источника обновлений**.

5. В окне **Выбор источника обновлений** выберите папку общего доступа, в которой хранится пакет обновлений, или введите полный путь к папке общего доступа в поле **Источник**.
6. Нажмите на кнопку **OK**.
7. На закладке **Источник** снимите флажки рядом с названиями тех источников обновлений, которые не являются указанной вами папкой общего доступа.
8. Нажмите на кнопку **OK**.
9. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Выбор режима запуска для задачи обновления

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

1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 46).
2. В левой части окна в разделе **Задачи** выберите подраздел **Обновление**.

   В правой части окна отобразятся параметры обновления баз программы.
3. Нажмите на кнопку **Режим запуска**.

   Откроется закладка **Режим запуска** окна **Обновление**.
4. В блоке **Режим запуска** выберите один из следующих вариантов режима 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.
5. Выполните одно из следующих действий:
   - Если вы выбрали вариант **Автоматически** или **Вручную**, перейдите к пункту 6 инструкции.
   - Если вы выбрали вариант **По расписанию**, задайте параметры расписания запуска задачи обновления. Для этого выполните следующие действия:
     a. В раскрывающемся списке **Периодичность** укажите, когда следует запускать задачу обновления. Выберите один из следующих вариантов: **Минуты**, **Часы**, **Дни**, **Каждую неделю**, **В указанное время**, **Каждый месяц**, **После запуска программы**.
     b. В зависимости от выбранного в раскрывающемся списке **Периодичность** элемента задайте значения параметров, которые уточняют время запуска задачи обновления.
     c. В поле **Отложить запуск после старта программы на** укажите время, на которое следует отложить запуск задачи обновления после старта Kaspersky Endpoint Security.

Если в раскрывающемся списке **Периодичность** выбран элемент **После запуска программы**, поле **Отложить запуск после старта программы на** недоступно.

d. Установите флажок **Запускать пропущенные задачи**, если вы хотите, чтобы Kaspersky Endpoint Security запускал при первой возможности не запущенные вовремя задачи обновления.

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

6. Нажмите на кнопку **OK**.
7. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

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. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 46).
2. В левой части окна в разделе **Задачи** выберите подраздел **Обновление**.

   В правой части окна отобразятся параметры обновления баз программы.
3. В блоке **Режим запуска и источник обновлений** нажмите на кнопку **Режим запуска**.

   Откроется закладка **Режим запуска** окна **Обновление**.
4. На закладке **Режим запуска** в блоке **Пользователь** установите флажок **Запускать задачу с правами пользователя**.
5. В поле **Имя** введите имя учетной записи пользователя, права которого требуется использовать для доступа к источнику обновлений.
6. В поле **Пароль** введите пароль пользователя, права которого требуется использовать для доступа к источнику обновлений.
7. Нажмите на кнопку **OK**.
8. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

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.

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

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

1. Откройте главное окно программы (на стр. 43).
2. Нажмите на кнопку **Задачи**, расположенную в нижней части главного окна программы.

   Откроется окно **Задачи**.
3. По левой клавише мыши выберите блок с названием задачи обновления.

   Раскроется выбранный блок.
4. Выполните одно из следующих действий:
   - Выберите в меню пункт **Запустить**, если вы хотите запустить задачу обновления.

     Статус выполнения задачи, отображающийся под названием задачи обновления, изменится на *Выполняется*.
   - Выберите в меню пункт **Остановить**, если вы хотите остановить задачу обновления.

     Статус выполнения задачи, отображающийся под названием задачи обновления, изменится на *Остановлена*.

► *Чтобы запустить или остановить задачу обновления при отображении упрощенного интерфейса программы (см. раздел "Упрощенный интерфейс программы" на стр. 47), 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.

Откат последнего обновления

После первого обновления антивирусных баз программы становится доступна функция отката к предыдущим базам программы.

Каждый раз, когда пользователь запускает обновление, Kaspersky Endpoint Security создает резервную копию используемых антивирусных баз программы и только потом приступает к их обновлению. Это позволяет вернуться к использованию предыдущих баз 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. Откройте главное окно программы.
2. Нажмите на кнопку **Задачи**, расположенную в нижней части главного окна программы.

   Откроется окно **Задачи**.
3. По левой клавише мыши выберите блок с названием задачи отката обновления.

   Раскроется выбранный блок.
4. Нажмите на кнопку **Запустить**.

   Запустится задача отката обновления.

   Статус выполнения задачи, отображающийся под названием задачи отката обновления, изменится на *Выполняется*.

Настройка параметров прокси-сервера

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

1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 46).
2. В левой части окна в разделе **Задачи** выберите подраздел **Обновление**.

   В правой части окна отобразятся параметры обновления баз программы.
3. В блоке **Прокси-сервер** нажмите на кнопку **Настройка**.

   Откроется окно **Параметры прокси-сервера**.

   > Вы также можете открыть окно **Параметры прокси-сервера** из подраздела **Параметры программы** раздела **Общие параметры** в окне настройки параметров программы.
4. В окне **Параметры прокси-сервера** установите флажок **Использовать прокси-сервер**.
5. Выберите один из следующих вариантов определения адреса прокси-сервера:
   - **Автоматически определять адрес прокси-сервера**.

     Этот вариант выбран по умолчанию.
   - **Использовать указанные адрес и порт прокси-сервера**.
6. Если вы выбрали вариант **Использовать указанные адрес и порт прокси-сервера**, укажите значения в полях **Адрес** и **Порт**.
7. Если вы хотите включить использование аутентификации на прокси-сервере, установите флажок **Задать имя пользователя и пароль для аутентификации** и укажите значения в следующих полях:
   - **Имя пользователя**.

     Поле для ввода имени пользователя, которое используется при аутентификации на

прокси-сервере.

- **Пароль**.

  Поле для ввода пароля пользователя, который используется при аутентификации на прокси-сервере.

8. Если вы хотите выключить использование прокси-сервера при обновлении Kaspersky Endpoint Security из папки общего доступа, установите флажок **Не использовать прокси-сервер для локальных адресов**.
9. Нажмите на кнопку **OK**.

Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

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.

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.
- На форуме "Лаборатории Касперского" (https://forum.kaspersky.com).

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. 284).

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.

Этот раздел содержит информацию об особенностях и настройке задач проверки, уровнях безопасности, методах и технологиях проверки, а также инструкции по работе с файлами, которые Kaspersky Endpoint Security не обработал во время антивирусной проверки.

В этом разделе

О задачах проверки

Для поиска вирусов и других программ, представляющих угрозу, а также для проверки целостности модулей программы в состав Kaspersky Endpoint Security включены следующие задачи:

- **Полная проверка**. Тщательная проверка всей системы. По умолчанию Kaspersky Endpoint Security проверяет следующие объекты:
  - память ядра;
  - объекты, загрузка которых осуществляется при старте операционной системы;
  - загрузочные секторы;
  - резервное хранилище операционной системы;
  - все жесткие и съемные диски.
- **Проверка важных областей**. По умолчанию Kaspersky Endpoint Security проверяет память ядра, запущенные процессы и загрузочные секторы.
- **Выборочная проверка**. Kaspersky Endpoint Security проверяет объекты, выбранные пользователем. Вы можете проверить любой объект из следующего списка:
  - память ядра;
  - объекты, загрузка которых осуществляется при старте операционной системы;
  - резервное хранилище операционной системы;
  - почтовый ящик Outlook;
  - все жесткие, съемные и сетевые диски;
  - любой выбранный файл.

- **Проверка целостности**. Kaspersky Endpoint Security проверяет модули программы на наличие повреждений или изменений.

Задача полной проверки и задача проверки важных областей являются специфическими. Для этих задач не рекомендуется изменять область проверки.

После запуска задач проверки (см. раздел "Запуск и остановка задачи проверки" на стр. 187) процесс выполнения проверки отображается под названием запущенной задачи проверки в окне **Задачи**.

Информация о результатах проверки и обо всех событиях, произошедших во время выполнения задач проверки, записывается в отчет Kaspersky Endpoint Security.

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. Откройте главное окно программы (на стр. 43).
2. Нажмите на кнопку **Задачи**, расположенную в нижней части главного окна программы.

   Откроется окно **Задачи**.
3. По левой клавише мыши выберите блок с названием задачи проверки.

   Раскроется выбранный блок.
4. Выполните одно из следующих действий:
   - Нажмите на кнопку **Запустить**, если вы хотите запустить задачу проверки.

     Статус выполнения задачи, отображающийся под названием задачи проверки, изменится на *Выполняется*.
   - Выберите в контекстном меню пункт **Остановить**, если вы хотите остановить задачу проверки.

     Статус выполнения задачи, отображающийся под названием задачи проверки, изменится на *Остановлена*.

► *Чтобы запустить или остановить задачу проверки при отображении упрощенного интерфейса программы (см. раздел "Упрощенный интерфейс программы" на стр. 47), 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.

Настройка параметров задач проверки

Для настройки параметров задач проверки вы можете выполнить следующие действия:

- Изменить уровень безопасности.

  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.

- Изменить действие, которое выполняет Kaspersky Endpoint Security при обнаружении зараженного файла.

- Сформировать область проверки.

  Вы можете расширить или сузить область проверки, добавив или удалив объекты проверки или изменив тип проверяемых файлов.

- Оптимизировать проверку.

  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. Технологии iChecker и iSwift позволяют оптимизировать скорость проверки файлов за счет исключения из проверки файлов, не измененных с момента их последней проверки.

- Настроить проверку составных файлов.

- Настроить методы 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. В процессе эвристического анализа Kaspersky Endpoint Security анализирует активность, которую объекты производят в операционной системе. Эвристический анализ позволяет обнаруживать вредоносные объекты, записей о которых еще нет в базах Kaspersky Endpoint Security.

- Выбрать режим запуска задач 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.

- Настроить запуск задач проверки с правами другого пользователя.

- Задать параметры проверки съемных дисков при подключении.

В этом разделе

Изменение уровня безопасности

Для выполнения задач проверки Kaspersky Endpoint Security применяет разные наборы параметров. Наборы параметров, сохраненные в программе, называют *уровнями безопасности*. Предустановлены три уровня безопасности: **Высокий**, **Рекомендуемый**, **Низкий**. Параметры уровня безопасности **Рекомендуемый** считаются оптимальными. Они рекомендованы специалистами "Лаборатории Касперского".

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

1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 46).
2. В левой части окна в разделе **Задачи** выберите подраздел с названием нужной задачи проверки: **Полная проверка**, **Проверка важных областей**, **Выборочная проверка**.

   В правой части окна отобразятся параметры выбранной задачи проверки.
3. В блоке **Уровень безопасности** выполните одно из следующих действий:
   - Если вы хотите применить один из предустановленных уровней безопасности (**Высокий**, **Рекомендуемый**, **Низкий**), выберите его при помощи ползунка.
   - Если вы хотите настроить уровень безопасности самостоятельно, нажмите на кнопку **Настройка** и задайте параметры в открывшемся окне с названием задачи проверки.

     После того как вы самостоятельно настроили уровень безопасности, название уровня безопасности в блоке **Уровень безопасности** изменится на **Другой**.
   - Если вы хотите изменить уровень безопасности на **Рекомендуемый**, нажмите на кнопку **По умолчанию**.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

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. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 46).
2. В левой части окна в разделе **Задачи** выберите подраздел с названием нужной задачи проверки: **Полная проверка**, **Проверка важных областей**, **Выборочная проверка**, **Проверка из контекстного меню**.

   В правой части окна отобразятся параметры выбранной задачи проверки.
3. В блоке **Действие при обнаружении угрозы**, выберите один из следующих вариантов:
   - Установите флажок **Лечить, удалять, если лечение невозможно**, если вы хотите, чтобы при обнаружении зараженных файлов Kaspersky Endpoint Security пытался вылечить их или удалял их, если лечение невозможно.
   - Установите флажок **Лечить, информировать, если лечение невозможно**, если вы хотите, чтобы при обнаружении зараженных файлов Kaspersky Endpoint Security пытался вылечить их и информировал вас, если лечение невозможно.
   - Установите флажок **Информировать**, если вы хотите, чтобы при обнаружении зараженных файлов Kaspersky Endpoint Security информировал вас об этом.

   При обнаружении зараженных файлов, являющихся частью приложения Windows Store, Kaspersky Endpoint Security выполняет действие **Удалить**.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Формирование списка проверяемых объектов

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

1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 46).
2. В левой части окна в разделе **Задачи** выберите подраздел с названием нужной задачи проверки: **Полная проверка**, **Проверка важных областей**, **Выборочная проверка**, **Проверка из контекстного меню**.

   В правой части окна отобразятся параметры выбранной задачи проверки.
3. Нажмите на кнопку **Область проверки**.

   Откроется окно **Область проверки**.
4. Если вы хотите добавить новый объект в область проверки, выполните следующие действия:

   a. Нажмите на кнопку **Добавить**.

   Откроется окно **Выбор области проверки**.

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

Все объекты, выбранные в окне **Выбор области проверки**, отобразятся в списке **Область проверки**.

c. Нажмите на кнопку **ОК**.

5. Если вы хотите изменить путь к объекту области проверки, выполните следующие действия:

a. Выберите объект из области проверки.

b. Нажмите на кнопку **Изменить**.

Откроется окно **Выбор области проверки**.

c. Введите новый путь к объекту области проверки.

d. Нажмите на кнопку **ОК**.

6. Если вы хотите удалить объект из области проверки, выполните следующие действия:

a. Выберите объект, который вы хотите удалить из области проверки.

Чтобы выбрать несколько объектов, выделяйте их, удерживая клавишу **CTRL**.

b. Нажмите на кнопку **Удалить**.

Откроется окно подтверждения удаления.

c. Нажмите на кнопку **Да** в окне подтверждения удаления.

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

7. Чтобы исключить объект из области проверки, в окне **Область проверки** снимите флажок рядом с ним.

Объект остается в списке объектов области проверки, но не проверяется во время выполнения задачи проверки.

8. Нажмите на кнопку **ОК**.

9. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Выбор типа проверяемых файлов

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

1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 46).

2. В левой части окна в разделе **Задачи** выберите подраздел с названием нужной задачи проверки: **Полная проверка**, **Проверка важных областей**, **Выборочная проверка**, **Проверка из контекстного меню**.

В правой части окна отобразятся параметры выбранной задачи проверки.

3. В блоке **Уровень безопасности** нажмите на кнопку **Настройка**.

Откроется окно с названием выбранной задачи проверки.

4. В окне с названием выбранной задачи проверки выберите закладку **Область действия**.

5. В блоке **Типы файлов** укажите тип файлов, которые вы хотите проверять во время выполнения

выбранной задачи проверки:

- Выберите **Все файлы**, если вы хотите проверять все файлы.
- Выберите **Файлы, проверяемые по формату**, если вы хотите проверять файлы тех форматов, которые наиболее подвержены заражению.
- Выберите **Файлы, проверяемые по расширению**, если вы хотите проверять файлы с расширениями, типичными для файлов, которые наиболее подвержены заражению.

Выбирая тип проверяемых файлов, нужно учитывать следующее:

- Вероятность внедрения вредоносного кода в файлы некоторых форматов (например, TXT) и его последующей активации низка. В то же время существуют форматы файлов, которые содержат (например, форматы EXE, DLL) или могут содержать исполняемый код (например, формат DOC). Риск внедрения в такие файлы вредоносного кода и его активации высок.
- 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 компонент Защита от файловых угроз анализирует заголовок файла. Если в результате выясняется, что файл имеет формат EXE, то программа проверяет его.

6. В окне с названием задачи проверки нажмите на кнопку **OK**.
7. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Оптимизация проверки файлов

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

1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 46).
2. В левой части окна в разделе **Задачи** выберите подраздел с названием нужной задачи проверки: **Полная проверка**, **Проверка важных областей**, **Выборочная проверка**, **Проверка из контекстного меню**.

   В правой части окна отобразятся параметры выбранной задачи проверки.
3. В блоке **Уровень безопасности** нажмите на кнопку **Настройка**.

   Откроется окно с названием выбранной задачи проверки.
4. В открывшемся окне выберите закладку **Область действия**.
5. В блоке **Оптимизация проверки** выполните следующие действия:
   - Установите флажок **Проверять только новые и измененные файлы**.
   - Установите флажок **Пропускать файлы, если их проверка длится более** и задайте длительность проверки одного файла (в секундах).
6. Нажмите на кнопку **OK**.
7. Нажмите на кнопку **Сохранить**, чтобы сохранить 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. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 46).
2. В левой части окна в разделе **Задачи** выберите подраздел с названием нужной задачи проверки: **Полная проверка**, **Проверка важных областей**, **Выборочная проверка**.

   В правой части окна отобразятся параметры выбранной задачи проверки.
3. В блоке **Уровень безопасности** нажмите на кнопку **Настройка**.

   Откроется окно с названием выбранной задачи проверки.
4. В открывшемся окне выберите закладку **Область действия**.
5. В блоке **Проверка составных файлов** укажите, какие составные файлы вы хотите проверять: архивы, установочные пакеты, файлы офисных форматов, файлы почтовых форматов, защищенные паролем архивы.
6. Если в блоке **Оптимизация проверки** снят флажок **Проверять только новые и измененные файлы**, нажмите на ссылку **все / новые**, расположенную рядом с названием типа составного файла, чтобы выбрать, следует ли проверять все файлы этого типа или только новые файлы этого типа.

   Ссылка меняет свое значение при нажатии.

   Если флажок **Проверять только новые и измененные файлы** установлен, то проверяются только новые файлы.
7. Нажмите на кнопку **Дополнительно**.

   Откроется окно **Составные файлы**.
8. 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**.
9. Нажмите на кнопку **ОК**.
10. В окне с названием задачи проверки нажмите на кнопку **ОК**.
11. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Использование методов проверки

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

1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 46).
2. В левой части окна в разделе **Задачи** выберите подраздел с названием нужной задачи проверки: **Полная проверка**, **Проверка важных областей**, **Выборочная проверка**, **Проверка из контекстного меню**.

   В правой части окна отобразятся параметры выбранной задачи проверки.
3. В блоке **Уровень безопасности** нажмите на кнопку **Настройка**.

   Откроется окно с названием выбранной задачи проверки.
4. В открывшемся окне выберите закладку **Дополнительно**.
5. 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**.
6. Нажмите на кнопку **OK**.
7. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Использование технологий проверки

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

1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 46).
2. В левой части окна в разделе **Задачи** выберите подраздел с названием нужной задачи проверки: **Полная проверка**, **Проверка важных областей**, **Выборочная проверка**, **Проверка из контекстного меню**.

   В правой части окна отобразятся параметры выбранной задачи проверки.
3. В блоке **Уровень безопасности** нажмите на кнопку **Настройка**.

   Откроется окно с названием выбранной задачи проверки.
4. В открывшемся окне выберите закладку **Дополнительно**.
5. В блоке **Технологии проверки** установите флажки около названий технологий, которые вы хотите использовать во время проверки.
6. Нажмите на кнопку **OK**.
7. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Выбор режима запуска для задачи проверки

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

1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров

программы" на стр. 46).

2. В левой части окна в разделе **Задачи** выберите подраздел с названием нужной задачи: **Полная проверка**, **Проверка важных областей**, **Выборочная проверка**.

   В правой части окна отобразятся параметры выбранной задачи проверки.

3. Нажмите на кнопку **Режим запуска**.

   Откроется окно свойств выбранной задачи на закладке **Режим запуска**.

4. В блоке **Режим запуска** выберите режим запуска задачи: **Вручную** или **По расписанию**.

5. Если вы выбрали вариант **По расписанию**, задайте параметры расписания. Для этого выполните следующие действия:

   a. В раскрывающемся списке **Периодичность** выберите периодичность запуска задачи (**Минуты**, **Часы**, **Дни**, **Каждую неделю**, **В указанное время**, **Каждый месяц**, **После запуска программы**, **После каждого обновления**).

   b. В зависимости от выбранной периодичности настройте дополнительные параметры, которые уточняют расписание запуска задачи.

   c. 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.

   d. Установите флажок **Выполнять только во время простоя компьютера**, если вы хотите, чтобы Kaspersky Endpoint Security приостанавливал задачу, когда ресурсы компьютера заняты.

   Этот вариант расписания позволяет экономить вычислительную мощность компьютера во время работы.

6. Нажмите на кнопку **OK**.

7. Нажмите на кнопку **Сохранить**, чтобы сохранить 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. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 46).

2. В левой части окна в разделе **Задачи** выберите подраздел с названием нужной задачи: **Полная проверка**, **Проверка важных областей**, **Выборочная проверка**.

В правой части окна отобразятся параметры выбранной задачи проверки.

3. Нажмите на кнопку **Режим запуска**.

   Откроется окно свойств выбранной задачи на закладке **Режим запуска**.

4. На закладке **Режим запуска** в блоке **Пользователь** установите флажок **Запускать задачу с правами пользователя**.
5. В поле **Имя** введите имя пользователя, права которого требуется использовать для запуска задачи проверки.
6. В поле **Пароль** введите пароль пользователя, права которого требуется использовать для запуска задачи проверки.
7. Нажмите на кнопку **ОК**.
8. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

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. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 46).
2. В левой части окна в разделе **Задачи** выберите подраздел **Проверка съемных дисков**.

   В правой части окна отобразятся параметры проверки съемных дисков.

3. В раскрывающемся списке **Действие при подключении съемного диска** выберите нужное действие:
   - **Не проверять**.
   - **Подробная проверка**.

     В этом режиме Kaspersky Endpoint Security проверяет все файлы, расположенные на съемном диске, в том числе вложенные файлы внутри составных объектов.

   - **Быстрая проверка**.

     В этом режиме Kaspersky Endpoint Security проверяет только потенциально заражаемые файлы, а также не распаковывает составные объекты.

4. Выполните одно из следующих действий:
   - 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.
   - Если вы хотите, чтобы Kaspersky Endpoint Security проверял все жесткие диски, снимите флажок **Максимальный размер съемного диска**.
5. Выполните одно из следующих действий:
   - Если вы хотите, чтобы Kaspersky Endpoint Security отображал ход проверки съемных дисков в

отдельном окне, установите флажок **Отображать ход проверки**.

- Если вы хотите, чтобы Kaspersky Endpoint Security запускал проверку съемных дисков в фоновом режиме, снимите флажок **Отображать ход проверки**.

6. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Работа с активными угрозами

Этот раздел содержит инструкции по работе с зараженными файлами, которые Kaspersky Endpoint Security не обработал в процессе проверки компьютера на вирусы и другие программы, представляющие угрозу.

В этом разделе

Об активных угрозах

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**.

Вы можете вручную запустить задачу выборочной проверки файлов из списка активных угроз после обновления антивирусных баз программы. После проверки статус файлов может измениться. Согласно статусу вы можете самостоятельно выполнить необходимые действия с файлами.

Например, вы можете выполнить следующие действия:

- удалить файлы со статусом *Зараженный* (см. раздел "*Удаление файлов из списка активных угроз*" на стр. 199);

- восстановить те зараженные файлы, в которых содержится важная информация, а также восстановить файлы со статусом *Вылечен* и *Не заражен.*

Работа со списком активных угроз

Список активных угроз представлен в виде таблицы событий, связанных с зараженными файлами, которые по каким-либо причинам не были обработаны.

Вы можете выполнять следующие действия с файлами из списка активных угроз:

- просматривать список активных угроз;
- проверять из списка активных угроз, используя текущую версию антивирусных баз Kaspersky Endpoint Security;
- восстанавливать файлы из списка активных угроз в исходные папки или в другую выбранную вами папку (в случае, если исходная папка размещения файла недоступна для записи);
- удалять файлы из списка активных угроз;
- открыть папку исходного размещения файла из списка активных угроз.

Кроме того, вы можете выполнять следующие действия, работая с табличными данными:

- фильтровать активные угрозы по значениям граф или по условиям сложного фильтра;
- использовать функцию поиска активных угроз;
- сортировать активные угрозы;
- изменять порядок и набор граф, отображаемых в списке активных угроз;
- группировать активные угрозы.

Если требуется, вы можете скопировать информацию о выбранных активных угрозах в буфер обмена.

В этом разделе

Запуск задачи выборочной проверки файлов из списка активных угроз

Вы можете вручную запустить задачу выборочной проверки зараженных файлов, которые по каким-либо причинам не были обработаны. Проверку можно запустить, например, если по какой-либо причине последняя проверка была прервана или если вы хотите повторно проверить файлы из списка активных угроз после очередного обновления антивирусных баз программы.

► *Чтобы запустить задачу выборочной проверки файлов из списка активных угроз, выполните следующие действия:*

1. Откройте главное окно программы (на стр. 43).
2. Нажмите на блок **<...> активных угроз**.

Откроется окно **Активные угрозы**.

3. В таблице в окне **Активные угрозы** выберите одно или несколько событий, относящихся к файлам, которые вы хотите проверить.

   Чтобы выбрать несколько событий, выделяйте их, удерживая клавишу **CTRL**.

4. Запустите задачу выборочной проверки файлов одним из следующих способов:

   - Нажмите на кнопку **Перепроверить**.
   - По правой клавише мыши откройте контекстное меню и выберите пункт **Перепроверить**.

Удаление файлов из списка активных угроз

► *Чтобы удалить файлы из списка активных угроз, выполните следующие действия:*

1. Откройте главное окно программы (на стр. 43).
2. Нажмите на блок **<...> активных угроз**.

   Откроется окно **Активные угрозы**.

3. В таблице в окне **Активные угрозы** выберите одно или несколько событий, относящихся к файлам, которые вы хотите удалить.

   Чтобы выбрать несколько событий, выделяйте их, удерживая клавишу **CTRL**.

4. Удалите файлы одним из следующих способов:

   - Нажмите на кнопку **Удалить**.
   - По правой клавише мыши откройте контекстное меню и выберите пункт **Удалить**.

Проверка целостности модулей программы

Этот раздел содержит информацию об особенностях и настройке задачи проверки целостности.

В этом разделе

О задаче проверки целостности

Kaspersky Endpoint Security проверяет модули программы, находящиеся в папке установки программы, на наличие повреждений или изменений. Если модуль программы имеет некорректную цифровую подпись, то такой модуль считается поврежденным.

После запуска задачи проверки целостности (см. раздел "Запуск и остановка задачи проверки целостности" на стр. 200) процесс ее выполнения отображается в строке под названием задачи в окне **Задачи**.

Информация о результатах выполнения задачи проверки целостности фиксируется в отчетах (см. раздел "Работа с отчетами" на стр. 203).

Запуск и остановка задачи проверки целостности

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

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

1. Откройте главное окно программы (на стр. 43).
2. Нажмите на кнопку **Задачи**, расположенную в нижней части главного окна программы.

   Откроется окно **Задачи**.
3. По левой клавише мыши выберите блок с названием задачи проверки целостности.

   Раскроется выбранный блок.
4. Выполните одно из следующих действий:
   - Нажмите на кнопку **Запустить**, если вы хотите запустить задачу проверки целостности.

     Статус выполнения задачи, отображающийся под названием задачи проверки целостности, изменится на *Выполняется*.
   - Выберите в контекстном меню пункт **Остановить**, если вы хотите остановить задачу проверки

целостности.

Статус выполнения задачи, отображающийся под названием задачи проверки целостности, изменится на *Остановлена*.

► *Чтобы запустить или остановить задачу проверки целостности при отображении упрощенного интерфейса программы (см. раздел "Упрощенный интерфейс программы" на стр. 47), 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 целостности, чтобы запустить ее;
   - выберите запущенную задачу проверки целостности, чтобы остановить ее;
   - выберите остановленную задачу проверки целостности, чтобы возобновить ее или запустить ее заново.

Выбор режима запуска для задачи проверки целостности

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

1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 46).
2. В левой части окна в разделе **Задачи** выберите подраздел **Проверка целостности**.

   В правой части окна отобразятся параметры задачи проверки целостности.
3. В блоке **Режим запуска** выберите один из следующих вариантов:
   - Выберите вариант **Вручную**, если вы хотите запускать задачу проверки целостности вручную.
   - Выберите вариант **По расписанию**, если вы хотите настроить расписание запуска задачи проверки целостности.
4. Если на предыдущем шаге вы выбрали вариант **По расписанию**, задайте параметры расписания запуска задачи. Для этого выполните следующие действия:
   a. В раскрывающемся списке **Периодичность** укажите, когда следует запускать задачу проверки целостности. Выберите один из следующих вариантов: **Минуты**, **Часы**, **Дни**, **Каждую неделю**, **В указанное время**, **Каждый месяц**, **После запуска программы**.
   b. В зависимости от выбранного в раскрывающемся списке **Периодичность** элемента задайте значение параметров, которые уточняют время запуска задачи.
   c. Установите флажок **Запускать пропущенные задачи**, если вы хотите, чтобы Kaspersky Endpoint Security запускал при первой возможности не запущенную по расписанию задачу проверки целостности.

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

d. Установите флажок **Выполнять только во время простоя компьютера**, если вы хотите, чтобы Kaspersky Endpoint Security приостанавливал задачу, когда ресурсы компьютера заняты.

   Этот вариант расписания позволяет экономить вычислительную мощность компьютера во время работы.

5. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Работа с отчетами

Этот раздел содержит инструкции о том, как настроить параметры отчетов и как работать с отчетами.

В этом разделе

Об отчетах

Информация о работе каждого компонента Kaspersky Endpoint Security, 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 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 Kaspersky Endpoint Security;
- имя пользователя Microsoft Windows;
- адреса веб-страниц, открываемых пользователем.

Данные в отчете представлены в виде таблицы, которая содержит список событий. 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, необходимо нажать на кнопку ⊞ рядом с названием графы. События, зарегистрированные в работе разных компонентов или 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.
- Отчет о работе компонента или о выполнении задачи Kaspersky Endpoint Security.
- Отчет **Шифрование**. Содержит информацию о событиях, возникающих при шифровании и расшифровке данных.

В отчетах применяются следующие уровни важности событий:

- **Информационные события**. Значок  . События справочного характера, как правило, не несущие важной информации.
- **Важные события**. Значок  . События, на которые нужно обратить внимание, поскольку они отражают важные ситуации в работе Kaspersky Endpoint Security.
- **Критические события**. Значок  . 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;
- 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. 207) по компонентам и задачам Kaspersky Endpoint Security, объединенным в группы. Kaspersky Endpoint Security удаляет все записи выбранных отчетов от наиболее ранней записи вплоть до текущего момента.

Если Kaspersky Endpoint Security работает под управлением Kaspersky Security Center, то информация о событиях может быть передана на Сервер администрирования Kaspersky Security Center. Подробнее о работе с отчетами в Kaspersky Security Center вы можете прочитать в Справочной системе Kaspersky Security Center.

Настройка параметров отчетов

Вы можете выполнить следующие действия для настройки параметров отчетов:

- Настроить максимальный срок 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. Вы можете отменить ограничение по времени или изменить максимальный срок хранения отчетов.

- Настроить максимальный размер 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. Вы можете отменить ограничение на размер файла отчета или установить другое значение.

В этом разделе

Настройка максимального срока хранения отчетов

► *Чтобы настроить максимальный срок хранения отчетов, выполните следующие действия:*

1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 46).
2. В левой части окна в разделе **Общие параметры** выберите подраздел **Отчеты и хранение**.
3. В правой части окна в блоке **Отчеты** выполните одно из следующих действий:
   - Установите флажок **Хранить отчеты не более**, если хотите ограничить срок хранения отчетов. В поле справа от флажка **Хранить отчеты не более** укажите максимальный срок хранения отчетов.

     По умолчанию максимальный срок хранения отчетов составляет 30 дней.
   - Снимите флажок **Хранить отчеты не более**, если хотите отменить ограничение срока хранения отчетов.

   По умолчанию ограничение срока хранения отчетов включено.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Настройка максимального размера файла отчета

► *Чтобы настроить максимальный размер файла отчета, выполните следующие действия:*

1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 46).
2. В левой части окна в разделе **Общие параметры** выберите подраздел **Отчеты и хранение**.
3. В правой части окна в блоке **Отчеты** выполните одно из следующих действий:
   - Установите флажок **Максимальный размер файла**, если хотите ограничить размер файла отчета. В поле справа от флажка **Максимальный размер файла** укажите максимальный размер файла отчета.

     По умолчанию ограничение размера файла отчета составляет 1024 МБ.
   - Снимите флажок **Максимальный размера файла**, если хотите отменить ограничение на размер файла отчета.

   По умолчанию ограничение размера файла отчета включено.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

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. Откройте главное окно программы (на стр. 43).
2. Нажмите на кнопку **Отчеты**, расположенную в нижней части главного окна программы.

   Откроется окно **Отчеты**.
3. 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 работе 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**.

Просмотр информации о событии в отчете

Вы можете просматривать подробную сводную информацию о каждом событии в отчете.

► *Чтобы просмотреть подробную сводную информацию о событии в отчете, выполните следующие действия:*

1. Откройте главное окно программы (на стр. 43).
2. Нажмите на кнопку **Отчеты**, расположенную в нижней части главного окна программы.

   Откроется окно **Отчеты**.
3. В левой части окна выберите нужный вам отчет о работе компонента или задачи.

   В правой части окна в таблице отобразятся события, входящие в состав отчета. Для поиска отдельных событий в отчете можно использовать функции фильтрации, поиска и сортировки.
4. Выберите в отчете нужное вам событие.

В нижней части окна отобразится блок со сводной информацией о событии.

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. Откройте главное окно программы (на стр. 43).
2. Нажмите на кнопку **Отчеты**, расположенную в нижней части главного окна программы.

   Откроется окно **Отчеты**.
3. В левой части окна **Отчеты** в списке компонентов и задач выберите компонент или задачу.

   В правой части окна отобразится отчет, содержащий список событий о работе выбранного компонента или задачи Kaspersky Endpoint Security.
4. Если требуется, измените представление данных в отчете с помощью следующих способов:
   - фильтрация событий;
   - поиск событий;
   - изменение расположения граф;
   - сортировка событий.
5. Нажмите на кнопку **Сохранить отчет**, расположенную в верхней правой части окна.

   Откроется контекстное меню.
6. В контекстном меню выберите нужную кодировку для сохранения файла отчета: **Сохранить в ANSI** или **Сохранить в Unicode**.

   Откроется стандартное окно Microsoft Windows **Сохранить как**.
7. В открывшемся окне **Сохранить как** укажите папку, в которую вы хотите сохранить файл отчета.
8. В поле **Имя файла** введите название файла отчета.
9. В поле **Тип файла** выберите нужный формат файла отчета: TXT или CSV.
10. Нажмите на кнопку **Сохранить**.

Удаление информации из отчетов

► *Чтобы удалить информацию из отчетов, выполните следующие действия*:

1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 46).
2. В левой части окна в разделе **Общие параметры** выберите подраздел **Отчеты и хранение**.
3. В правой части окна в блоке **Отчеты** нажмите на кнопку **Удалить отчеты**.

   Откроется окно **Удаление отчетов**.
4. Установите флажки для тех отчетов, из которых вы хотите удалить информацию:

- **Все отчеты**.
- **Отчет компонентов защиты**. Содержит информацию о работе следующих компонентов Kaspersky Endpoint Security:
  - Анализ поведения.
  - Защита от эксплойтов.
  - Предотвращение вторжений.
  - Защита от файловых угроз.
  - Защита от веб-угроз.
  - Защита от почтовых угроз.
  - Защита от сетевых угроз.
  - Защита от атак BadUSB.
- **Отчет компонентов контроля**. Содержит информацию о работе следующих компонентов Kaspersky Endpoint Security:
  - Контроль программ.
  - Веб-Контроль.
- **Отчет о шифровании данных**. Содержит информации о выполненных задачах шифрования данных.
- **Отчет задач проверки**. Содержит информацию о следующих выполненных задачах проверки:
  - Полная проверка.
  - Проверка важных областей.
  - Выборочная проверка.

  Информация о выполнении задачи Проверка целостности удаляется только если установлен флажок **Все отчеты**.
- **Отчет задач обновления**. Содержит информацию о выполненных задачах обновления.
- **Отчет компонента Сетевой экран**. Содержит информацию о работе Сетевого экрана.

5. Нажмите на кнопку **ОК**.

Служба уведомлений

Этот раздел содержит информацию о службе уведомлений, оповещающих пользователя о событиях в работе Kaspersky Endpoint Security, а также инструкции о том, как настроить параметры уведомлений.

В этом разделе

Об уведомлениях Kaspersky Endpoint Security

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 антивирусных баз программы, а может фиксировать ошибку в работе некоторого компонента, которую 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.

Настройка параметров службы уведомлений

Вы можете выполнить следующие действия для настройки службы уведомлений:

- Настроить параметры журналов событий, где Kaspersky Endpoint Security сохраняет события.
- Настроить отображение уведомлений на экране.
- Настроить доставку уведомлений по электронной почте.

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. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 46).
2. В левой части окна в разделе **Общие параметры** выберите подраздел **Интерфейс**.

   В правой части окна отобразятся параметры интерфейса Kaspersky Endpoint Security.
3. В блоке **Уведомления** нажмите на кнопку **Настройка**.

   Откроется окно **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.
4. В левой части окна выберите компонент или задачу, для которой вы хотите настроить параметры журналов событий.
5. В графах **Сохранять в локальном журнале** и **Сохранять в журнале событий Windows** установите флажки напротив нужных событий.

   События, напротив которых установлен флажок в графе **Сохранять в локальном журнале**, 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**.

   > События могут содержать следующие данные пользователя: пути к файлам, проверяемым с помощью Kaspersky Endpoint Security; пути к ключам реестра, изменяемым Kaspersky Endpoint Security; имя пользователя Microsoft Windows; адреса веб-страниц, открываемых пользователем.
6. Нажмите на кнопку **ОК**.
7. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Настройка отображения и доставки уведомлений

► *Чтобы настроить отображение и доставку уведомлений, выполните следующие действия:*

1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров

программы" на стр. 46).

2. В левой части окна в разделе **Общие параметры** выберите подраздел **Интерфейс**.

   В правой части окна отобразятся параметры интерфейса Kaspersky Endpoint Security.

3. В блоке **Уведомления** нажмите на кнопку **Настройка**.

   Откроется окно **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.

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.

   > События могут содержать следующие данные пользователя: пути к файлам, проверяемым с помощью Kaspersky Endpoint Security; пути к ключам реестра, изменяемым Kaspersky Endpoint Security; имя пользователя Microsoft Windows; адреса веб-страниц, открываемых пользователем.

7. Нажмите на кнопку **Настройка почтовых уведомлений**.

   Откроется окно **Настройка почтовых уведомлений**.

8. Установите флажок **Отправлять сообщения о событиях**, чтобы включить доставку информации о событиях в работе Kaspersky Endpoint Security, отмеченных в графе **Уведомлять по почте**.

9. Укажите параметры доставки почтовых уведомлений.

10. В окне **Настройка почтовых уведомлений** нажмите на кнопку **ОК**.

11. В окне **Уведомления** нажмите на кнопку **ОК**.

12. Нажмите на кнопку **Сохранить**, чтобы сохранить 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. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 46).

2. В левой части окна в разделе **Общие параметры** выберите подраздел **Интерфейс**.

   В правой части окна отобразятся параметры интерфейса Kaspersky Endpoint Security.

3. В блоке **Предупреждения** установите флажки напротив тех категорий событий, уведомления о

которых вы хотите видеть в области уведомлений Microsoft Windows.

4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

При возникновении событий, относящихся к выбранным категориям, значок программы (см. раздел "Значок программы в области уведомлений" на стр. 42) в области уведомлений будет меняться на  или  в зависимости от важности предупреждения.

Работа с резервным хранилищем

Этот раздел содержит инструкции о том, как настроить параметры резервного хранилища и как работать с резервным хранилищем.

В этом разделе

О резервном хранилище

Резервное хранилище – это список резервных копий файлов, которые были удалены или изменены в процессе лечения. *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 ProgramData\Kaspersky Lab\KES\QB.

Права доступа к этой папке предоставлены пользователям группы Administrators. 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.

Настройка параметров резервного хранилища

Вы можете выполнить следующие действия для настройки параметров резервного хранилища:

- Настроить максимальный срок хранения копий 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. Вы можете отменить ограничение по времени или

изменить максимальный срок хранения файлов.

- Настроить максимальный размер резервного хранилища.

  По умолчанию максимальный размер резервного хранилища составляет 100 МБ. После достижения максимального размера Kaspersky Endpoint Security автоматически удаляет наиболее старые файлы из резервного хранилища таким образом, чтобы не превышался его максимальный размер. Вы можете отменить ограничение на максимальный размер резервного хранилища или изменить максимальный размер.

В этом разделе

Настройка максимального срока хранения файлов в резервном хранилище

► *Чтобы настроить максимальный срок хранения файлов в резервном хранилище, выполните следующие действия:*

1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 46).
2. В левой части окна в разделе **Общие параметры** выберите подраздел **Отчеты и хранение**.
3. Выполните одно из следующих действий:
   - В правой части окна в блоке **Резервное хранилище** установите флажок **Хранить объекты не более**, если хотите ограничить срок хранения копий файлов в резервном хранилище. В поле справа от флажка **Хранить объекты не более** укажите максимальный срок хранения копий файлов в резервном хранилище. По умолчанию максимальный срок хранения копий файлов в резервном хранилище составляет 30 дней.
   - В правой части окна в блоке **Резервное хранилище** снимите флажок **Хранить объекты не более**, если хотите отменить ограничение срока хранения копий файлов в резервном хранилище.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Настройка максимального размера резервного хранилища

► *Чтобы настроить максимальный размер резервного хранилища, выполните следующие действия:*

1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 46).
2. В левой части окна в разделе **Общие параметры** выберите подраздел **Отчеты и хранение**.
3. Выполните одно из следующих действий:
   - Если вы хотите ограничить суммарный размер резервного хранилища, установите флажок

Максимальный размер хранилища в правой части окна в блоке **Резервное хранилище** и укажите максимальный размер резервного хранилища в поле справа от флажка **Максимальный размер хранилища**.

По умолчанию максимальный размер хранилища данных, включающего в себя резервные копии файлов, составляет 100 МБ.

- Если вы хотите отменить ограничение на размер резервного хранилища, снимите флажок **Максимальный размер хранилища** в правой части окна в блоке **Параметры резервного хранилища**.

По умолчанию размер резервного хранилища не ограничен.

4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Восстановление и удаление файлов из резервного хранилища

Если в файле обнаружен вредоносный код, Kaspersky Endpoint Security блокирует файл, присваивает ему статус *Зараженный*, 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.

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*).

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.

Набор резервных копий файлов представлен в виде таблицы.

Работая с резервным хранилищем, вы можете выполнять следующие действия с резервными копиями файлов:

- Просматривать набор резервных копий файлов.

  Для резервной копии файла отображается путь к папке исходного размещения этого файла. Путь к папке исходного размещения файла может содержать персональные данные.

- Восстанавливать файлы из резервных копий в папки их исходного размещения.
- Удалять резервные копии файлов из резервного хранилища.

Кроме того, вы можете выполнять следующие действия, работая с табличными данными:

- фильтровать резервные копии по графам, в том числе по условиям сложного фильтра;
- использовать функцию поиска резервных копий;
- сортировать резервные копии;
- изменять порядок и набор граф, отображаемых в таблице резервных копий.

Вы можете скопировать информацию о выбранных файлах резервного хранилища в буфер обмена. Чтобы выбрать несколько файлов резервного хранилища, откройте по правой клавише мыши контекстное меню любого файла и выберите пункт **Выделить все**. Далее отметьте те файлы, с которых вы хотите снять выделение, удерживая клавишу **CTRL**.

В этом разделе

Восстановление файлов из резервного хранилища

Если в резервное хранилище помещено несколько расположенных в одной и той же папке файлов с одинаковыми именами и различным содержимым, то для восстановление доступен только тот файл, который был помещен в резервное хранилище последним.

► *Чтобы восстановить файлы из резервного хранилища, выполните следующие действия:*

1. Откройте главное окно программы (на стр. 43).
2. Нажмите на кнопку **Хранилища**, расположенную в нижней части главного окна программы.

   Откроется окно **Резервное хранилище**.
3. Если вы хотите восстановить все файлы из резервного хранилища, то в окне **Резервное хранилище** в контекстном меню любого файла выберите пункт **Восстановить все**.

   Kaspersky Endpoint Security восстановит все файлы из их резервных копий в папки их исходного размещения.
4. Если вы хотите восстановить один или несколько файлов из резервного хранилища, то выполните следующие действия:
   a. В таблице в окне **Резервное хранилище** выберите один или несколько файлов резервного хранилища.

      Чтобы выбрать несколько файлов резервного хранилища, откройте по правой клавише мыши контекстное меню любого файла и выберите пункт **Выделить все**. Далее отметьте те файлы, с которых вы хотите снять выделение, удерживая клавишу **CTRL**.
   b. Восстановите файлы одним из следующих способов:
      - Нажмите на кнопку **Восстановить**.

- По правой клавише мыши откройте контекстное меню и выберите пункт **Восстановить**.

Kaspersky Endpoint Security восстановит файлы из выбранных резервных копий в папки их исходного размещения.

Удаление резервных копий файлов из резервного хранилища

► *Чтобы удалить резервные копии файлов из резервного хранилища, выполните следующие действия:*

1. Откройте главное окно программы (на стр. 43).
2. Нажмите на кнопку **Хранилища**, расположенную в нижней части главного окна программы.
3. Откроется окно **Резервное хранилище**.
4. Если вы хотите удалить все файлы из резервного хранилища, то выполните одно из следующих действий:
   - В контекстном меню любого файла выберите пункт **Удалить все**.
   - Нажмите на кнопку **Очистить хранилище**.

   Kaspersky Endpoint Security удалит все резервные копии файлов из резервного хранилища.
5. Если вы хотите удалить один или несколько файлов из резервного хранилища, то выполните следующие действия:
   a. В таблице в окне **Резервное хранилище** выберите один или несколько файлов резервного хранилища.

      Чтобы выбрать несколько файлов резервного хранилища, откройте по правой клавише мыши контекстное меню любого файла и выберите пункт **Выделить все**. Далее отметьте те файлы, с которых вы хотите снять выделение, удерживая клавишу **CTRL**.

   b. Удалите файлы одним из следующих способов:
      - Нажмите на кнопку **Удалить**.
      - По правой клавише мыши откройте контекстное меню и выберите пункт **Удалить**.

   Kaspersky Endpoint Security удалит выбранные резервные копии файлов из резервного хранилища.

Дополнительная настройка программы

Этот раздел содержит информацию о настройке общих параметров Kaspersky Endpoint Security.

В этом разделе

Доверенная зона

Этот раздел содержит информацию о доверенной зоне и инструкции о том, как настроить исключения из проверки и сформировать список доверенных программ.

В этом разделе

О доверенной зоне

Доверенная зона - это сформированный администратором системы список объектов и программ, которые Kaspersky Endpoint Security не контролирует в процессе работы. Иначе говоря, это набор исключений из проверки.

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.

Вы можете исключать из проверки следующее:

- файлы определенного формата;
- файлы по маске;
- отдельные файлы;
- папки;
- процессы программ.

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 в качестве вспомогательного компонента вредоносной программы. К таким программам относятся, например, программы удаленного администрирования, IRC-клиенты, FTP-серверы, различные утилиты для остановки процессов или сокрытия их работы, клавиатурные шпионы, программы вскрытия паролей, программы автоматического дозвона на платные веб-сайты. Это программное обеспечение не классифицируется как вирусы. 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" по ссылке www.securelist.com/ru/threats/detect http://www.securelist.com/ru/threats/detect.

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 Remote Administrator. Это система удаленного доступа, позволяющая работать на удаленном компьютере. 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.
- Защита от эксплойтов.
- Предотвращение вторжений.
- Защита от файловых угроз.
- Защита от веб-угроз.

- Защита от почтовых угроз.
- Задачи проверки.

Список 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. 223).

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.

Создание исключения из проверки

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.

► *Чтобы создать исключение из проверки, выполните следующие действия:*

1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 46).
2. В левой части окна в разделе **Общие параметры** выберите подраздел **Исключения**.

   В правой части окна отобразятся параметры исключений.
3. В блоке **Исключения из проверки и доверенная зона** нажмите на кнопку **Настройка**.

   Откроется окно **Доверенная зона** на закладке **Исключения из проверки**.

4. Нажмите на кнопку **Добавить**.

   Откроется окно **Исключение из проверки**. В этом окне вы можете сформировать исключение из проверки, используя один или несколько критериев из блока **Свойства**.

5. Если вы хотите исключить из проверки файл или папку, выполните следующие действия:

   a. В блоке **Свойства** установите флажок **Файл или папка**.

   b. По ссылке **выберите файл или папку**, расположенной в блоке **Описание исключения из проверки**, откройте окно **Имя файла или папки**.

   c. Введите имя файла или папки, маску имени файла или папки или выберите файл или папку в дереве папок, нажав на кнопку **Обзор**.

   d. Нажмите на кнопку **ОК** в окне **Имя файла или папки**.

      Ссылка на добавленный файл или папку появится в блоке **Описание исключения из проверки** окна **Исключение из проверки**.

6. Если вы хотите исключить из проверки объекты с определенным названием, выполните следующие действия:

   a. В блоке **Свойства** установите флажок **Название объекта**.

   b. По ссылке **введите название объекта**, расположенной в блоке **Описание исключения из проверки**, откройте окно **Название объекта**.

   c. Введите название или маску названия объекта согласно классификации Вирусной энциклопедии "Лаборатории Касперского".

   d. Нажмите на кнопку **ОК** в окне **Название объекта**.

      Ссылка на добавленное название объекта появится в блоке **Описание исключения из проверки** окна **Исключение из проверки**.

7. Если вы хотите исключить из проверки объект с определенным хешем, выполните следующие действия:

   a. В блоке **Свойства** установите флажок **Хеш объекта**.

   b. По ссылке **введите хеш объекта**, расположенной в блоке **Описание исключения из проверки**, откройте окно **Хеш объекта**.

   c. Введите SHA256-хеш объекта согласно классификации Вирусной энциклопедии "Лаборатории Касперского" или выберите файл, нажав на кнопку **Обзор**.

   d. Нажмите на кнопку **ОК** в окне **Хеш объекта**.

      Ссылка на добавленный хеш объекта появится в блоке **Описание исключения из проверки** окна **Исключение из проверки**.

8. Если необходимо, в поле **Комментарий** введите краткий комментарий к создаваемому исключению из проверки.

9. Определите компоненты Kaspersky Endpoint Security, в работе которых должно быть использовано исключение из проверки:

   a. По ссылке **любые**, расположенной в блоке **Описание исключения из проверки**, активируйте ссылку **выберите компоненты**.

   b. По ссылке **выберите компоненты** откройте окно **Компоненты защиты**.

   c. Установите флажки напротив тех компонентов, на работу которых должно распространяться исключение из проверки.

d. Нажмите на кнопку **ОК** в окне **Компоненты защиты**.

Если компоненты указаны в параметрах исключения из проверки, то исключение применяется при проверке только этими компонентами Kaspersky Endpoint Security.

Если компоненты не указаны в параметрах исключения из проверки, то исключение применяется при проверке всеми компонентами Kaspersky Endpoint Security.

10. Нажмите на кнопку **ОК** в окне **Исключение из проверки**.

Добавленное исключение из проверки появится в таблице на закладке **Исключения из проверки** окна **Доверенная зона**. В блоке **Описание исключения из проверки** отобразятся заданные параметры этого исключения из проверки.

11. Нажмите на кнопку **ОК** в окне **Доверенная зона**.
12. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Изменение исключения из проверки

► *Чтобы изменить исключение из проверки, выполните следующие действия:*

1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 46).
2. В левой части окна в разделе **Общие параметры** выберите подраздел **Исключения**.

   В правой части окна отобразятся параметры исключений.
3. В блоке **Исключения из проверки и доверенная зона** нажмите на кнопку **Настройка**.

   Откроется окно **Доверенная зона** на закладке **Исключения из проверки**.
4. В списке выберите нужное исключение из проверки.
5. Измените параметры исключения из проверки одним из следующих способов:
   - Нажмите на кнопку **Изменить**.

     Откроется окно **Исключения из проверки**.
   - Откройте окно для изменения нужного параметра по ссылке в поле **Описание исключения из проверки**.
6. Если на предыдущем шаге вы нажали на кнопку **Изменить**, нажмите на кнопку **ОК** в окне **Исключение из проверки**.

   В блоке **Описание исключения из проверки** отобразятся измененные параметры исключения из проверки.
7. Нажмите на кнопку **ОК** в окне **Доверенная зона**.
8. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Удаление исключения из проверки

► *Чтобы удалить исключение из проверки, выполните следующие действия:*

1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 46).

2. В левой части окна в разделе **Общие параметры** выберите подраздел **Исключения**.

   В правой части окна отобразятся параметры исключений.

3. В блоке **Исключения из проверки и доверенная зона** нажмите на кнопку **Настройка**.

   Откроется окно **Доверенная зона** на закладке **Исключения из проверки**.

4. В списке исключений из проверки выберите нужное исключение из проверки.
5. Нажмите на кнопку **Удалить**.

   Удаленное исключение из проверки исчезнет из списка.

6. Нажмите на кнопку **ОК** в окне **Доверенная зона**.
7. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Запуск и остановка работы исключения из проверки

► *Чтобы запустить или остановить работу исключения из проверки, выполните следующие действия:*

1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 46).
2. В левой части окна в разделе **Общие параметры** выберите подраздел **Исключения**.

   В правой части окна отобразятся параметры исключений.

3. В блоке **Исключения из проверки и доверенная зона** нажмите на кнопку **Настройка**.

   Откроется окно **Доверенная зона** на закладке **Исключения из проверки**.

4. В списке исключений из проверки выберите нужное исключение.
5. Выполните одно из следующих действий:
   - Установите флажок рядом с названием исключения из проверки, если вы хотите запустить работу этого исключения.
   - Снимите флажок рядом с названием исключения из проверки, если вы хотите временно приостановить работу этого исключения.
6. Нажмите на кнопку **ОК**.
7. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Формирование списка доверенных программ

► *Чтобы сформировать список доверенных программ, выполните следующие действия:*

1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 46).
2. В левой части окна в разделе **Общие параметры** выберите подраздел **Исключения**.

   В правой части окна отобразятся параметры исключений.

3. В блоке **Исключения из проверки и доверенная зона** нажмите на кнопку **Настройка**.

Откроется окно **Доверенная зона**.

4. В окне **Доверенная зона** выберите закладку **Доверенные программы**.
5. Если вы хотите добавить программу в список доверенных программ, выполните следующие действия:
   a. Нажмите на кнопку **Добавить**.
   b. В раскрывшемся контекстном меню выполните одно из следующих действий:
      - Выберите пункт **Программы**, если вы хотите найти программу в списке установленных на компьютере программ.

        Откроется окно **Выбор программы**.
      - Выберите пункт **Обзор**, если вы хотите указать путь к исполняемому файлу нужной программы.

        Откроется стандартное окно Microsoft Windows **Открыть**.
   c. Выберите программу одним из следующих способов:
      - Если на предыдущем шаге вы выбрали пункт **Программы**, выберите программу в списке установленных на компьютере программ и нажмите на кнопку **ОК** в окне **Выбор программы**.
      - Если на предыдущем шаге вы выбрали пункт **Обзор**, укажите путь к исполняемому файлу нужной программы и нажмите на кнопку **Открыть** в стандартном окне Microsoft Windows **Открыть**.

   В результате выполненных действий откроется окно **Исключения из проверки для программы**.
   d. Установите флажки напротив нужных правил доверенной зоны для выбранной программы:
      - **Не проверять открываемые файлы**.
      - **Не контролировать активность программы**.
      - **Не наследовать ограничения родительского процесса (программы)**.
      - **Не контролировать активность дочерних программ**.
      - **Не блокировать взаимодействие с интерфейсом программы**.
      - **Не проверять сетевой трафик**.
   e. Нажмите на кнопку **ОК** в окне **Исключения из проверки для программы**.

      В списке доверенных программ появится добавленная доверенная программа.
6. Если вы хотите изменить параметры доверенной программы, выполните следующие действия:
   a. Выберите доверенную программу из списка доверенных программ.
   b. Нажмите на кнопку **Изменить**.
   c. Откроется окно **Исключения из проверки для программы**.
   d. Установите или снимите флажки напротив нужных правил доверенной зоны для выбранной программы.

Если в окне **Исключения из проверки для программы** не выбрано ни одно из правил доверенной зоны для программы, то происходит включение доверенной программы в проверку (см. раздел "Включение и выключение действия правил доверенной зоны на программу из списка доверенных программ" на стр. 225). Доверенная программа не удаляется из списка доверенных программ, но флажок для нее снимается.

e. Нажмите на кнопку **OK** в окне **Исключения из проверки для программы**.

7. Если вы хотите удалить доверенную программу из списка доверенных программ, выполните следующие действия:

   a. Выберите доверенную программу из списка доверенных программ.

   b. Нажмите на кнопку **Удалить**.

8. Нажмите на кнопку **OK** в окне **Доверенная зона**.

9. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

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. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 46).

2. В левой части окна в разделе **Общие параметры** выберите подраздел **Исключения**.

   В правой части окна отобразятся параметры исключений.

3. В блоке **Исключения из проверки и доверенная зона** нажмите на кнопку **Настройка**.

   Откроется окно **Доверенная зона**.

4. В окне **Доверенная зона** выберите закладку **Доверенные программы**.

5. В списке доверенных программ выберите нужную доверенную программу.

6. Выполните одно из следующих действий:

   - Установите флажок рядом с названием доверенной программы, если хотите выключить ее из проверки Kaspersky Endpoint Security.

   - Снимите флажок рядом с названием доверенной программы, если хотите включить ее в проверку Kaspersky Endpoint Security.

7. Нажмите на кнопку **OK**.

8. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Использование доверенного системного хранилища сертификатов

Использование системного хранилища сертификатов позволяет исключать из антивирусной проверки программы, подписанные доверенной цифровой подписью.

► *Чтобы начать использовать доверенное системное хранилище сертификатов, выполните следующие действия:*

1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 46).
2. В левой части окна в разделе **Общие параметры** выберите подраздел **Исключения**.

   В правой части окна отобразятся параметры исключений.
3. В блоке **Исключения из проверки и доверенная зона** нажмите на кнопку **Настройка**.

   Откроется окно **Доверенная зона**.
4. В окне **Доверенная зона** выберите закладку **Доверенное системное хранилище сертификатов**.
5. Установите флажок **Использовать доверенное системное хранилище сертификатов**.
6. В раскрывающемся списке **Доверенное системное хранилище сертификатов** выберите, какое системное хранилище Kaspersky Endpoint Security должен считать доверенным.
7. Нажмите на кнопку **ОК** в окне **Доверенная зона**.
8. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Контроль сетевого трафика

Этот раздел содержит информацию о контроле сетевого трафика и инструкции о том, как настроить параметры контролируемых сетевых портов.

В этом разделе

О контроле сетевого трафика

Во время работы Kaspersky Endpoint Security компоненты Защита от почтовых угроз (на стр. 108) и Защита от веб-угроз (на стр. 102) контролируют потоки данных, передаваемые по определенным протоколам и проходящие через определенные открытые TCP- и UDP-порты компьютера пользователя. Так, 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 операционной системы на несколько групп в соответствии с вероятностью их взлома. Сетевые порты, отведенные для служб, которые могут быть уязвимыми, следует 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 компонент Защита от почтовых угроз и компонент Защита от веб-угроз должны обращать особое внимание во время слежения за сетевым трафиком.

Настройка параметров контроля сетевого трафика

Вы можете выполнить следующие действия для настройки параметров контроля сетевого трафика:

- Включить контроль всех сетевых портов.
- Сформировать список контролируемых сетевых портов.
- Сформировать список программ, для которых контролируются все сетевые порты.

В этом разделе

Включение контроля всех сетевых портов

► *Чтобы включить контроль всех сетевых портов, выполните следующие действия:*

1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 46).
2. В левой части окна в разделе **Общие параметры** выберите подраздел **Исключения**.

   В правой части окна отобразятся параметры исключений.
3. В блоке **Контролируемые порты** выберите вариант **Контролировать все сетевые порты**.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Формирование списка контролируемых сетевых портов

► *Чтобы сформировать список контролируемых сетевых портов, выполните следующие действия:*

1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 46).
2. В левой части окна в разделе **Общие параметры** выберите подраздел **Исключения**.

   В правой части окна отобразятся параметры исключений.
3. В блоке **Контролируемые порты** выберите вариант **Контролировать только выбранные порты**.
4. Нажмите на кнопку **Настройка**.

   Откроется окно **Сетевые порты**. В окне **Сетевые порты** находится список сетевых портов, которые обычно используются для передачи электронной почты и сетевого трафика. Этот список сетевых портов включен в поставку Kaspersky Endpoint Security.
5. В списке сетевых портов выполните следующие действия:
   - Установите флажки напротив названий тех сетевых портов, которые вы хотите включить в список контролируемых сетевых портов.

     По умолчанию флажки установлены для всех сетевых портов, представленных в окне **Сетевые**

порты.

- Снимите флажки напротив названий тех сетевых портов, которые вы хотите исключить из списка контролируемых сетевых портов.

6. Если сетевой порт отсутствует в списке сетевых портов, добавьте его следующим образом:
   a. По ссылке **Добавить**, расположенной под списком сетевых портов, откройте окно **Сетевой порт**.
   b. В поле **Порт** введите номер сетевого порта.
   c. В поле **Описание** введите название сетевого порта.
   d. Нажмите на кнопку **ОК**.

      Окно **Сетевой порт** закроется. Добавленный вами сетевой порт отобразится в конце списка сетевых портов.
7. Нажмите на кнопку **ОК** в окне **Сетевые порты**.
8. Нажмите на кнопку **Сохранить**, чтобы сохранить 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, требуется установить флажок **Контролировать все сетевые порты** в блоке **Контролируемые порты** или настроить контроль всех сетевых портов для программ (см. раздел "Формирование списка программ, для которых контролируются все сетевые порты" на стр. 228), с помощью которых устанавливается FTP-соединение.

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. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 46).
2. В левой части окна в разделе **Общие параметры** выберите подраздел **Исключения**.

   В правой части окна отобразятся параметры исключений.
3. В блоке **Контролируемые порты** выберите вариант **Контролировать только выбранные порты**.
4. Нажмите на кнопку **Настройка**.

   Откроется окно **Сетевые порты**.
5. Установите флажок **Контролировать все порты для указанных программ**.

6. В списке программ, расположенном под флажком **Контролировать все порты для указанных программ**, выполните следующие действия:
   - Установите флажки напротив названий программ, для которых нужно контролировать все сетевые порты.

     По умолчанию флажки установлены для всех программ, представленных в окне **Сетевые порты**.
   - Снимите флажки напротив названий программ, для которых не нужно контролировать все сетевые порты.
7. Если программа отсутствует в списке программ, добавьте ее следующим образом:
   a. По ссылке **Добавить**, расположенной под списком программ, откройте контекстное меню.
   b. Выберите в контекстном меню способ добавления программы в список программ:
      - Выберите пункт **Программы**, если вы хотите выбрать программу из списка программ, установленных на компьютере. Откроется окно **Выбор программы**, с помощью которого вы можете указать название программы.
      - Выберите пункт **Обзор**, если вы хотите указать местонахождение исполняемого файла программы. Откроется стандартное окно Microsoft Windows **Открыть**, с помощью которого вы можете указать название исполняемого файла программы.

     После выбора программы откроется окно **Программа**.
   c. В поле **Название** введите название для выбранной программы.
   d. Нажмите на кнопку **OK**.

     Окно **Программа** закроется. Добавленная вами программа отобразится в конце списка программ.
8. Нажмите на кнопку **OK** в окне **Сетевые порты**.
9. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Самозащита Kaspersky Endpoint Security

Этот раздел содержит информацию о механизмах самозащиты Kaspersky Endpoint Security и защиты от внешнего управления Kaspersky Endpoint Security и инструкции о том, как настроить параметры этих механизмов.

В этом разделе

О самозащите 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.

Стабильность системы безопасности компьютера пользователя обеспечивают реализованные в Kaspersky Endpoint Security механизмы самозащиты и защиты от внешнего управления.

Механизм самозащиты предотвращает изменение и удаление файлов программы на жестком диске, процессов в памяти, записей в системном реестре.

Механизм защиты от внешнего управления позволяет блокировать все попытки управления службами программы 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.

Включение и выключение механизма самозащиты

По умолчанию механизм самозащиты Kaspersky Endpoint Security включен. При необходимости вы можете выключить механизм самозащиты.

► *Чтобы включить или выключить механизм самозащиты, выполните следующие действия:*

1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 46).
2. В левой части окна в разделе **Общие параметры** выберите подраздел **Параметры программы**.

   В правой части окна отобразятся дополнительные параметры Kaspersky Endpoint Security.
3. Выполните одно из следующих действий:
   - Установите флажок **Включить самозащиту**, если вы хотите включить механизм самозащиты.
   - Снимите флажок **Включить самозащиту**, если вы хотите выключить механизм самозащиты.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Включение и выключение механизма защиты от внешнего управления

По умолчанию механизм защиты от внешнего управления включен. При необходимости вы можете выключить механизм защиты от внешнего управления.

► *Чтобы включить или выключить механизм защиты от внешнего управления, выполните следующие действия:*

1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров

программы" на стр. 46).

2. В левой части окна в разделе **Общие параметры** выберите подраздел **Параметры программы**.

   В правой части окна отобразятся дополнительные параметры Kaspersky Endpoint Security.

3. Выполните одно из следующих действий:

   - Установите флажок **Выключить внешнее управление системными службами**, если вы хотите включить механизм защиты от внешнего управления.
   - Снимите флажок **Выключить внешнее управление системными службами**, если вы хотите выключить механизм защиты от внешнего управления.

4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

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. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 46).
2. В левой части окна в разделе **Общие параметры** выберите подраздел **Исключения**.

   В правой части окна отобразятся параметры исключений.

3. В блоке **Исключения из проверки и доверенная зона** нажмите на кнопку **Настройка**.

   Откроется окно **Доверенная зона**.

4. В окне **Доверенная зона** выберите закладку **Доверенные программы**.
5. Нажмите на кнопку **Добавить**.
6. В раскрывшемся контекстном меню выполните одно из следующих действий:

   - Выберите пункт **Программы**, если вы хотите найти программу удаленного администрирования в списке установленных на компьютере программ.

     Откроется окно **Выбор программы**.

   - Выберите пункт **Обзор**, если вы хотите указать путь к исполняемому файлу программы удаленного администрирования.

     Откроется стандартное окно Microsoft Windows **Открыть**.

7. Выберите программу одним из следующих способов:

   - Если на предыдущем шаге вы выбрали пункт **Программы**, выберите программу в списке установленных на компьютере программ и нажмите на кнопку **ОК** в окне **Выбор программы**.
   - Если на предыдущем шаге вы выбрали пункт **Обзор**, укажите путь к исполняемому файлу нужной программы и нажмите на кнопку **Открыть** в стандартном окне Microsoft Windows **Открыть**.

   В результате выполненных действий откроется окно **Исключения из проверки для программы**.

8. Установите флажок **Не контролировать активность программы**.

9. Нажмите на кнопку **ОК** в окне **Исключения из проверки для программы**.

   В списке доверенных программ появится добавленная доверенная программа.

10. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Производительность Kaspersky Endpoint Security и совместимость с другими программами

Этот раздел содержит информацию о производительности Kaspersky Endpoint Security и совместимости с другими программами, а также инструкции о том, как выбрать тип обнаруживаемых объектов и режим работы Kaspersky Endpoint Security.

В этом разделе

О производительности Kaspersky Endpoint Security и совместимости 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. 234), 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 (см. раздел "О задачах проверки" на стр. 186);
- задача проверки важных областей (см. раздел "О задачах проверки" на стр. 186);
- задача выборочной проверки (см. раздел "О задачах проверки" на стр. 186);
- задача проверки целостности (см. раздел "О задаче проверки целостности" на стр. 200).

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 (см. раздел "Включение и выключение технологии лечения активного заражения для рабочих станций" на стр. 234). *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 файловых серверов невозможен из-за особенностей программы Kaspersky Endpoint Security для файловых серверов. 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 для файловых серверов" на стр. 235).

В случае обнаружения активного заражения на файловом сервере, на Kaspersky Security Center передается событие о необходимости лечения активного заражения. Для лечения активного заражения на файловом сервере требуется включить технологию лечения активного заражения для файловых серверов и запустить групповую задачу *Поиск вирусов* в удобное для пользователей файлового сервера время.

Выбор типов обнаруживаемых объектов

► *Чтобы выбрать типы обнаруживаемых объектов, выполните следующие действия:*

1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 46).
2. В левой части окна в разделе **Общие параметры** выберите подраздел **Исключения**.

   В правой части окна отобразятся параметры исключений.
3. В блоке **Объекты для обнаружения** нажмите на кнопку **Настройка**.

   Откроется окно **Объекты для обнаружения**.
4. Установите флажки для типов объектов, которые должен обнаруживать Kaspersky Endpoint Security:
   - **Вредоносные утилиты**.
   - **Рекламные программы**.
   - **Программы автодозвона**.
   - **Другие**.
   - **Упакованные файлы, которые могут нанести вред**.
   - **Многократно упакованные файлы**.
5. Нажмите на кнопку **ОК**.

   Окно **Объекты для обнаружения** закроется. В блоке **Объекты для обнаружения** под надписью **Включено обнаружение объектов следующих типов** отобразятся выбранные вами типы объектов.
6. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Включение и выключение технологии лечения активного заражения для рабочих станций

► *Чтобы включить или выключить технологию лечения активного заражения для рабочих станций, выполните следующие действия:*

1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 46).
2. В левой части окна в разделе **Общие параметры** выберите подраздел **Параметры программы**.

   В правой части окна отобразятся дополнительные параметры Kaspersky Endpoint Security.
3. В правой части окна выполните одно из следующих действий:
   - Установите флажок **Применять технологию лечения активного заражения**, если хотите включить технологию лечения активного заражения.

- Снимите флажок **Применять технологию лечения активного заражения**, если хотите выключить технологию лечения активного заражения.

4. Нажмите на кнопку **Сохранить**, чтобы сохранить 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.

Включение и выключение технологии лечения активного заражения для файловых серверов

► *Чтобы включить технологию лечения активного заражения для файловых 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 файловых 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. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 46).
2. В левой части окна в разделе **Общие параметры** выберите подраздел **Параметры программы**.

В правой части окна отобразятся дополнительные параметры Kaspersky Endpoint Security.

3. В блоке **Производительность** выполните следующие действия:

   - Установите флажок **Откладывать задачи по расписанию при работе от аккумулятора**, если вы хотите включить 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.

   - Снимите флажок **Откладывать задачи по расписанию при работе от аккумулятора**, если вы хотите выключить режим энергосбережения. В этом случае Kaspersky Endpoint Security выполняет задачи, для которых задан запуск по расписанию, независимо от источника питания компьютера.

4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Включение и выключение режима передачи ресурсов другим программам

► *Чтобы включить или выключить режим передачи ресурсов другим программам, выполните следующие действия:*

1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 46).
2. В левой части окна в разделе **Общие параметры** выберите подраздел **Параметры программы**.

   В правой части окна отобразятся дополнительные параметры Kaspersky Endpoint Security.

3. В блоке **Производительность** выполните следующие действия:

   - Установите флажок **Уступать ресурсы другим программам**, если вы хотите включить 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.

   - Снимите флажок **Уступать ресурсы другим программам**, если вы хотите выключить режим передачи ресурсов другим программам. В этом случае Kaspersky Endpoint Security выполняет

задачи, для которых задан запуск по расписанию, независимо от работы других программ.

По умолчанию режим передачи ресурсов другим программам включен.

4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Защита паролем

Этот раздел содержит информацию об ограничении доступа к Kaspersky Endpoint Security с помощью пароля.

В этом разделе

Об ограничении доступа к Kaspersky Endpoint Security

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.

Чтобы ограничить доступ к Kaspersky Endpoint Security, вы можете задать имя пользователя и пароль и указать операции, для выполнения которых программа должна запрашивать эти данные.

При обновлении с предыдущих версий программы до Kaspersky Endpoint Security 11 для Windows пароль, если был задан, сохраняется. Для первого изменения параметров защиты паролем требуется использовать имя пользователя KLAdmin, заданное по умолчанию.

Включение и выключение защиты паролем

Рекомендуется с осторожностью использовать пароль для ограничения доступа к программе. Если вы забыли пароль, то для получения инструкций по выключению защиты паролем следует обратиться в Службу технической поддержки "Лаборатории Касперского" (см. раздел "Обращение в Службу технической поддержки" на стр. 284).

► *Чтобы включить защиту паролем, выполните следующие действия:*

1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 46).
2. В левой части окна в разделе **Общие параметры** выберите подраздел **Интерфейс**.

   В правой части окна отобразятся параметры интерфейса Kaspersky Endpoint Security.
3. В блоке **Защита паролем** нажмите на кнопку **Настройка**.

   Откроется окно **Защита паролем**.
4. Установите флажок **Включить защиту паролем**.
5. В поле **Имя пользователя** введите имя пользователя, которое нужно будет указывать в окне **Проверка пароля** при последующем совершении операций, защищенных паролем.
6. В поле **Новый пароль** введите пароль для доступа к программе.
7. В поле **Подтверждение пароля** повторите пароль.
8. Если вы хотите ограничить доступ для всех операций с программой, в блоке **Область действия пароля** нажмите на кнопку **Выбрать все**.
9. Если вы хотите ограничить доступ пользователя выборочно, в блоке **Область действия пароля** установите флажки рядом с названиями нужных операций:
   - **Настройка параметров программы**.
   - **Завершение работы программы**.
   - **Выключение компонентов защиты**.
   - **Выключение компонентов контроля**.
   - **Удаление ключа**.
   - **Удаление / изменение / восстановление программы**.
   - **Восстановление доступа к данным на зашифрованных устройствах**.
   - **Просмотр отчетов**.
10. Нажмите на кнопку **ОК**.

    Программа проверяет введенные пароли. Если пароли совпадают, программа применяет пароль. Если пароли не совпадают, программа предлагает повторно подтвердить пароль в поле **Подтверждение пароля**.
11. Нажмите на кнопку **Сохранить** в окне настройки параметров программы, чтобы сохранить внесенные изменения.

После включения защиты паролем программа будет запрашивать пароль каждый раз при совершении операции, включенной в область действия пароля. Вы можете установить флажок **Запомнить пароль на текущую сессию** в окне **Проверка пароля**, если вы хотите, чтобы во время текущей сессии работы программа больше не требовала ввода пароля при попытке выполнения защищенной операции.

Снятый флажок **Запомнить пароль на текущую сессию** означает, что программа запрашивает пароль каждый раз при попытке выполнения защищенной операции.

► *Чтобы выключить защиту паролем, выполните следующие действия:*

1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров

программы" на стр. 46).

2. В левой части окна в разделе **Общие параметры** выберите подраздел **Интерфейс**.

   В правой части окна отобразятся параметры интерфейса Kaspersky Endpoint Security.

3. В блоке **Защита паролем** нажмите на кнопку **Настройка**.

   Откроется окно **Защита паролем**.

4. Снимите флажок **Включить защиту паролем**.

5. Нажмите на кнопку **ОК**.

6. Нажмите на кнопку **Сохранить** в окне настройки параметров программы, чтобы сохранить внесенные изменения.

   Откроется окно **Проверка пароля**.

7. В поле **Имя пользователя** введите имя пользователя.

8. В поле **Пароль** введите пароль доступа к Kaspersky Endpoint Security.

9. Нажмите на кнопку **ОК**.

Изменение пароля доступа к Kaspersky Endpoint Security

► *Чтобы изменить пароль доступа к Kaspersky Endpoint Security, выполните следующие действия:*

1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 46).

2. В левой части окна в разделе **Общие параметры** выберите подраздел **Интерфейс**.

   В правой части окна отобразятся параметры интерфейса Kaspersky Endpoint Security.

3. В блоке **Защита паролем** нажмите на кнопку **Настройка**.

   Откроется окно **Защита паролем**.

4. В поле **Имя пользователя** введите имя пользователя.

5. В поле **Новый пароль** введите новый пароль для доступа к программе.

6. В поле **Подтверждение пароля** повторите новый пароль.

7. Нажмите на кнопку **ОК**.

   Программа проверяет введенные пароли. Если пароли совпадают, программа применяет новый пароль и закрывает окно **Защита паролем**. Если пароли не совпадают, программа предлагает повторно подтвердить пароль в поле **Подтверждение пароля**.

8. Нажмите на кнопку **Сохранить** в окне настройки параметров программы, чтобы сохранить внесенные изменения.

   Откроется окно **Проверка пароля**.

9. В поле **Имя пользователя** введите имя пользователя.

10. В поле **Пароль** введите старый пароль доступа к Kaspersky Endpoint Security.

11. Нажмите на кнопку **ОК**.

Об использовании временного пароля

При работе на клиентских компьютерах, управляемых политикой Kaspersky Security Center, у пользователей может возникнуть необходимость совершить с программой Kaspersky Endpoint Security операции, защищенные паролем на уровне политики. При включенной защите паролем только администратор Kaspersky Security Center может совершать операции, указанные в области действия пароля. Однако если связь с Kaspersky Security Center потеряна (например, пользователь находится вне корпоративной сети), работа с локальным интерфейсом Kaspersky Endpoint Security ограничена.

Чтобы предоставить пользователю возможность совершать необходимые операции, не сообщая пароль, установленный в параметрах политики, администратор Kaspersky Security Center может создать временный пароль. Действие временного пароля ограничено по времени и по области применения. После ввода временного пароля в локальном интерфейсе программы пользователю становятся доступны операции, разрешенные администратором Kaspersky Security Center.

По истечении срока действия временного пароля Kaspersky Endpoint Security продолжает работать согласно параметрам политики Kaspersky Security Center. Операции, защищенные паролем на уровне политики, становятся недоступны пользователю.

Создание временного пароля с помощью Консоли администрирования Kaspersky Security Center

► *Чтобы создать и передать пользователю временный пароль, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева Консоли администрирования откройте папку с названием группы администрирования, к которой принадлежит компьютер пользователя, запросившего временный пароль.
3. В рабочей области выберите закладку **Устройства**.
4. В контекстном меню компьютера пользователя, запросившего временный пароль, выберите пункт **Свойства**.

   Откроется окно **Свойства: <Название компьютера>**.
5. В окне **Свойства: <Название компьютера>** выберите раздел **Программы**.
6. Выберите **Kaspersky Endpoint Security для Windows** и откройте окно со свойствами программы одним из следующих способов:
   - Нажмите на кнопку **Свойства** внизу экрана.
   - Выберите пункт **Свойства** контекстного меню программы.

   Откроется окно **Параметры программы "<Название программы>"**.
7. В окне **Параметры программы "<Название программы>"** в разделе **Общие параметры** выберите подраздел **Интерфейс**.
8. В блоке **Защита паролем** нажмите на кнопку **Настройка**.

   Откроется окно **Защита паролем**.
9. В окне **Защита паролем** в блоке **Временный пароль** нажмите на кнопку **Настройка**.

Кнопка доступна, если в политике Kaspersky Security Center, под которой работает компьютер, включена защита паролем для программы Kaspersky Endpoint Security.

Откроется окно **Создание временного пароля**.

10. В поле **Дата истечения** установите дату, до наступления которой пользователь может применить временный пароль.

    После наступления этой даты временный пароль становится недействительным. Для предоставления доступа к совершению операций в локальном интерфейсе Kaspersky Endpoint Security необходимо создать новый временный пароль.

11. В таблице **Область действия временного пароля** установите флажки напротив тех операций, которые должны быть доступны пользователю на протяжении действия временного пароля.

12. Нажмите на кнопку **Создать**.

    Откроется окно **Временный пароль** с зашифрованным паролем.

13. Скопируйте и передайте пользователю пароль, а также инструкцию по его применению.

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. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 46).
2. В левой части окна в разделе **Общие параметры** выберите подраздел **Управление параметрами**.

   В правой части окна отобразятся функции управления параметрами.

3. В блоке **Управление параметрами** нажмите на кнопку **Сохранить**.

   Откроется стандартное окно Microsoft Windows **Выбор конфигурационного файла**.

4. 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. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 46).
2. В левой части окна в разделе **Общие параметры** выберите подраздел **Управление параметрами**.

   В правой части окна отобразятся функции управления параметрами.
3. В блоке **Управление параметрами** нажмите на кнопку **Загрузить**.

   Откроется стандартное окно Microsoft Windows **Выбор конфигурационного файла**.
4. Укажите путь к конфигурационному файлу.
5. Нажмите на кнопку **Открыть**.

Все значения параметров Kaspersky Endpoint Security будут установлены в соответствии с выбранным конфигурационным файлом.

Управление программой через Kaspersky Security Center

Этот раздел содержит информацию об управлении программой Kaspersky Endpoint Security через Kaspersky Security Center.

В этом разделе

Об управлении программой через 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 задачи обновления и проверки.

В разделе о Контроле программ вы можете найти информацию об управление правилами Контроля программ с помощью Kaspersky Security Center (см. раздел "Управление правилами Контроля программ с помощью Kaspersky Security Center" на стр. 138).

Вы можете найти информацию об управлении программой через Kaspersky Security Center, не указанную в этой справке, в справке для Kaspersky Security Center.

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

Версия плагина управления может отличаться от версии 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.

Особенности работы с плагинами управления разных версий

С помощью плагина управления вы можете изменять следующие элементы:

- политики;
- профили политик;
- групповые задачи;
- локальные задачи;
- локальные параметры программы Kaspersky Endpoint Security.

Для управления программой Kaspersky Endpoint Security через Kaspersky Security Center требуется плагин управления, версия которого равна или выше версии, указанной в информации о совместимости Kaspersky Endpoint Security с плагином управления. Вы можете посмотреть минимальную необходимую версию плагина управления в файле installer.ini, входящем в комплект поставки.

При открытии любого элемента плагин управления проверяет информацию о совместимости. Если версия плагина управления равна или выше версии, указанной в информации о совместимости, то вы можете изменять параметры этого элемента. В противном случае изменение параметров выбранного элемента с помощью плагина управления недоступно. Рекомендуется обновить плагин управления.

Изменение ранее заданных параметров с помощью плагина управления более поздней версии

С помощью плагина управления более поздней версии вы можете изменять все ранее заданные параметры, а также настраивать новые параметры, которых не было в плагине управления версии, используемой вами ранее.

Для новых параметров плагин управления более поздней версии устанавливает значения по умолчанию при первом сохранении политики, профиля политики или задачи.

После того, как вы изменили параметры политики, профиля политики или групповой задачи с помощью плагина управления более поздней версии, эти элементы становятся недоступны для плагина управления предыдущих версий. Локальные параметры программы Kaspersky Endpoint Security и параметры локальных задач по-прежнему доступны для плагина управления предыдущих версий.

Запуск и остановка Kaspersky Endpoint Security на клиентском компьютере

► *Чтобы запустить или остановить программу на клиентском компьютере, 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 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**.

   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 для Windows.
8. Выполните следующие действия:
   - Если вы хотите запустить программу, справа от списка программ "Лаборатории Касперского" нажмите на кнопку  или выполните следующие действия:
     a. Выберите пункт **Свойства** в контекстном меню программы Kaspersky Endpoint Security или нажмите на кнопку **Свойства**, расположенную под списком программ «Лаборатории Касперского».

        Откроется окно **Параметры программы "Kaspersky Endpoint Security для Windows (11.0.0)"**.
     b. В разделе **Общие** нажмите на кнопку **Запустить** в правой части окна.
   - Если вы хотите остановить работу программы, справа от списка программ "Лаборатории Касперского" нажмите на кнопку  или выполните следующие действия:
     a. Выберите пункт **Свойства** в контекстном меню программы Kaspersky Endpoint Security или нажмите на кнопку **Свойства**, расположенную под списком программ «Лаборатории Касперского».

        Откроется окно **Параметры программы "Kaspersky Endpoint Security для Windows (11.0.0)"**.
     b. В разделе **Общие** нажмите на кнопку **Остановить** в правой части окна.

Настройка параметров Kaspersky Endpoint Security

► *Чтобы настроить параметры Kaspersky Endpoint Security, 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 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 для Windows.
8. Выполните одно из следующих действий:
   - В контекстном меню программы Kaspersky Endpoint Security для Windows выберите пункт **Свойства**.
   - 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 *Руководстве администратора 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.

Управление задачами

Этот раздел содержит информацию об управлении задачами для Kaspersky Endpoint Security. Подробнее о концепции управления задачами через Kaspersky Security Center вы можете прочитать в *Руководстве администратора для Kaspersky Security Center*.

В этом разделе

О задачах для Kaspersky Endpoint Security

Kaspersky Security Center управляет работой программ "Лаборатории Касперского", установленных на клиентских компьютерах, с помощью задач. Задачи реализуют основные функции управления, например, добавление ключа, проверку компьютера, обновление антивирусных баз программы.

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, не входящих в группы администрирования.

Задачи для наборов компьютеров, не входящих в группы администрирования, выполняются только для клиентских компьютеров, указанных в параметрах задачи. Если в набор компьютеров, для которого сформирована задача, добавлены новые клиентские компьютеры, то для них эта задача не выполняется. В этом случае требуется создать новую задачу или изменить параметры уже существующей задачи.

Для удаленного управления программой Kaspersky Endpoint Security вы можете работать со следующими задачами любого из перечисленных типов:

- **Добавление ключа**. Kaspersky Endpoint Security добавляет ключ, в том числе дополнительный, для активации программы.
- **Изменение состава компонентов программы**. Kaspersky Endpoint Security устанавливает или удаляет на клиентских компьютерах компоненты согласно списку компонентов, указанному в параметрах задачи.
- **Инвентаризация**. Kaspersky Endpoint Security получает информацию обо всех исполняемых файлах программ, хранящихся на компьютерах.

  Вы можете включить инвентаризацию DLL-модулей и файлов скриптов. В этом случае Kaspersky Security Center будет получать информацию о DLL-модулях, загружаемых на компьютере с установленной программой Kaspersky Endpoint Security, и о файлах, содержащих скрипты.

  Включение инвентаризации DLL-модулей и файлов скриптов значительно увеличивает время выполнения задачи инвентаризации и размер базы данных.

  Если на компьютере с установленной программой Kaspersky Endpoint Security не установлен компонент Контроль программ, то задача инвентаризации на этом компьютере завершится с ошибкой.
- **Обновление**. Kaspersky Endpoint Security обновляет антивирусные базы программы в соответствии с установленными параметрами обновления.
- **Откат обновления**. Kaspersky Endpoint Security откатывает последнее обновление антивирусных баз.
- **Поиск вирусов**. Kaspersky Endpoint Security проверяет на вирусы и другие программы, представляющие угрозу, области компьютера, указанные в параметрах задачи.
- **Проверка доступности KSN**. Kaspersky Endpoint Security отправляет запрос о доступности серверов KSN и обновляет статус подключения KSN.
- **Проверка целостности**. Kaspersky Endpoint Security получает данные о составе модулей программы, установленных на клиентском компьютере, и проверяет цифровую подпись каждого из модулей.
- **Управление учетными записями Агента аутентификации**. В процессе выполнения задачи Kaspersky Endpoint Security создает команды для удаления, добавления или изменения учетных записей Агента аутентификации.

Вы можете выполнять следующие действия над задачами:

- запускать, останавливать, приостанавливать и возобновлять выполнение задач;

- создавать новые задачи;
- изменять параметры задач.

Права на доступ к параметрам задач 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.

Настройка режима работы с задачами

► *Чтобы настроить режим работы с задачами в локальном интерфейсе Kaspersky Endpoint Security, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева Консоли администрирования откройте папку с названием группы администрирования, для которой вы хотите настроить режим работы с задачами в локальном интерфейсе Kaspersky Endpoint Security.
3. В рабочей области выберите закладку **Политики**.
4. Выберите нужную вам политику.
5. Откройте окно **Свойства: <Название политики>** одним из следующих способов:
   - В контекстном меню политики выберите пункт **Свойства**.
   - Перейдите по ссылке **Настроить параметры политики**, которая находится в правой части рабочей области Консоли администрирования.
6. В разделе **Локальные задачи** выберите подраздел **Управление задачами**.
7. В блоке **Управление задачами** выполните следующие действия:
   - Если вы хотите разрешить пользователям работу с локальными задачами в интерфейсе и командной строке Kaspersky Endpoint Security, установите флажок **Разрешить использование локальных задач**.

     Если флажок снят, функционирование локальных задач прекращается. В этом режиме локальные задачи не запускаются по расписанию. Также локальные задачи недоступны для запуска и редактирования в локальном интерфейсе Kaspersky Endpoint Security и при работе с командной строкой.

   - Если вы хотите разрешить пользователям просматривать список групповых задач, установите флажок **Разрешить отображение групповых задач**.
   - Если вы хотите разрешить пользователям изменять параметры групповых задач, установите флажок **Разрешить управление групповыми задачами**.
8. Нажмите на кнопку **OK**, чтобы сохранить внесенные изменения.
9. Примените политику.

   Подробнее о применении политики Kaspersky Security Center вы можете прочитать в *Руководстве администратора для Kaspersky Security Center.*

Создание локальной задачи

► *Чтобы создать локальную задачу, 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 входит нужный вам клиентский компьютер.
3. В рабочей области выберите закладку **Устройства**.
4. Выберите компьютер, для которого вы хотите создать локальную задачу.
5. Выполните одно из следующих действий:
   - В контекстном меню клиентского компьютера выберите пункт **Все задачи** → **Создать задачу**.
   - В контекстном меню клиентского компьютера выберите пункт **Свойства** и в открывшемся окне **Свойства: <Название компьютера>** на закладке **Задачи** нажмите на кнопку **Добавить**.
   - В раскрывающемся списке **Выполнить действие** выберите элемент **Создать задачу**.

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

Создание групповой задачи

► *Чтобы создать групповую задачу, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. Выполните одно из следующих действий:
   - Выберите папку **Управляемые устройства** дерева Консоли администрирования, если вы хотите создать групповую задачу для всех компьютеров, управляемых через программу Kaspersky Security Center.
   - В папке **Управляемые устройства** дерева Консоли администрирования выберите папку с названием группы администрирования, в состав которой входят нужные клиентские компьютеры.
3. В рабочей области выберите закладку **Задачи**.
4. Нажмите на кнопку **Создать задачу**.

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

Создание задачи для выборки устройств

► *Чтобы создать задачу для выборки устройств, выполните следующие действия:*

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

Запустится мастер создания задачи.

4. Следуйте указаниям мастера создания задачи.

Запуск, остановка, приостановка и возобновление выполнения задачи

Если на клиентском компьютере запущена программа (см. раздел "Запуск и остановка Kaspersky Endpoint Security на клиентском компьютере" на стр. 244) Kaspersky Endpoint Security, вы можете запустить / остановить / приостановить / возобновить выполнение задачи на этом клиентском компьютере через Kaspersky Security Center. Если программа Kaspersky Endpoint Security остановлена, выполнение запущенных задач прекращается, а управлять запуском, остановкой, приостановкой и возобновлением задач через Kaspersky Security Center становится невозможным.

► *Чтобы запустить / остановить / приостановить / возобновить выполнение локальной задачи, 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 входит нужный вам клиентский компьютер.
3. В рабочей области выберите закладку **Устройства**.
4. Выберите компьютер, на котором вы хотите запустить / остановить / приостановить / возобновить выполнение локальной задачи.
5. По правой клавише мыши откройте контекстное меню клиентского компьютера и выберите пункт **Свойства**.

   Откроется окно свойств клиентского компьютера.
6. Выберите раздел **Задачи**.

   В правой части окна отобразится список локальных задач.
7. Выберите локальную задачу, выполнение которой вы хотите запустить / остановить / приостановить / возобновить.
8. Выполните необходимое действие с задачей одним из следующих способов:
   - По правой клавише мыши откройте контекстное меню локальной задачи и выберите пункт **Запустить** / **Остановить** / **Приостановить** / **Возобновить**.
   - Нажмите на кнопку  /  справа от списка локальных задач, чтобы запустить или остановить локальную задачу.
   - Выполните следующие действия:
     a. Нажмите на кнопку **Свойства** под списком локальных задач или выберите пункт **Свойства** в контекстном меню задачи.

        Откроется окно **Свойства <Название задачи>**.
     b. На закладке **Общие** нажмите на кнопку **Запустить** / **Остановить** / **Приостановить** / **Возобновить**.

► *Чтобы запустить / остановить / приостановить / возобновить выполнение групповой задачи, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева Консоли администрирования откройте папку с названием группы администрирования, для которой вы хотите запустить / остановить / приостановить / возобновить выполнение групповой задачи.
3. В рабочей области выберите закладку **Задачи**.

   В правой части окна отобразятся групповые задачи.
4. Выберите групповую задачу, выполнение которой вы хотите запустить / остановить / приостановить / возобновить.
5. Выполните необходимое действие с задачей одним из следующих способов:
   - В контекстном меню групповой задачи выберите пункт **Запустить** / **Остановить** / **Приостановить** / **Возобновить**.
   - Нажмите на кнопку / в правой части окна, чтобы запустить или остановить групповую задачу.
   - Выполните следующие действия:
     a. Перейдите по ссылке **Настроить параметры задачи** в правой части рабочей области Консоли администрирования или выберите пункт **Свойства** в контекстном меню задачи.

        Откроется окно **Свойства <Название задачи>**.
     b. На закладке **Общие** нажмите на кнопку **Запустить** / **Остановить** / **Приостановить** / **Возобновить**.

► *Чтобы запустить / остановить / приостановить / возобновить выполнение задачи для выборки компьютеров, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Задачи** дерева Консоли администрирования выберите задачу для выборки компьютеров, выполнение которой вы хотите запустить / остановить / приостановить / возобновить.
3. Выполните одно из следующих действий:
   - В контекстном меню задачи выберите пункт **Запустить** / **Остановить** / **Приостановить** / **Возобновить**.
   - Нажмите на кнопку / в правой части окна, чтобы запустить или остановить задачу для набора компьютеров.
   - Выполните следующие действия:
     a. Перейдите по ссылке **Настроить параметры задачи** в правой части рабочей области Консоли администрирования или выберите пункт **Свойства** в контекстном меню задачи.

        Откроется окно **Свойства <Название задачи>**.
     b. На закладке **Общие** нажмите на кнопку **Запустить** / **Остановить** / **Приостановить** / **Возобновить**.

Изменение параметров задачи

► *Чтобы изменить параметры локальной задачи, 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 входит нужный вам клиентский компьютер.
3. В рабочей области выберите закладку **Устройства**.
4. Выберите компьютер, для которого вы хотите настроить параметры программы.
5. По правой клавише мыши откройте контекстное меню клиентского компьютера и выберите пункт **Свойства**.

   Откроется окно свойств клиентского компьютера.
6. Выберите раздел **Задачи**.

   В правой части окна отобразится список локальных задач.
7. Выберите в списке локальных задач нужную локальную задачу.
8. Нажмите на кнопку **Свойства**.

   Откроется окно **Свойства: <Название локальной задачи>**.
9. В окне **Свойства: <Название локальной задачи>** выберите раздел **Параметры**.
10. Измените параметры локальной задачи.
11. В окне **Свойства: <Название локальной задачи>** нажмите на кнопку **OK**, чтобы сохранить внесенные изменения.
12. В окне **Свойства: <Название компьютера>** нажмите на кнопку **OK**, чтобы сохранить внесенные изменения.

► *Чтобы изменить параметры групповой задачи, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** откройте папку с названием нужной группы администрирования.
3. В рабочей области выберите закладку **Задачи**.

   В рабочей области Консоли администрирования отобразятся групповые задачи.
4. Выберите нужную групповую задачу.
5. По правой клавише мыши откройте контекстное меню групповой задачи и выберите пункт **Свойства**.

   Откроется окно **Свойства: <Название групповой задачи>**.
6. В окне **Свойства: <Название групповой задачи>** выберите раздел **Параметры**.
7. Измените параметры групповой задачи.
8. В окне **Свойства: <Название групповой задачи>** нажмите на кнопку **OK**, чтобы сохранить внесенные изменения.

► *Чтобы изменить параметры задачи для выборки компьютеров, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Задачи** дерева Консоли администрирования выберите задачу для выборки компьютеров, параметры которой вы хотите изменить.
3. По правой клавише мыши откройте контекстное меню задачи для выборки компьютеров и выберите пункт **Свойства**.

   Откроется окно **Свойства: <Название задачи для выборки компьютеров>**.
4. В окне **Свойства: <Название задачи для выборки компьютеров>** выберите раздел **Параметры**.
5. Измените параметры задачи для выборки компьютеров.
6. В окне **Свойства: <Название задачи для выборки компьютеров>** нажмите на кнопку **ОК**, чтобы сохранить внесенные изменения.

Все разделы окна свойств задач, кроме раздела **Параметры**, стандартны для программы Kaspersky Security Center. Их подробное описание вы можете прочитать в *Руководстве администратора для Kaspersky Security Center*. Раздел **Параметры** содержит специфические параметры Kaspersky Endpoint Security для Windows. Его содержимое зависит от выбранной задачи и от ее типа.

Настройка параметров задачи инвентаризации

Вы можете настроить следующие параметры для задачи инвентаризации:

- **Область инвентаризации**. В этом блоке вы можете указать объекты файловой системы, которые будут проверены в ходе инвентаризации. В качестве объектов могут выступать локальные и сетевые папки, съемные и жесткие диски или весь компьютер целиком.
- **Параметры задачи инвентаризации**. В этом блоке вы можете настроить следующие параметры:
  - **Выполнять проверку во время простоя компьютера**. Флажок включает / выключает функцию, которая приостанавливает задачу инвентаризации, если ресурсы компьютера заняты. Kaspersky Endpoint Security приостанавливает задачу инвентаризации, если не включена экранная заставка и разблокирован компьютер.
  - **Инвентаризация модулей DLL-модулей**. Флажок включает / выключает функцию, которая анализирует данные о DLL-модулях и и передает результаты анализа на Сервер администрирования.
  - **Инвентаризация файлов скриптов**. Флажок включает / выключает функцию, которая анализирует данные о файлах, содержащих скрипты, и передает результаты анализа на Сервер администрирования.
  - **Дополнительно**. По этой кнопке открывается окно **Дополнительные параметры**, в котором вы можете настроить следующие параметры:
    - **Проверять только новые и измененные файлы**. Флажок включает / выключает режим проверки только новых файлов и тех файлов, которые изменились после предыдущей инвентаризации.
    - **Пропускать файлы, если их проверка длится более**. Флажок включает / выключает ограничение длительности проверки одного файла. По истечении заданного в поле справа периода времени Kaspersky Endpoint Security прекращает проверку файла.

- **Проверять архивы**. Флажок включает / выключает проверку архивов форматов RAR, ARJ, ZIP, CAB, LHA, JAR, ICE на наличие исполняемых файлов.
- **Проверять дистрибутивы**. Флажок включает / выключает проверку дистрибутивов в процессе выполнения задачи инвентаризации.
- **Не распаковывать составные файлы большого размера**.

  Если флажок установлен, то Kaspersky Endpoint Security не проверяет составные файлы, размеры которых больше заданного в поле **Максимальный размер файла** 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**.

- **Максимальный размер файла**. Kaspersky Endpoint Security не распаковывает только те файлы, размер которых больше указанного в этом поле значения. Значение задается в мегабайтах.

Управление политиками

Этот раздел содержит информацию о создании и настройке политик для Kaspersky Endpoint Security. Более подробную информацию о концепции управления программой Kaspersky Endpoint Security при помощи политик Kaspersky Security Center вы можете прочитать в *Руководстве администратора для Kaspersky Security Center*.

В этом разделе

О политиках

При помощи политик вы можете установить одинаковые значения параметров работы программы Kaspersky Endpoint Security для всех клиентских компьютеров, входящих в состав группы администрирования.

Вы можете локально изменять значения параметров, заданные политикой, для отдельных компьютеров в группе администрирования при помощи Kaspersky Endpoint Security. Вы можете изменять локально только те параметры, изменение которых не запрещено политикой.

Возможность изменять параметры программы на клиентском компьютере определяется статусом относящегося к этим параметрам «замка» в свойствах политики:

- Закрытый "замок" () означает следующее:
  - Kaspersky Security Center накладывает запрет на изменение параметров, к которым относится этот замок, из интерфейса Kaspersky Endpoint Security на клиентских компьютерах. На всех клиентских компьютерах Kaspersky Endpoint Security использует одинаковые значения этих параметров – те, которые заданы в свойствах политики.
  - Kaspersky Security Center накладывает запрет на изменение параметров, к которым относится этот замок, в свойствах тех политик для вложенных групп администрирования и подчиненных Серверов администрирования, в которых включена функция **Наследовать параметры политики верхнего уровня**. Используются те значения этих параметров, которые заданы в свойствах политики верхнего уровня иерархии.
- Открытый "замок" () означает следующее:
  - Kaspersky Security Center снимает запрет на изменение параметров, к которым относится этот замок, из интерфейса Kaspersky Endpoint Security на клиентских компьютерах. На каждом клиентском компьютере Kaspersky Endpoint Security работает согласно локальному значению этих параметров, если компонент включен.
  - Kaspersky Security Center снимает запрет на изменение параметров, к которым относится этот замок, в свойствах тех политик для вложенных групп администрирования и подчиненных Серверов администрирования, в которых включена функция **Наследовать параметры политики верхнего уровня**. Значения этих параметров не зависят от того, что указано в свойствах политики верхнего уровня иерархии.

Локальные параметры программы изменяются в соответствии с параметрами политики после первого применения 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.

Выделены следующие функциональные области Kaspersky Endpoint Security:

- Базовая защита. Функциональная область включает компоненты Защита от файловых угроз, Защита от почтовых угроз, Защита от веб-угроз, Защита от сетевых угроз, Сетевой экран, задачи проверки.
- Контроль программ. Функциональная область включает компонент Контроль программ.
- Доверенная зона. Функциональная область включает Доверенную зону.
- Веб-Контроль. Функциональная область включает компонент Веб-Контроль.
- Продвинутая защита. Функциональная область включает параметры KSN, компоненты Анализ поведения, Защита от эксплойтов, Предотвращение вторжений, Откат вредоносных действий.
- Базовая функциональность. Функциональная область включает общие параметры программы, не указанные в других функциональных областях, в том числе: лицензирование, задачи инвентаризации и обновления антивирусных баз программы, самозащита, дополнительные параметры программы, отчеты и хранилища, параметры защиты паролем и интерфейса программы.

Вы можете выполнять следующие действия над политикой:

- Создавать политику.
- Изменять параметры политики.

  Если учетная запись пользователя, под которой вы осуществили доступ к Серверу администрирования, не имеет прав на изменение параметров отдельных функциональных областей, то параметры этих функциональных областей недоступны для изменения.

- Удалять политику.
- Изменять состояние политики.

Информацию о работе с политиками, не касающуюся взаимодействия с Kaspersky Endpoint Security, вы можете прочитать в *Руководстве администратора для Kaspersky Security Center*.

Создание политики

► *Чтобы создать политику, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. Выполните одно из следующих действий:
   - Выберите папку **Управляемые устройства** дерева Консоли администрирования, если вы хотите создать политику для всех управляемых программой Kaspersky Security Center компьютеров.
   - 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. Выполните одно из следующих действий:
   - Нажмите на кнопку **Создать политику**.
   - По правой клавише мыши откройте контекстное меню и выберите пункт **Создать → Политику**.

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

Изменение параметров политики

► *Чтобы изменить параметры политики, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева Консоли администрирования откройте папку с названием нужной группы администрирования, для которой вы хотите изменить параметры политики.
3. В рабочей области выберите закладку **Политики**.

4. Выберите нужную политику.
5. Откройте окно **Свойства: <Название политики>** одним из следующих способов:
   - В контекстном меню политики выберите пункт **Свойства**.
   - Перейдите по ссылке **Настроить параметры политики**, которая находится в правой части рабочей области Консоли администрирования.

   Параметры политики для Kaspersky Endpoint Security для Windows включают в себя параметры компонентов и параметры программы (см. раздел "Настройка параметров Kaspersky Endpoint Security" на стр. 245). В разделах **Продвинутая защита**, **Базовая защита** и **Контроль безопасности** окна **Свойства: <Название политики>** представлены параметры компонентов защиты и контроля, в разделе **Шифрование данных** представлены параметры полнодискового шифрования, шифрования файлов, шифрования съемных дисков, в разделе **Endpoint Sensor** приведены параметры компонента Endpoint Sensor, в разделе **Локальные задачи** приведены параметры локальных и групповых задач, а в разделе **Общие параметры** представлены параметры программы.

   Параметры шифрования данных и компонентов контроля в параметрах политики отображаются, если установлены соответствующий флажки в окне Kaspersky Security Center **Настройка интерфейса**. По умолчанию эти флажки установлены.
6. Измените параметры политики.
7. В окне **Свойства: <Название политики>** нажмите на кнопку **OK**, чтобы сохранить внесенные изменения.

Индикатор уровня защиты в окне свойств политики

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 **Подробнее**, по которой открывается окно **Рекомендованные компоненты защиты**. В этом окне вы можете включить любой из рекомендованных компонентов защиты.

Настройка отображения интерфейса программы

► *Чтобы настроить отображение интерфейса программы, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева Консоли администрирования откройте папку с названием группы администрирования, для которой вы хотите настроить отображение интерфейса программы.
3. В рабочей области выберите закладку **Политики**.
4. Выберите нужную политику.
5. Откройте окно **Свойства: <Название политики>** одним из следующих способов:
   - В контекстном меню политики выберите пункт **Свойства**.
   - Перейдите по ссылке **Настроить параметры политики**, которая находится в правой части рабочей области Консоли администрирования.
6. В разделе **Общие параметры** выберите подраздел **Интерфейс**.
7. 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 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.
8. 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. 47).

   Флажок доступен, если установлен флажок **Отображать интерфейс программы**.

Отправка сообщений пользователей на сервер Kaspersky Security Center

У пользователя может возникнуть необходимость отправить сообщение администратору локальной сети

организации в следующих случаях:

- Контроль программ запретил запуск программы.

  Шаблон сообщения с запросом разрешения на запуск заблокированной программы доступен в интерфейсе Kaspersky Endpoint Security в разделе Контроль программ (см. стр. 135).

- Веб-Контроль заблокировал доступ к веб-ресурсу.

  Шаблон сообщения с запросом доступа к заблокированному веб-ресурсу доступен в интерфейсе Kaspersky Endpoint Security в разделе Веб-Контроль (см. раздел "Изменение шаблонов сообщений Веб-Контроля" на стр. 170).

Способ отправки сообщений, а также выбор используемого шаблона зависит от наличия или отсутствия на компьютере с установленной программой Kaspersky Endpoint Security действующей политики Kaspersky Security Center и связи с Сервером администрирования Kaspersky Security Center. Возможны следующие сценарии:

- Если на компьютере с установленной программой Kaspersky Endpoint Security не действует политика Kaspersky Security Center, то сообщение пользователя отправляется администратору локальной сети организации по электронной почте.

  Для заполнения полей сообщения используются значения полей из шаблона, заданного в локальном интерфейсе Kaspersky Endpoint Security.

- Если на компьютере с установленной программой Kaspersky Endpoint Security действует политика Kaspersky Security Center, то Kaspersky Endpoint Security отправляет стандартное сообщение на Сервер администрирования Kaspersky Security Center.

  В этом случае сообщения пользователей доступны для просмотра в хранилище событий Kaspersky Security Center (см. раздел "Просмотр сообщений пользователей в хранилище событий Kaspersky Security Center" на стр. 259). Для заполнения полей сообщения используются значения полей из шаблона, заданного в политике Kaspersky Security Center.

- Если на компьютере с установленной программой Kaspersky Endpoint Security действует политика для автономных пользователей Kaspersky Security Center, то способ отправки сообщения зависит от наличия связи с Kaspersky Security Center:

  - Если связь с Kaspersky Security Center установлена, то Kaspersky Endpoint Security отправляет стандартное сообщение на Сервер администрирования Kaspersky Security Center.
  - Если связь с Kaspersky Security Center отсутствует, то сообщение пользователя отправляется администратору локальной сети организации по электронной почте.

  Для заполнения полей сообщения в обоих случаях используются значения полей из шаблона, заданного в политике Kaspersky Security Center.

Просмотр сообщений пользователей в хранилище событий Kaspersky Security Center

Компоненты Контроль программ (см. раздел "Изменение шаблонов сообщений Контроля программ" на стр. 135) и Веб-Контроль (см. раздел "Изменение шаблонов сообщений Веб-Контроля" на стр. 170) предоставляют пользователям локальной сети организации, на компьютерах которых установлена программа Kaspersky Endpoint Security, возможность отправлять сообщения администратору.

Возможны два способа доставки сообщения администратору от пользователя:

- В виде события в хранилище событий Kaspersky Security Center.

  Событие пользователя передается в хранилище событий Kaspersky Security Center, если программа Kaspersky Endpoint Security, установленная на компьютере пользователя, работает под активной политикой.

- В виде сообщения электронной почты.

  Информация пользователя передается в виде сообщения электронной почты, если к компьютеру с установленной программой Kaspersky Endpoint Security применена политика или политика для автономных пользователей.

► *Чтобы просмотреть сообщение пользователя в хранилище событий Kaspersky Security Center, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В узле **Сервер администрирования** дерева Консоли администрирования выберите закладку **События**.

   В рабочей области Kaspersky Security Center отображаются все события, произошедшие во время работы программы Kaspersky Endpoint Security, в том числе и сообщения администратору, приходящие от пользователей локальной сети организации.
3. Чтобы настроить фильтр событий, в раскрывающемся списке **События выборки** выберите элемент **Запросы пользователей**.
4. Выберите сообщение администратору.
5. Откройте окно **Параметры события** одним из следующих способов:
   - По правой клавише мыши откройте контекстное меню события и выберите пункт **Свойства**.
   - Нажмите на кнопку **Открыть окно свойств события** в правой части рабочей области Консоли администрирования.

Работа с программой из командной строки

Этот раздел содержит описание работы с Kaspersky Endpoint Security из командной строки.

В этом разделе

Команды

Для работы с программой из командной строки доступны следующие команды:

Таблица 3. Команды для работы с программой

Команды	Действие
HELP	показать справку
SCAN	запустить задачу антивирусной проверки
UPDATE	обновить антивирусные базы программы
ROLLBACK	выполнить откат последнего обновления антивирусных баз
TRACES	включить / выключить трассировку
START	запустить задачу
STOP	остановить выполняемую задачу
STATUS	показать статус задачи
STATISTICS	показать статистику выполнения задачи
RESTORE	восстановить файл из карантина
EXPORT	экспортировать параметры программы
IMPORT	импортировать параметры программы
ADDKEY	добавить ключ
LICENSE	выполнить операции с лицензией

Команды	Действие
PBATESTRESET	удалить информацию о совместимости системного жесткого диска и Агента аутентификации (более подробную информацию можно найти в *Руководстве администратора*)
EXIT	завершить работу программы
EXITPOLICY /password=<password>	выключить политику Kaspersky Security Center (операция защищена паролем)
STARTPOLICY	включить политику Kaspersky Security Center, которая была выключена с помощью команды EXITPOLICY
RENEW	открыть веб-страницу покупки лицензий в браузере
CLS	очистить экран консоли
MESSAGES <on|off>	включить или выключить интерактивный режим

Команда SCAN

```
Применение:
SCAN [<files>] [/ALL][/MEMORY][/STARTUP][/MAIL][/REMDRIVES]
[/FIXDRIVES][/NETDRIVES][/QUARANTINE] [/@:<filelist.lst>]
[/i<0-4>] [-e:a|s|b|<filemask>|<seconds>]
[/R[A]:<report_file>] [/C:<settings_file>]
SCAN /VLNS2 [/WUA][/WSUSCAB <wsus_file>] [<files>] [/lst <filelist.lst>]
```

Сканирование на уязвимости:

- /VLNS2 - сканировать на уязвимости;
- /WUA - сканировать с помощью WUA (отключено по умолчанию);
- /WSUSCAB <wsus_file> - указать WSUS файл.

Область проверки:

- <files> - список файлов и папок через пробелы (длинные пути должны быть заключены в кавычки);
- /ALL - проверять компьютер;
- /MEMORY - проверять память компьютера;
- /STARTUP - проверять объекты автозапуска;
- /MAIL - проверять почтовые ящики;
- /REMDRIVES - проверять съемные диски;
- /FIXDRIVES - проверять жесткие диски;
- /NETDRIVES - проверять сетевые диски;
- /QUARANTINE - проверять файлы на карантине;
- /@:<filelist.lst> - проверять файлы, перечисленные в заданном списке.

Действия над обнаруженными объектами:

- `/i0` - уведомлять;
- `/i1` - лечить и пропускать, если лечение невозможно;
- `/i2` - лечить и удалять, если лечение невозможно (при этом программа не удаляет файлы из контейнеров, но удаляет контейнеры с исполняемым расширением);
- `/i3` - лечить и удалять, если лечение невозможно (при этом программа удаляет контейнеры, если удаление объекта из контейнера невозможно);
- `/i4` - удалять (в том числе удалять контейнеры, если удаление объекта из контейнера невозможно);
- `/i8` (по умолчанию) - спрашивать пользователя немедленно;
- `/i9` - спрашивать пользователя после завершения задачи.

Режим проверки:

- `/fe` - быстрый (по расширению);
- `/fi` - интеллектуальный (по формату);
- `/fa` (по умолчанию) - полный (проверяются все файлы).

Исключения:

- `-e:a` - пропускать архивы;
- `-e:b` - пропускать почтовые базы и текст сообщений электронной почты;
- `-e:<filemask>` - пропускать файлы по маске;
- `-e:<seconds>` - пропускать файлы, проверяемые дольше указанного количества <секунд>;
- `-es:<size>` - пропускать файлы размером более указанного количества <мегабайт>.

Отчеты:

- `/R:<report_file>` - сохранять в отчет только критические события;
- `/RA:<report_file>` - сохранять в отчет все события.

Дополнительные параметры:

- `/iChecker=<on|off>` - включить или выключить технологию iChecker;
- `/iSwift=<on|off>` - включить или выключить технологию iSwift;
- `/C:<settings_file>` - указать конфигурационный файл.

Примеры:

- `avp.com SCAN /R:log.txt /MEMORY /STARTUP /MAIL "C:\Documents and Settings\All Users\My Documents" "C:\Program Files" C:\Downloads\test.exe`
- `avp.com SCAN /MEMORY /@:objects2scan.txt /C:scan_settings.txt /RA:scan.log`
- `avp.com SCAN /VLNS2`
- `avp.com SCAN /VLNS2 /RA:scan.log /WUA C:\Windows\`

Команда UPDATE

Применение:

```
UPDATE [source] [/R[A]:<report_file>] [/C:<settings_file>]
```

Параметры:

- `source` - веб-адрес или путь к локальной папке источника обновлений;
- `/R:<report_file>` - сохранять в отчет только критические события;
- `/RA:<report_file>` - сохранять в отчет все события;
- `/C:<settings_file>` - указать конфигурационный файл.

Примеры:

```
avp.com UPDATE "ftp://my_server/kav updates" /RA:avbases_upd.txt
```

Команда ROLLBACK

Применение:

```
ROLLBACK /login=<login> /password=<password> [/R[A]:<report_file>]
```

Параметры:

- `/R:<report_file>` - сохранять в отчет только критические события;
- `/RA:<report_file>` - сохранять в отчет все события.

Примеры:

```
avp.com ROLLBACK /RA:rollback.txt
```

Команда TRACES

Применение:

```
TRACES on/off [<trace_level>] [all|dbg|file]
```

Параметры:

- `on` - включить трассировку;
- `off` - выключить трассировку;
- `<trace_level>` - уровень детализации трассировки (доступные значения: 100, 200, 300, 400, 500, 600);
- `all` - использовать функцию `OutputDebugString` и сохранять файл трассировки;
- `dbg` - использовать функцию `OutputDebugString` для вывода файла трассировки;
- `file` - сохранять файл трассировки.

Примеры:

- `avp.com TRACES on 500`

- `avp.com TRACES on 500 dbg`
- `avp.com TRACES off`
- `avp.com TRACES 500`
- `avp.com TRACES off file`

Команда START

Применение:

```
START <Profile> [/R[A]:<report_file>]
```

Параметры:

- `<Profile>` - название профиля;
- `/R:<report_file>` - сохранять в отчет только критические события;
- `/RA:<report_file>` - сохранять в отчет все события.

Доступные профили:

- ApsStorageTask;
- DeviceControl;
- EntAppControl;
- File_Monitoring (FM);
- Group_Scan;
- HipsTask (HIPS);
- IM_Monitoring (IM);
- Mail_Monitoring (EM);
- Rollback;
- RollbackPatch;
- Scan_IdleScan;
- Scan_My_Computer;
- Scan_Objects;
- Scan_Qscan;
- Scan_Quarantine;
- Scan_Startup (STARTUP);
- SW2;
- Updater;
- VulnsScan2 (VA);
- VulnsScan2rt (VART);
- Web_Monitoring (WM);

- WebControl.

Примеры:

```
avp.com START Scan_Objects
```

Команда STOP

Применение:

```
STOP <Profile> /login=<login> /password=<password>
```

Параметр `<Profile>` - название профиля.

Получение списка доступных профилей: avp.com HELP STOP

Доступные профили:

- ApsStorageTask;
- DeviceControl;
- EntAppControl;
- File_Monitoring (FM);
- Group_Scan;
- HipsTask (HIPS);
- IM_Monitoring (IM);
- Mail_Monitoring (EM);
- Rollback;
- RollbackPatch;
- Scan_IdleScan;
- Scan_My_Computer;
- Scan_Objects;
- Scan_Qscan;
- Scan_Quarantine;
- Scan_Startup (STARTUP);
- SW2;
- Updater;
- VulnsScan2 (VA);
- VulnsScan2rt (VART);
- Web_Monitoring (WM);
- WebControl.

Команда STATUS

Применение:

`STATUS [Profile]`

Доступные профили:

- AdvDis;
- AntiBanner;
- AntiPhishingEx;
- AppActivityMonitorService;
- AppStartLog;
- ApsStorageTask;
- AVService;
- AVZ_PrivacyCleaner;
- AVZ_RunScript;
- AVZ_Scan_Vulnerabilities;
- AVZ_SecurityTweaker;
- Avz_Troubleshoot;
- CFDeterministicAntiMalware;
- CfPragueAdapter;
- CfResponseProvider;
- Controls;
- CustomUrlProcess;
- DeterministicAntiPhishing;
- DeviceControl;
- DeviceControlService;
- EntAppControl;
- EntAppControlActive;
- EntAppControllerService;
- EntAppControlService;
- EnterpriseApplicationCategorizer;
- EnterpriseApplicationFileInfoProvider;
- File_Monitoring (FM);
- FinanceUrlCategorizer;
- FTP;
- Group_Scan;
- HeuristicAntiPhishing;
- Hips;

- HipsRequester;
- HipsTask (HIPS);
- HTTP;
- httpscan (HTTP);
- ICQ;
- IM_Monitoring (IM);
- IMAP;
- IntegrityControl;
- Inventory_Scan;
- IRC;
- Jabber;
- KSN;
- LocalizationManager;
- Mail_Monitoring (EM);
- MMP;
- MSN;
- NetWatch;
- NNTP;
- POP3;
- ProcessMonitorStatistics;
- ProcMon;
- Protection (RTP);
- QB;
- Rollback;
- RollbackPatch;
- Scan_IdleScan;
- Scan_My_Computer;
- Scan_Objects;
- Scan_Qscan;
- Scan_Quarantine;
- Scan_Startup (STARTUP);
- SMTP;
- SW2;
- SW2U;
- ThreatsDisinfector;

- TimeControl;
- TrafficMonitor;
- UDS;
- Updater;
- VerCheck;
- VulnerabilityStorage;
- VulnsScan2 (VA);
- VulnsScan2rt (VART);
- Web_Monitoring (WM);
- WebContentCategorizer;
- WebControl;
- WebControlTestAccessService;
- WebControlUrlNormalizerService;
- WebNetStat;
- YHO.

Команда STATISTICS

Применение:

```
STATISTICS <Profile>
```

Доступные профили:

- ApsStorageTask;
- DeviceControl;
- EntAppControl;
- File_Monitoring (FM);
- Group_Scan;
- HipsTask (HIPS);
- IM_Monitoring (IM);
- Mail_Monitoring (EM);
- Rollback;
- RollbackPatch;
- Scan_IdleScan;
- Scan_My_Computer;
- Scan_Objects;
- Scan_Qscan;
- Scan_Quarantine;

- Scan_Startup (STARTUP);
- SW2;
- Updater;
- VulnsScan2 (VA);
- VulnsScan2rt (VART);
- Web_Monitoring (WM);
- WebControl.

Команда RESTORE

Применение:

```
RESTORE [/REPLACE] <filename>
```

Параметры:

- `/REPLACE` - переписать существующий файл;
- `<filename>` - имя восстанавливаемого файла.

Примеры:

```
avp.com RESTORE /REPLACE C:\eicar.com
```

Команда EXPORT

Применение:

```
EXPORT <Profile> <filename>
```

Параметры:

- `<Profile>` - название профиля, параметры которого должны быть экспортированы;
- `<filename>` - имя файла, в который должны быть экспортированы параметры.

  Используйте расширение txt для файлов в текстовом формате.

Примеры:

- `avp.com EXPORT rtp rtp_settings.dat - binary export`
- `avp.com EXPORT fm fm_settings.txt - plain export`

Доступные профили:

- ApsStorageTask;
- DeviceControl;
- EntAppControl;
- File_Monitoring (FM);
- Group_Scan;
- HipsTask (HIPS);

- IM_Monitoring (IM);
- Mail_Monitoring (EM);
- Rollback;
- RollbackPatch;
- Scan_IdleScan;
- Scan_My_Computer;
- Scan_Objects;
- Scan_Qscan;
- Scan_Quarantine;
- Scan_Startup (STARTUP);
- SW2;
- Updater;
- VulnsScan2 (VA);
- VulnsScan2rt (VART);
- Web_Monitoring (WM);
- WebControl.

Команда IMPORT

Применение:

```
IMPORT <filename> /login=<login> /password=<password>
```

Параметры:

`<filename>` - файл, в который должны быть импортированы параметры (поддерживаются только бинарные файлы).

Примеры:

```
avp.com IMPORT settings.dat
```

Команда ADDKEY

Применение:

```
ADDKEY <filename> [/login=<login> /password=<password>]
```

Параметры:

`<filename>` - имя файла ключа.

Примеры:

```
avp.com ADDKEY 00000000.key
```

Команда LICENSE

Применение:

```
LICENSE <command> [/login=<login> /password=<password>]
```

Параметры:

- `command` - команда, которую требуется выполнить;
- `/ADD <filename>` - добавить ключ;
- `/ADD <activation code>` - активировать программу с помощью кода активации;
- `/DEL` - удалить ключ.

Примеры:

- `avp.com LICENSE /ADD 00000000.key`
- `avp.com LICENSE /ADD AAAAA-BBBBB-CCCCC-DDDDD`
- `avp.com LICENSE /DEL /login=login /password=password`

Команда EXIT

Применение:

```
EXIT /login=<login> /password=<password>
```

Примеры:

```
avp.com EXIT /login=login /password=password
```

Команда EXITPOLICY

Применение:

```
EXITPOLICY /password=<password>
```

Примеры:

```
avp.com EXITPOLICY /login=login /password=password
```

Команда STARTPOLICY

Применение:

```
STARTPOLICY /password=<password>
```

Примеры:

```
avp.com STARTPOLICY /password=password
```

Сообщения об ошибках

При работе с программой возможно появление следующих сообщений об ошибках:

Таблица 4. Сообщения об ошибках и коды возврата

Сообщение об ошибке в командной строке	Код возврата в Shell

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)	
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

Сообщение об ошибке в командной строке	Код возврата в Shell
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	
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>	

Сообщение об ошибке в командной строке	Код возврата в Shell
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	
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
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

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 5. Символьные и числовые значения кодов возврата

Символьные значения	Числовые значения	Доступно для команд

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

Символьные значения	Числовые значения	Доступно для команд
[1-127]	[1-127]	LICENSE: /Check /Add (ActivateByCode) /Add (ActivateByKeyEx) /AddTicket
errACCESS_DENIED	8000045	STOP EXITPOLICY
SHELL_RET_FAILED	2	START STOP STATUS STATISTICS MODE HELP EXPORT IMPORT EXIT ADDKEY INETSWIFT EXITPOLICY STARTPOLICY UPDATE ROLLBACK RENEW TRACE\TRACES SPYWARE MESSAGES RESTORE PBATESTRESET SCAN
-SHELL_RET_FAILED	-2	LICENSE: /Add (ActivateByKeyEx) /AddTicket

Символьные значения	Числовые значения	Доступно для команд
SHELL_RET_NO_LICENCE	2	START UPDATE ROLLBACK SCAN
SHELL_RET_OK	0	START STOP STATUS STATISTICS HELP EXPORT IMPORT EXIT ADDKEY INETSWIFT EXITPOLICY STARTPOLICY UPDATE ROLLBACK RENEW TRACE\TRACES SLC SPYWARE LETSDUMP MESSAGES RESTORE PBATESTRESET 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 TRACE\TRACES SPYWARE RESTORE 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.

Обращение в Службу технической поддержки

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

В этом разделе

Способы получения технической поддержки

Если вы не нашли решения вашей проблемы в документации 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.

Перед обращением 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).

Получение информации для Службы технической поддержки

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.

Перечисленные выше действия должны выполняться только под руководством специалистов Службы технической поддержки по полученным от них инструкциям. Самостоятельное изменение параметров работы программы способами, не описанными в Руководстве администратора или в рекомендациях специалистов Службы технической поддержки, может привести к замедлению и сбоям в работе операционной системы, снижению уровня защиты компьютера, а также к нарушению доступности и целостности обрабатываемой информации.

В этом разделе

Создание файла трассировки

► *Чтобы создать файл трассировки, выполните следующие действия:*

1. Откройте главное окно программы (на стр. 43).
2. В главном окне программы нажмите на кнопку **Поддержка**.

   Откроется окно **Поддержка**.
3. В окне **Поддержка** нажмите на кнопку **Трассировка системы**.

   Откроется окно **Информация для поддержки**.
4. Чтобы запустить процесс трассировки, выберите один из следующих элементов в раскрывающемся списке **Трассировка**:
   - **Включена**.

     Выберите этот элемент, чтобы включить трассировку.
   - **С ротацией**.

     Выберите этот элемент, чтобы включить трассировку и ограничить максимальное количество

файлов трассировки и максимальный размер каждого из файлов трассировки. Если записано максимальное количество файлов трассировки максимального размера, то удаляется наиболее старый файл трассировки и начинается запись нового файла трассировки.

Если выбран этот элемент, вы можете указать значение для следующих полей:

- **Максимальное количество файлов для ротации**.

  В этом поле вы можете указать максимальное количество записываемых файлов трассировки.

- **Максимальный размер каждого файла**.

  В этом поле вы можете указать максимальный размер каждого из записываемых файлов трассировки.

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. Воспроизведите ситуацию, в которой у вас возникает проблема.

7. Чтобы остановить процесс трассировки, вернитесь в окно **Информация для поддержки** и выберите **Выключена** в раскрывающемся списке **Трассировка**.

После создания файла трассировки вы можете перейти к загрузке результатов трассировки на сервер "Лаборатории Касперского".

О составе и хранении файлов трассировки

Пользователь сам несет 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 хранятся в папке ProgramData\Kaspersky Lab.

Файлы трассировки имеют название `KES<номер версии_dateXX.XX_timeXX.XX_pidXXX.><тип файла трассировки>.log`.

Файл трассировки Агента аутентификации хранится в папке System Volume Information и имеет название `KLFDE.{EB2A5993-DFC8-41a1-B050-F0824113A33A}.PBELOG.bin`.

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.

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.
- Имя пользователя и пароль, если они передавались в открытом виде. Эти данные могут записываться в файлы трассировки при проверке интернет-трафика. Трафик записывается в файлы трассировки только из trafmon2.ppl.
- Имя пользователя и пароль, 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.

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 плагинов программы

Файлы трассировки плагинов программы, помимо общих данных, содержат следующую информацию:

- Файл трассировки плагина запуска задачи проверки из контекстного меню shellex.dll.log содержит информацию о выполнении задачи проверки и данные, необходимые для устранения неполадок в работе плагина.
- Файлы трассировки плагина компонента Защита от почтовых угроз mcou.OUTLOOK.EXE может содержать части сообщений электронной почты, в том числе адреса электронной почты.

Содержание файла трассировки Агента аутентификации

Файл трассировки Агента аутентификации, помимо общих данных, содержит информацию о работе Агента аутентификации и действиях, которые выполняет пользователь в Агенте аутентификации.

О составе и хранении файлов дампов

Пользователь сам несет ответственность за обеспечение безопасности полученной информации и, в частности, за контроль и ограничение доступа к полученной информации, хранимой на компьютере.

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.

Файл дампа содержит всю информацию о рабочей памяти процессов Kaspersky Endpoint Security на момент создания этого файла дампа. В том числе файл дампа может содержать персональные данные.

Включение и выключение записи дампов

► *Чтобы включить или выключить запись дампов, выполните следующие действия:*

1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 46).
2. В левой части выберите подраздел **Параметры программы** в разделе **Общие параметры**.

   В правой части окна отобразятся параметры программы.
3. В блоке **Отладочная информация** нажмите на кнопку **Настройка**.

   Откроется окно **Отладочная информация**.
4. Выполните одно из следующих действий:
   - Установите флажок **Включить запись дампов**, если вы хотите чтобы программа записывала дампы программы.
   - Снимите флажок **Включить запись дампов**, если вы не хотите чтобы программа записывала дампы программы.
5. Нажмите на кнопку **ОК** в окне **Отладочная информация**.
6. Нажмите на кнопку **Сохранить** в главном окне программы, чтобы сохранить внесенные изменения.

Включение и выключение защиты 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. 287). 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. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 46).
2. В левой части выберите подраздел **Параметры программы** в разделе **Общие параметры**.

   В правой части окна отобразятся параметры программы.
3. В блоке **Отладочная информация** нажмите на кнопку **Настройка**.

   Откроется окно **Отладочная информация**.
4. Выполните одно из следующих действий:
   - Установите флажок **Включить защиту файлов дампов и файлов трассировки**, если вы хотите включить защиту.
   - Снимите флажок **Включить защиту файлов дампов и файлов трассировки**, если вы хотите выключить защиту.
5. Нажмите на кнопку **ОК** в окне **Отладочная информация**.
6. Нажмите на кнопку **Сохранить** в главном окне программы, чтобы сохранить внесенные изменения.

Файлы дампов и файлы трассировки, записанные при включенной защите, остаются защищенными после отключения этой функции.

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.

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

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 идентифицировать ключ сертификата. Отпечаток создаётся путём применения криптографической хеш-функции к значению ключа.

П

Параметры задачи

Параметры работы программы, специфичные для каждого типа задач.

Параметры программы

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

Патч (от англ. patch – заплатка)

Небольшое дополнение к программе, которое устраняет недостатки, обнаруженные в процессе работы с программой, или устанавливает обновления.

Портативный файловый менеджер

Программа, предоставляющая интерфейс для работы с зашифрованными файлами на съемных дисках при отсутствии на компьютере функциональности шифрования.

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.

АО "Лаборатория Касперского"

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

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

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

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

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

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

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

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

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

Сайт "Лаборатории Касперского": https://www.kaspersky.ru

Вирусная энциклопедия:	https://securelist.ru/
Вирусная лаборатория:	https://virusdesk.kaspersky.ru/ (для проверки подозрительных файлов и сайтов)
Веб-форум "Лаборатории Касперского":	https://forum.kaspersky.com

Информация о стороннем коде

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

Приложение. 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 6. 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	**Включить Kaspersky Security Network**	Флажок снят. Допускается устанавливать флажок только при использовании Локального KSN (KPSN).
Контроль безопасности — Контроль программ	**Включить Контроль программ**	Флажок установлен.
Общие параметры — Параметры программы	**Запускать Kaspersky Endpoint Security для Windows при включении компьютера**	Флажок установлен.
Общие параметры — Параметры программы	**Применять технологию лечения активного заражения**	Флажок установлен.
Общие параметры — Исключения — Объекты для обнаружения	**Вирусы, черви; Троянские программы; Вредоносные утилиты; Упакованные файлы, которые могут нанести вред; Многократно упакованные файлы**	Флажок установлен.
Общие параметры — Исключения	**Исключения из проверки и доверенная зона**	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.

Сущность, к которой относится параметр	Название параметра	Безопасное значение или диапазон значений параметра (сертифицированная конфигурация)
Базовая защита — Защита от файловых угроз	**Включить Защиту от файловых угроз**	Флажок установлен.
Базовая защита — Защита от файловых угроз	**Уровень безопасности**	**Рекомендуемый** или **Высокий** (необходимо настроить некоторые параметры в соответствии с настоящей таблицей).
Базовая защита — Защита от файловых угроз (настройка) — Общие	**Типы файлов**	Все файлы.
Базовая защита — Защита от файловых угроз (настройка) — Общие	**Область защиты**	Список областей не меньше, чем заданный по умолчанию.
Базовая защита — Защита от файловых угроз (настройка) — Производительность	**Эвристический анализ**	Флажок установлен.
Базовая защита — Защита от файловых угроз (настройка) — Производительность	**Проверять архивы**	Флажок установлен.
Базовая защита — Защита от файловых угроз	**Действие при обнаружении угрозы**	Выбран вариант **Лечить, удалять, если лечение невозможно**
Базовая защита — Защита от веб-угроз	**Включить Защиту от веб-угроз**	Флажок установлен.
Базовая защита — Защита от веб-угроз	**Уровень безопасности**	**Рекомендуемый** или **Высокий** (необходимо настроить некоторые параметры в соответствии с настоящей таблицей).
Базовая защита — Защита от веб-угроз	**Действие при обнаружении угрозы**	Выбран вариант **Запрещать загрузку**
Базовая защита — Защита от почтовых угроз	**Включить Защиту от почтовых угроз**	Флажок установлен.
Базовая защита — Защита от почтовых угроз	**Уровень безопасности**	**Рекомендуемый** или **Высокий** (необходимо настроить некоторые параметры в соответствии с настоящей таблицей).

Сущность, к которой относится параметр	Название параметра	Безопасное значение или диапазон значений параметра (сертифицированная конфигурация)
Базовая защита — Защита от почтовых угроз	**Действие при обнаружении угрозы**	Выбран вариант **Лечить, удалять, если лечение невозможно**
Продвинутая защита — Откат вредоносных действий	**Включить Откат вредоносных действий**	Флажок установлен.
Базовая защита — Защита от сетевых угроз	**Включить Защиту от сетевых угроз**	Флажок установлен.
Базовая защита — Защита от сетевых угроз	**Добавить атакующий компьютер в список блокирования на <N> минут**	Флажок установлен. 60 минут - рекомендуемое время блокирования.
Базовая защита — Защита от сетевых угроз	**Исключения**	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.
Задачи — Обновление	**Загружать обновления модулей программы**	Флажок снят.
Общие параметры — Параметры программы	**Включить самозащиту**	Флажок установлен.
Общие параметры — Параметры программы	**Выключить внешнее управление системными службами**	Флажок установлен.
Общие параметры — Интерфейс — Защита паролем (настройка)	**Включить защиту паролем**	Флажок установлен. Администратор безопасности должен установить надежный пароль и область действия (все опции).