KASPERSKY

Kaspersky Endpoint Security 10 для Windows

Руководство администратора

Версия программы: 10 Service Pack 2

Содержание

Contents

О Kaspersky Endpoint Security для Windows

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

В этом разделе

Что нового

В Kaspersky Endpoint Security для Windows появились следующие возможности и улучшения:

1. Контроль запуска программ:
    - поддержка серверных операционных систем;
    - контроль загрузки DLL-модулей и драйверов;
    - управление списком объектов в задаче инвентаризации (DLL-модули, файлы скриптов);
    - контроль объектов по новому критерию - по атрибутам сертификатов цифровой подписи;
    - создание отчета по тестовым запускам запрещенных программ;

- поддержка двух режимов работы Контроля запуска программ: "черный список" и "белый список";
- использование SHA256-хеша для контроля и инвентаризации объектов;
- контроль запуска скриптов из интерпретатора PowerShell;
- использование доверенного системного хранилища сертификатов.

2. Управление Microsoft BitLocker - шифрованием жестких дисков с помощью технологии BitLocker от компании Microsoft:
   - удаленное управление шифрованием;
   - мониторинг зашифрованных устройств;
   - создание отчетов шифрования устройств;
   - восстановление доступа к зашифрованным устройствам.
3. Шифрование диска Kaspersky:
   - поддержка ввода учетных данных в предзагрузочной среде Агента аутентификации с помощью виртуальной клавиатуры;
   - режим шифрования только занятого пространства на устройстве;
   - поддержка шифрования на планшетах (MS Surface версий 3 и 4).
4. Контроль активности программ:
   - контроль доступа программ к устройствам аудио- и видеозаписи.
5. Веб-Контроль:
   - настройка правил доступа к веб-ресурсам для дополнительных категорий веб-ресурсов.
6. Контроль устройств:
   - запись в журнал событий, связанных с удалением и сохранением файлов на USB-устройствах;

- формирование списка доверенных сетей Wi-Fi по следующим параметрам: имя, тип шифрования и тип аутентификации;
- управление правами доступа пользователей к операциям чтения и записи файлов на CD/DVD-дисках.

7. Почтовый Антивирус:
   - возможность удалять и переименовывать файлы указанных типов, находящиеся внутри архивов.
8. Kaspersky Security Network:
   - отображение KSN в качестве причины, по которой принято решение о способе обработки объекта, в отчетах Kaspersky Endpoint Security и Kaspersky Security Center;
   - отправление запроса в KSN о репутации выбранного файла;
   - отображение статуса доступности серверов KSN для клиентских компьютеров с установленной программой Kaspersky Endpoint Security.

Комплект поставки

Комплект поставки Kaspersky Endpoint Security содержит следующие файлы:

- файлы, необходимые для установки программы (см. раздел "О способах установки программы" на стр. 27) всеми доступными способами;
- файлы пакетов обновлений, которые используются при установке программы;
- файл klcfginst.msi для установки плагина управления Kaspersky Endpoint Security через Kaspersky Security Center;
- файл ksn_<ID языка>.txt, с помощью которого вы можете ознакомиться с условиями участия в Kaspersky Security Network (см. раздел "Участие в Kaspersky Security Network" на стр. 544);

- файл license.txt, с помощью которого вы можете ознакомиться с Лицензионным соглашением (см. раздел "О Лицензионном соглашении" на стр. 71);
- файл incompatible.txt со списком несовместимого программного обеспечения;
- файл installer.ini, содержащий внутренние параметры дистрибутива.

> Не рекомендуется изменять значения этих параметров. Если вы хотите изменить параметры установки, используйте файл setup.ini (см. раздел "Описание параметров установки в файле setup.ini" на стр. 42).

Для получения доступа к файлам требуется распаковать дистрибутив.

Организация защиты компьютера

Kaspersky Endpoint Security обеспечивает комплексную защиту компьютера от различного вида угроз, сетевых и мошеннических атак.

Каждый тип угроз обрабатывается отдельным компонентом. Компоненты можно включать и выключать независимо друг от друга, а также настраивать параметры их работы.

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

Чтобы поддерживать Kaspersky Endpoint Security в актуальном состоянии, требуется *обновление* баз и модулей программы, используемых в работе программы. По умолчанию программа обновляется автоматически, но при необходимости вы можете вручную обновить базы и модули программы.

К компонентам контроля относятся следующие компоненты программы:

- **Контроль запуска программ**. Компонент отслеживает попытки запуска программ пользователями и регулирует запуск программ.

- **Предотвращение вторжений**. Компонент регистрирует действия, совершаемые программами в операционной системе, и регулирует деятельность программ исходя из того, к какой группе компонент относит эту программу. Для каждой группы программ задан набор правил. Эти правила регламентируют доступ программ к персональным данным пользователя и ресурсам операционной системы. К таким данным относятся файлы пользователя (папка "Мои документы", файлы cookie, данные об активности пользователя), а также файлы, папки и ключи реестра, содержащие параметры работы и важные данные наиболее часто используемых программ.

- **Контроль устройств**. Компонент позволяет установить гибкие ограничения доступа к устройствам, являющимся источниками информации (например, жесткие диски, съемные диски, ленточные накопители, CD/DVD-диски), инструментами передачи информации (например, модемы), инструментами превращения информации в твердую копию (например, принтеры) или интерфейсами, с помощью которых устройства подключаются к компьютеру (например, USB, Bluetooth, Infrared).

- **Веб-Контроль**. Компонент позволяет установить гибкие ограничения доступа к веб-ресурсам для разных групп пользователей.

Работа компонентов контроля основана на правилах:

- Предотвращение вторжений использует правила контроля программ (см. раздел "О правилах Контроля запуска программ" на стр. 183).

- Контроль активности программ использует правила контроля программ (см. раздел "Работа с правилами контроля программ" на стр. 218).

- Контроль устройств использует правила доступа к устройствам и правила доступа к шинам подключения (см. раздел "О правилах доступа к устройствам и шинам подключения" на стр. 238).

- Веб-Контроль использует правила доступа к веб-ресурсам (см. раздел "О правилах доступа к веб-ресурсам" на стр. 275).

К компонентам защиты относятся следующие компоненты программы:

- **Файловый Антивирус**. Компонент позволяет избежать заражения файловой системы компьютера. Компонент запускается при старте Kaspersky Endpoint Security,

постоянно находится в оперативной памяти компьютера и проверяет все открываемые, сохраняемые и запускаемые файлы на компьютере и на всех присоединенных дисках. Файловый Антивирус перехватывает каждое обращение к файлу и проверяет этот файл на присутствие вирусов и других программ, представляющих угрозу.

- **Мониторинг системы**. Компонент получает данные о действиях программ на компьютере и предоставляет эту информацию другим компонентам для более эффективной защиты компьютера.

- **Почтовый Антивирус**. Компонент проверяет входящие и исходящие сообщения электронной почты на наличие в них вирусов и других программ, представляющих угрозу.

- **Веб-Антивирус**. Компонент проверяет трафик, поступающий на компьютер пользователя по протоколам HTTP и FTP, а также устанавливает принадлежность ссылок к вредоносным или фишинговым веб-адресам.

- **Сетевой экран**. Компонент обеспечивает защиту данных, хранящихся на компьютере пользователя, блокируя большинство возможных для операционной системы угроз в то время, когда компьютер подключен к интернету или к локальной сети. Компонент фильтрует всю сетевую активность согласно правилам двух типов: сетевым правилам программ и сетевым пакетным правилам (см. раздел "О сетевых правилах" на стр. 143).

- **Мониторинг сети**. Компонент предназначен для просмотра в режиме реального времени информации о сетевой активности компьютера.

- **Защита от сетевых атак**. Компонент 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.

В программе Kaspersky Endpoint Security предусмотрены следующие задачи:

- **Полная проверка**. Kaspersky Endpoint Security выполняет проверку операционной системы, включая системную память, загружаемые при старте объекты, резервное хранилище операционной системы, а также все жесткие и съемные диски.

- **Выборочная проверка**. Kaspersky Endpoint Security проверяет объекты, выбранные пользователем.

- **Проверка важных областей**. Kaspersky Endpoint Security проверяет объекты, загрузка которых осуществляется при старте операционной системы, системную память и объекты заражения руткитами.

- **Обновление**. Kaspersky Endpoint Security загружает обновленные базы и модули программы. Это обеспечивает актуальность защиты компьютера от вирусов и других программ, представляющих угрозу.

Функциональность шифрования файлов позволяет шифровать файлы и папки, хранящиеся на локальных дисках компьютера. Функциональность шифрования дисков позволяет шифровать жесткие диски и съемные диски.

Удаленное управление через Kaspersky Security Center

Программа Kaspersky Security Center позволяет удаленно запускать и останавливать Kaspersky Endpoint Security на клиентском компьютере, управлять задачами и настраивать параметры работы программы.

Служебные функции программы

Kaspersky Endpoint Security включает ряд служебных функций. Служебные функции предусмотрены для поддержки программы в актуальном состоянии, расширения возможностей использования программы, для оказания помощи в работе.

- **Отчеты**. В процессе работы программы для каждого компонента и задачи программы формируется отчет. Отчет содержит список событий, произошедших во время работы Kaspersky Endpoint Security, и всех выполненных программой операций. В случае возникновения проблем отчеты можно отправлять в "Лабораторию Касперского", чтобы специалисты Службы технической поддержки могли подробнее изучить ситуацию.

- **Хранилище данных**. Если в ходе проверки компьютера на вирусы и другие программы, представляющие угрозу, программа обнаруживает зараженные файлы, она блокирует эти файлы. Копии вылеченных и удаленных файлов Kaspersky Endpoint Security сохраняет в *Резервном хранилище*. Файлы, которые не были обработаны по каким-либо причинам, Kaspersky Endpoint Security помещает в *список*

необработанных файлов. Вы можете проверять файлы, восстанавливать файлы в папку их исходного размещения, а также очищать хранилище данных.

- **Служба уведомлений**. Служба уведомлений позволяет пользователю быть в курсе событий о текущем состоянии защиты компьютера и о работе Kaspersky Endpoint Security. Уведомления могут доставляться на экран или по электронной почте.

- **Kaspersky Security Network**. Участие пользователя в Kaspersky Security Network позволяет повысить эффективность защиты компьютера за счет оперативного получения информации о репутации файлов, веб-ресурсов и программного обеспечения, полученной от пользователей во всем мире.

- **Лицензия**. Приобретение лицензии обеспечивает полнофункциональную работу программы, доступ к обновлению баз и модулей программы, а также консультации по телефону и электронной почте по вопросам, связанным с установкой, настройкой и использованием программы.

- **Поддержка**. Все зарегистрированные пользователи Kaspersky Endpoint Security могут обращаться за помощью к специалистам Службы технической поддержки. Вы можете отправить запрос из Персонального кабинета на веб-сайте Службы технической поддержки или получить консультацию наших сотрудников по телефону.

Если во время работы программы возникают ошибки или "зависания", программа может быть автоматически перезапущена.

Если в работе программы возникают повторяющиеся ошибки, которые приводят к прекращению работы, программа выполняет следующие действия:

1. Выключает функции контроля и защиты (функция шифрования продолжает работать).

2. Уведомляет пользователя о выключении функций.

3. После обновления антивирусных баз или применения обновлений модулей программы пытается восстановить работоспособность.

Программа получает сведения о повторяющихся ошибках и зависаниях с помощью специальных алгоритмов, определяемых специалистами "Лаборатории Касперского".

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 баз и модулей 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/kes10wks http://support.kaspersky.ru/kes10wks.

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/kes10fs http://support.kaspersky.ru/kes10fs.

Установка и удаление программы

Этот раздел содержит информацию о том, как установить Kaspersky Endpoint Security на компьютер, как выполнить первоначальную настройку программы, как обновить предыдущую версию программы, а также о том, как удалить программу с компьютера.

В этом разделе

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. 35).

  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.exe, входящий в комплект поставки (на стр. 18).

   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 (см. раздел "Аппаратные и программные требования" на стр. 24);
- выполнение аппаратных и программных требований (см. раздел "Аппаратные и программные требования" на стр. 24);
- 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 10 Service Pack 2 для Windows, а предыдущая версия программы автоматически удаляется. Это относится к следующим версиям программы:

- Антивирус Касперского 6.0 для Windows Workstations MP4 CF1 / MP4 CF2;
- Антивирус Касперского 6.0 для Windows Servers MP4 / MP4 CF2;
- Kaspersky Endpoint Security 10 Service Pack 1 для Windows;
- Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 1 для Windows;
- Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 2 для Windows;
- Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 3 для Windows.

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

На этом шаге следует ознакомиться с Лицензионным соглашением, которое заключается между вами и "Лабораторией Касперского".

Внимательно прочитайте Лицензионное соглашение и, если вы согласны со всеми его пунктами, установите флажок **Я принимаю условия Лицензионного соглашения**.

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 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 компоненты защиты и компонент Контроль активности программ с параметрами, рекомендуемыми специалистами "Лаборатории Касперского".

- **Стандартная установка**. Если вы выбираете этот тип установки, на компьютер пользователя устанавливаются компоненты защиты и компоненты контроля с параметрами, рекомендуемыми специалистами "Лаборатории Касперского".

- **Выборочная установка**. Если вы выбираете этот тип установки, вам предлагается выбрать компоненты для установки (см. раздел "Шаг 5. Выбор компонентов

программы для установки" на стр. 31) и указать папку, в которую будет установлена программа (см. раздел "Шаг 6. Выбор папки для установки программы" на стр. 33).

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. Файловый Антивирус является обязательным компонентом для установки. Вы не можете отменить его установку.

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

- Защита от атак BadUSB (на стр. 173).
- Шифрование дисков (см. раздел "Шифрование съемных дисков" на стр. 323).
- Шифрование файлов (см. раздел "Шифрование файлов на локальных дисках компьютера" на стр. 310).
- Управление Microsoft BitLocker (см. раздел "Шифрование жестких дисков с помощью технологии Шифрование диска BitLocker" на стр. 341).
- KATA Endpoint Sensor (на стр. 294).

Управление Microsoft BitLocker выполняет следующие функции:

- управление встроенным в операционную систему Windows шифрованием BitLocker;
- настройка параметров политики шифрования 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.

KATA 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 антивирусной проверки

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

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

Флажок **Исключить из антивирусной проверки области, рекомендованные компанией Microsoft** / **Исключить из антивирусной 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 антивирусной 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. 46).

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 /pKSN=1|0 /pINSTALLLEVEL=<значение> /pALLOWREBOOT=1|0 /pSKIPPRODUCTCHECK=1|0 /pSKIPPRODUCTUNINSTALL=1|0 /s`

или

`msiexec /i <название установочного пакета> EULA=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 (см. раздел "Комплект поставки" на стр. 18). 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.

- `KSN=1|0` означает согласие (1) или отказ (0) участвовать в программе Kaspersky Security Network (далее также "KSN"). Текст Положения об участии в KSN входит в комплект поставки Kaspersky Endpoint Security (см. раздел "Комплект поставки" на стр. 18). 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.

- `INSTALLLEVEL=<значение>` указывает на тип установки Kaspersky Endpoint Security (см. раздел "Шаг 4. Выбор типа установки" на стр. 30). 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 KATA 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`, по умолчанию Kaspersky Endpoint Security проводит проверку и выводит на экран список обнаруженных несовместимых программ.

- `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 /pKSN=1|0 /pINSTALLLEVEL=<значение> /pKLLOGIN=<Имя пользователя> /pKLPASSWD=***** /pKLPASSWDAREA=<область действия пароля> /s
  ```

  или

  ```
  msiexec /i <название дистрибутива> EULA=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. 42), содержащего общие параметры установки программы;
- конфигурационного файла install.cfg (см. раздел "Создание и использование конфигурационного файла" на стр. 484), 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.
   - `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.
   - `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 (см. раздел "Аппаратные и программные требования" на стр. 24).

  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.

- `MailAntiVirus` - установка компонента Почтовый Антивирус.
- `WebAntiVirus` - установка компонента Веб-Антивирус.
- `ApplicationPrivilegeControl` - установка компонента Контроль активности программ.
- `SystemWatcher` - установка компонента Мониторинг системы.
- `Firewall` - установка компонента Сетевой экран.
- `NetworkAttackBlocker` - установка компонента Защита от сетевых атак.
- `WebControl` - установка компонента Веб-Контроль.
- `DeviceControl` - установка компонента Контроль устройств.
- `ApplicationStartupControl` - установка компонента Контроль запуска программ.
- `FileEncryption` - установка библиотек для шифрования файлов и папок.
- `DiskEncryption` - установка библиотек для шифрования дисков.
- `KeyboardAuthorization` - установка компонента Защита от атак BadUSB.
- `AntiAPT` - установка компонента KATA 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.

Файловый Антивирус 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

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 один из следующих вариантов активации Kaspersky Endpoint Security:

- **Активировать с помощью кода активации**. Выберите этот вариант и введите код активации (см. раздел "О коде активации" на стр. 74), если вы хотите активировать программу с помощью кода активации.
- **Активировать с помощью файла ключа**. Выберите этот вариант, если вы хотите активировать программу с помощью файла ключа.
- **Активировать пробную версию**. Выберите этот вариант, если вы хотите активировать пробную версию программы. Пользователь может использовать полнофункциональную версию программы в течение срока действия, ограниченного лицензией на пробную версию программы. По истечении срока действия лицензии функциональность программы блокируется, повторная активация пробной версии программы недоступна.
- **Активировать позже**. Выберите этот вариант, если вы хотите пропустить этап активации Kaspersky Endpoint Security. Пользователь сможет работать только с компонентами Файловый Антивирус и Сетевой экран. Пользователь сможет обновить базы и модули Kaspersky Endpoint Security только один раз после установки программы. Вариант **Активировать позже** доступен только при первом запуске мастера первоначальной настройки программы, сразу после установки программы.

Для активации пробной версии программы или для активации программы с помощью кода активации требуется подключение компьютера к интернету.

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

Активация с помощью кода активации

Этот шаг доступен только при активации программы с помощью кода активации. Если вы проводите активацию пробной версии программы или если вы проводите активацию программы с помощью файла ключа, то этот шаг пропускается.

На этом шаге Kaspersky Endpoint Security отправляет данные на сервер активации, чтобы проверить введенный код активации:

- Если код активации успешно проходит проверку, мастер первоначальной настройки программы автоматически переходит к следующему окну.
- Если код активации не проходит проверку, на экране появляется соответствующее уведомление. В этом случае вам следует обратиться за информацией в компанию, где вы приобрели лицензию на Kaspersky Endpoint Security.
- Если число активаций с помощью кода активации превышено, на экране появляется соответствующее уведомление. Работа мастера первоначальной настройки программы прерывается, и программа предлагает вам обратиться в Службу технической поддержки "Лаборатории Касперского".

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

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**.

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 Контроль активности программ.
- **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**.

См. также

Организация защиты компьютера 19

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**.

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**.

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**.

Соглашение об участии в Kaspersky Security Network

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

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 участия в 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 участия в 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 10 Service Pack 2 для Windows требуется расшифровать все зашифрованные жесткие диски.

Вы можете обновить до версии Kaspersky Endpoint Security 10 Service Pack 2 для Windows следующие программы:

- Антивирус Касперского 6.0 для Windows Workstations MP4 CF1 (сборка 6.0.4.1424) / MP4 CF2 (сборка 6.0.4.1611).
- Антивирус Касперского 6.0 для Windows Servers MP4 (сборка 6.0.4.1424) / MP4 CF2 (сборка 6.0.4.1611).
- 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).

При обновлении любой из перечисленных выше программ до Kaspersky Endpoint Security 10 Service Pack 2 для Windows содержимое Резервного хранилища не переносится.

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. 35);
- удаленно с помощью программного комплекса Kaspersky Security Center (см. *Руководстве по внедрению 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 10 Service Pack 2 для Windows не нужно удалять предыдущую версию программы. Перед началом обновления предыдущей версии программы рекомендуется закрыть все работающие программы.

Удаление программы

Этот раздел содержит информацию о том, как удалить Kaspersky Endpoint Security с компьютера.

В этом разделе

О способах удаления программы

В результате удаления Kaspersky Endpoint Security компьютер и данные пользователя окажутся незащищенными.

Программа Kaspersky Endpoint Security может быть удалена с компьютера несколькими способами:

- локально в интерактивном режиме с помощью мастера установки программы (см. раздел "Удаление программы с помощью мастера установки программы" на стр. 56);
- локально в тихом режиме из командной строки (см. раздел "Удаление программы из командной строки" на стр. 58);
- удаленно с помощью программного комплекса Kaspersky Security Center (информация приведена в *Руководстве по внедрению Kaspersky Security Center*);
- удаленно через редактор управления групповыми политиками Microsoft Windows (см. сопроводительную документацию для операционной системы).

Удаление программы с помощью мастера установки программы

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

1. Откройте окно **ПАНЕЛЬ УПРАВЛЕНИЯ** одним из следующих способов:

   - Если вы используете Windows 7, то в меню **Пуск** выберите пункт **Панель управления**.
   - Если вы используете Windows 8 или Windows 8.1, то нажмите сочетание клавиш **WIN+I** и выберите пункт **Панель управления**.
   - Если вы используете Windows 10, то нажмите сочетание клавиш **WIN+X** и выберите пункт **Панель управления**.

2. В окне **Панель управления** выберите пункт **Программы и Компоненты**.
3. В списке установленных программ выберите элемент **Kaspersky Endpoint Security для Windows**.
4. Нажмите на кнопку **Удалить/Изменить**.

   Откроется окно **Выборочная установка** мастера установки программы.
5. В окне мастера установки программы **Изменение, восстановление или удаление программы** нажмите на кнопку **Удаление**.
6. Следуйте указаниям мастера установки программы.

В этом разделе

Шаг 1. Сохранение данных программы для повторного использования

На этом шаге вы можете указать, какие используемые программой данные вы хотите сохранить для дальнейшего использования при повторной установке программы (например, ее более новой версии). Если вы не укажете никаких данных, программа будет удалена полностью.

Чтобы сохранить данные программы для повторного использования,

установите флажки напротив тех данных, которые нужно сохранить:

- **Информация об активации** - данные, позволяющие в дальнейшем не активировать устанавливаемую программу, а автоматически использовать ее по действующей лицензии, если срок ее действия не истек к моменту установки.
- **Файлы резервного хранилища** - файлы, проверенные программой и помещенные в резервное хранилище.

  > Доступ к файлам резервного хранилища, сохраненным после удаления программы, возможен только из той же версии программы, в которой они были сохранены.
  >
  > Если вы планируете использовать объекты резервного хранилища после удаления программы, вам нужно восстановить их из хранилищ до удаления программы. Однако эксперты "Лаборатории Касперского" не рекомендуют восстанавливать объекты из резервного хранилища, так как это может нанести вред компьютеру.

- **Параметры работы программы** - значения параметров работы программы, установленные в процессе ее настройки.
- **Локальное хранилище ключей шифрования** - данные, которые обеспечивают прямой доступ к зашифрованным до удаления программы файлам и устройствам. После повторной установки программы с доступной функциональностью шифрования данных доступ к зашифрованным файлам и устройствам осуществляется напрямую.

Этот флажок установлен по умолчанию.

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

Шаг 2. Подтверждение удаления программы

Поскольку удаление программы ставит под угрозу защиту компьютера, требуется подтвердить ваше намерение удалить программу. Для этого нажмите на кнопку **Удалить**.

До завершения удаления программы вы в любой момент можете отменить это действие, нажав на кнопку **Отмена**.

Шаг 3. Удаление программы. Завершение удаления

На этом шаге мастер установки программы удаляет программу с компьютера пользователя. Дождитесь завершения удаления программы.

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

Удаление программы из командной строки

Вы можете запустить удаление программы из командной строки. Удаление производится в интерактивном или в тихом режиме (без запуска мастера установки программы).

Чтобы запустить удаление программы в интерактивном режиме,

в командной строке введите `setup.exe /x` или `msiexec.exe /x {7911E943-32CC-45D0-A29C-56E6EF762275}`.

Запустится мастер установки программы. Следуйте указаниям мастера установки программы (см. раздел "Удаление программы с помощью мастера установки программы" на стр. 56).

Чтобы запустить удаление программы в тихом режиме,

в командной строке введите `setup.exe /s /x` или `msiexec.exe /x {7911E943-32CC-45D0-A29C-56E6EF762275} /qn`.

Начнется удаление программы в тихом режиме (без запуска мастера установки).

Если операция удаления программы защищена паролем, в командной строке нужно указать имя пользователя и соответствующий ему пароль.

Чтобы удалить программу из командной строки при установленных имени пользователя и пароле, требуемых для подтверждения права на удаление / изменение / восстановление Kaspersky Endpoint Security, в интерактивном режиме,

в командной строке введите `setup.exe /pKLLOGIN=<Имя пользователя> /pKLPASSWD=***** /x` или

`msiexec.exe KLLOGIN=<Имя пользователя> KLPASSWD=***** /x {7911E943-32CC-45D0-A29C-56E6EF762275}`.

Запустится мастер установки программы. Следуйте указаниям мастера установки программы (см. раздел "Удаление программы с помощью мастера установки программы" на стр. 56).

Чтобы удалить программу из командной строки при установленных имени пользователя и пароле, требуемых для подтверждения права на удаление / изменение / восстановление Kaspersky Endpoint Security, в тихом режиме,

в командной строке введите `setup.exe /pKLLOGIN=<Имя пользователя> /pKLPASSWD=***** /s /x` или

`msiexec.exe /x {7911E943-32CC-45D0-A29C-56E6EF762275} KLLOGIN=<Имя пользователя> KLPASSWD=***** /qn`.

Удаление объектов и данных, оставшихся после тестовой работы Агента аутентификации

Если в процессе удаления программы Kaspersky Endpoint Security обнаруживает объекты и данные, оставшиеся на системном жестком диске после тестовой работы Агента аутентификации, то удаление программы прерывается и становится невозможным до тех пор, пока эти объекты и данные не будут удалены.

Объекты и данные могут остаться на системном жестком диске после тестовой работы Агента аутентификации только в исключительных ситуациях. Например, если после применения политики Kaspersky Security Center с установленными параметрами шифрования компьютер не перезагружался или после тестовой работы Агента аутентификации программа не запускается.

Вы можете удалить объекты и данные, оставшиеся на системном жестком диске после тестовой работы Агента аутентификации, двумя способами:

- с помощью политики Kaspersky Security Center;
- с помощью утилиты восстановления.

Чтобы удалить объекты и данные, оставшиеся после тестовой работы Агента аутентификации, с помощью политики Kaspersky Security Center, выполните следующие действия:

1. Примените к компьютеру политику Kaspersky Security Center с установленными параметрами для расшифровки (см. раздел "Расшифровка жестких дисков" на стр. 346) всех жестких дисков компьютера.
2. Запустите Kaspersky Endpoint Security.

Чтобы удалить объекты и данные, оставшиеся после тестовой работы Агента аутентификации, с помощью утилиты восстановления, выполните следующие действия:

1. На компьютере с подключенным системным жестким диском, на котором остались объекты и данные после тестовой работы Агента аутентификации, запустите исполняемый файл утилиты восстановления fdert.exe, созданный с помощью

программы Kaspersky Endpoint Security (см. раздел "Создание исполняемого файла утилиты восстановления" на стр. 384).

2. В окне утилиты восстановления в раскрывающемся списке **Выберите устройство** выберите системный жесткий диск, на котором хранятся объекты и данные для удаления.

3. Нажмите на кнопку **Диагностировать**.

4. Нажмите на кнопку **Удалить объекты и данные АА**.

Запустится процесс удаления объектов и данных, оставшихся после тестовой работы Агента аутентификации.

После удаления объектов и данных, оставшихся после тестовой работы Агента аутентификации, дополнительно может потребоваться удаление данных о несовместимости программы с Агентом аутентификации.

Чтобы удалить данные о несовместимости программы с Агентом аутентификации,

в командной строке введите команду `avp pbatestreset`.

Для выполнения команды `avp pbatestreset` требуются установленные компоненты шифрования.

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 Файловый Антивирус, 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 закладку **Центр управления** главного окна программы. С помощью закладки **Центр управления** вы можете регулировать работу компонентов и задач программы, просматривать статистику об обработанных файлах и найденных угрозах.

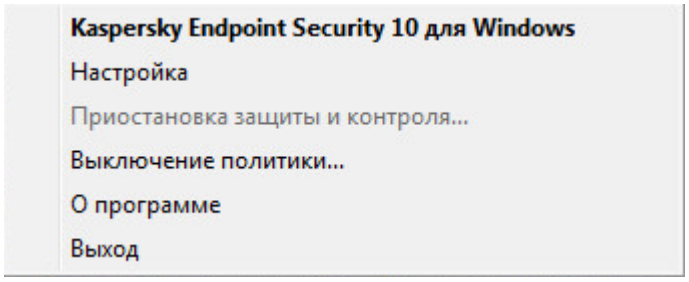
- **Настройка**. Открывает закладку **Настройка** главного окна программы. С помощью закладки **Настройка** вы можете изменить параметры программы, установленные по умолчанию.

- **Приостановка защиты и контроля** / **Возобновление защиты и контроля**. Временно выключает / включает 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.

- **Выключение политики** / **Включение политики**. Выключает / включает политику Kaspersky Security Center. Этот пункт контекстного меню доступен, если Kaspersky Endpoint Security работает под политикой 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

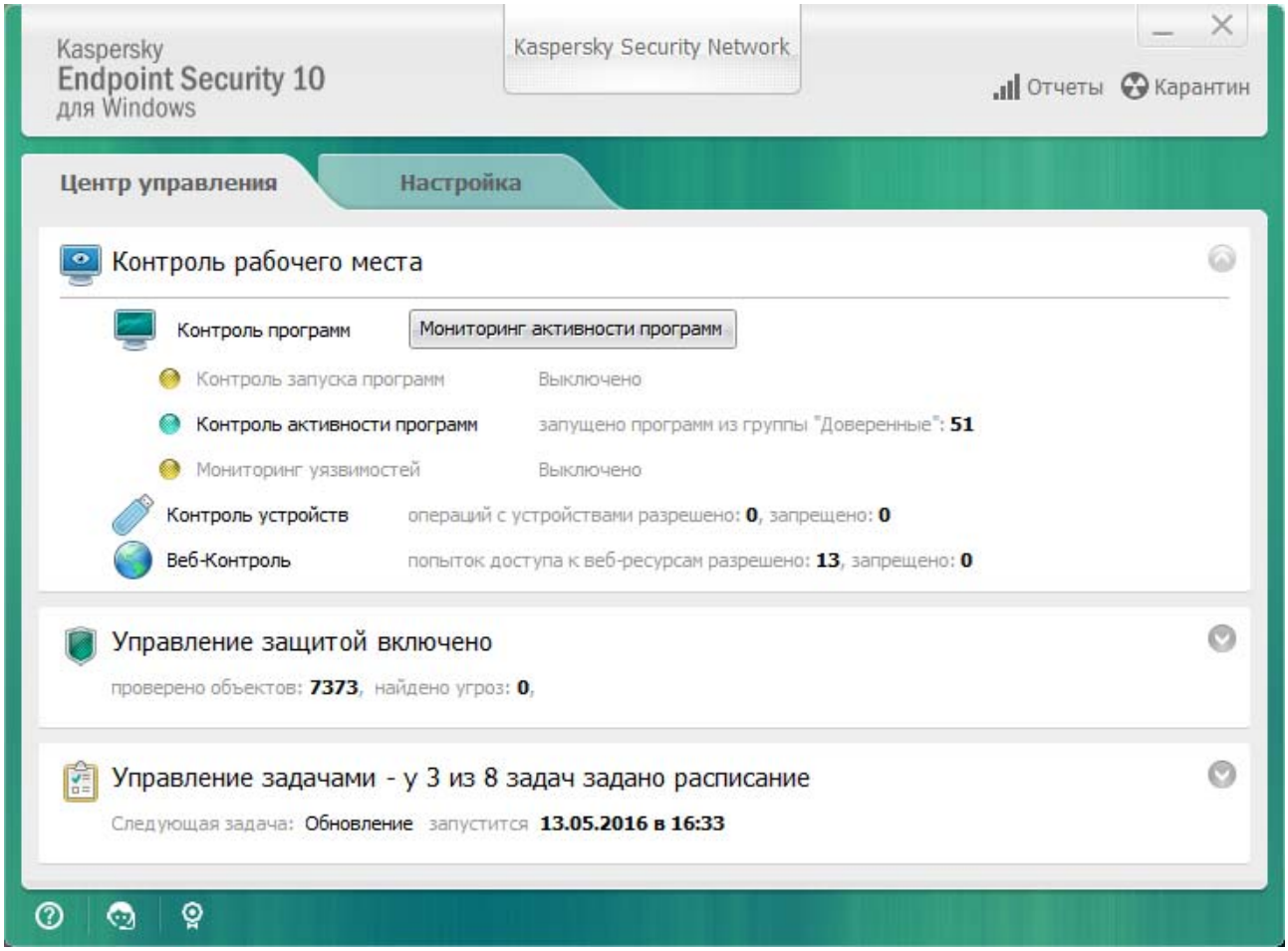
В главном окне Kaspersky Endpoint Security находятся элементы интерфейса, предоставляющие вам доступ к основным функциям программы.

Главное окно программы можно условно разделить на четыре части (см. рис. ниже):

- Верхняя часть окна с элементами интерфейса, с помощью которых вы можете просмотреть следующую информацию:
  - сведения о программе;
  - статистику Kaspersky Security Network;
  - список необработанных файлов;
  - хранилище копий зараженных файлов, которые были удалены в ходе работы программы;
  - отчеты о событиях, произошедших в ходе работы программы в целом, работы отдельных компонентов и выполнения задач.
- Закладка **Центр управления**, с помощью которой вы можете регулировать работу компонентов программы и выполнение задач. Когда вы открываете главное окно программы, в нем отображается закладка **Центр управления**.

- Закладка **Настройка**, с помощью которой вы можете изменять параметры программы, установленные по умолчанию.
- Нижняя часть окна, которая содержит следующие элементы:
  - **Кнопка**  . При нажатии на кнопку осуществляется переход к справочной системе Kaspersky Endpoint Security.
  - **Кнопка**  . 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**  /  . При нажатии на кнопку открывается окно **Лицензирование** с информацией о действующей лицензии.
  - **Кнопка**  /  /  . При нажатии на кнопку открывается окно **События** с информацией о доступных обновлениях, а также с запросами доступа к зашифрованным файлам и устройствам.

Кнопка доступна только при наличии запросов или неустановленных обновлений.



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. 63).

Закладка настройки параметров программы

Закладка настройки параметров Kaspersky Endpoint Security предназначена для настройки параметров работы программы в целом, отдельных ее компонентов, отчетов и хранилищ,

задач проверки и задачи обновления, а также для настройки 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.

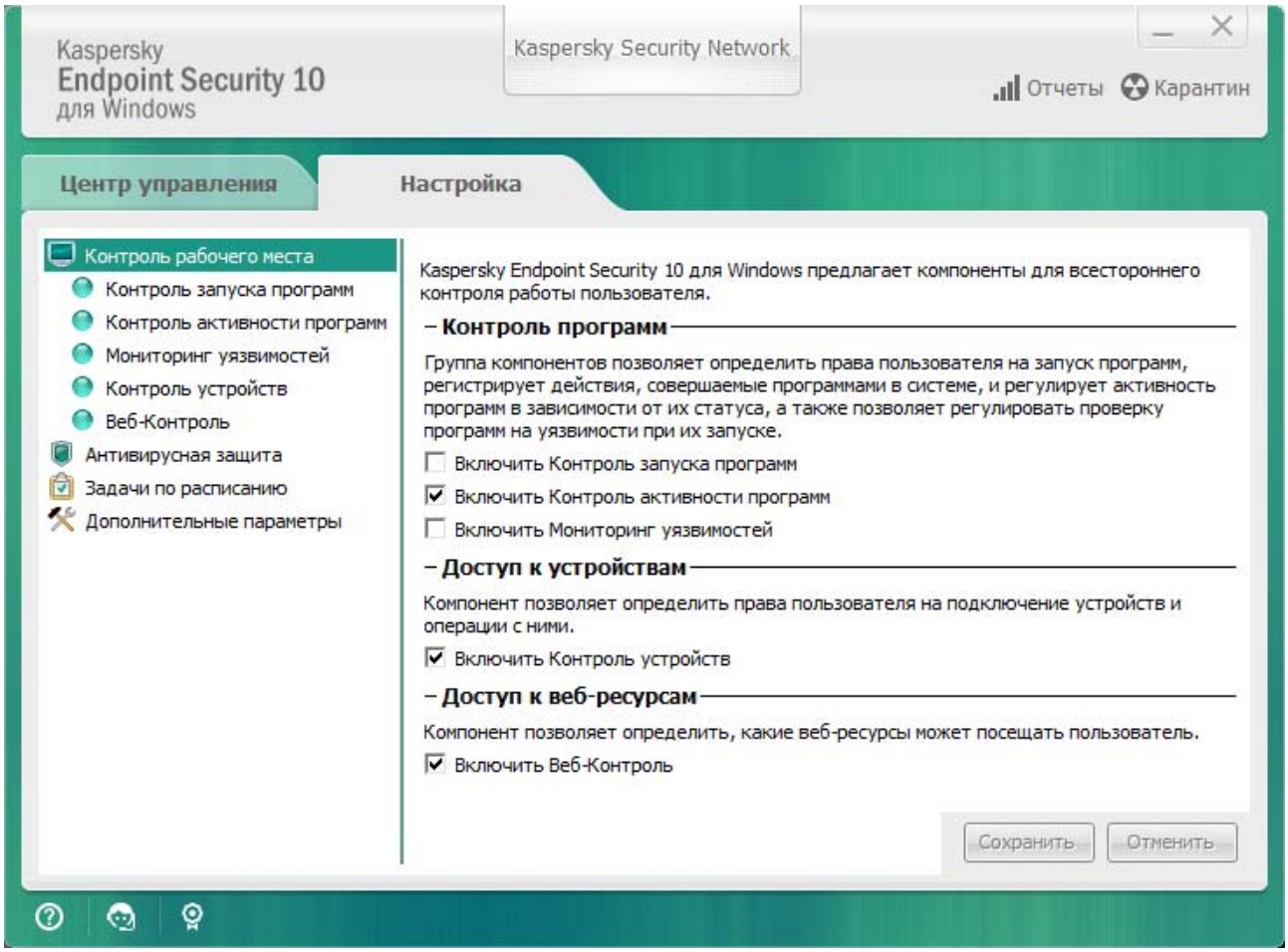


Figure 1: Окно настройки параметров программы

Чтобы открыть закладку настройки параметров программы, выполните одно из следующих действий:

- Выберите закладку **Настройка** в главном окне программы (см. раздел "Главное окно программы" на стр. 64).

- Выберите пункт **Настройка** в контекстном меню значка программы (см. раздел "Контекстное меню значка программы" на стр. 63).

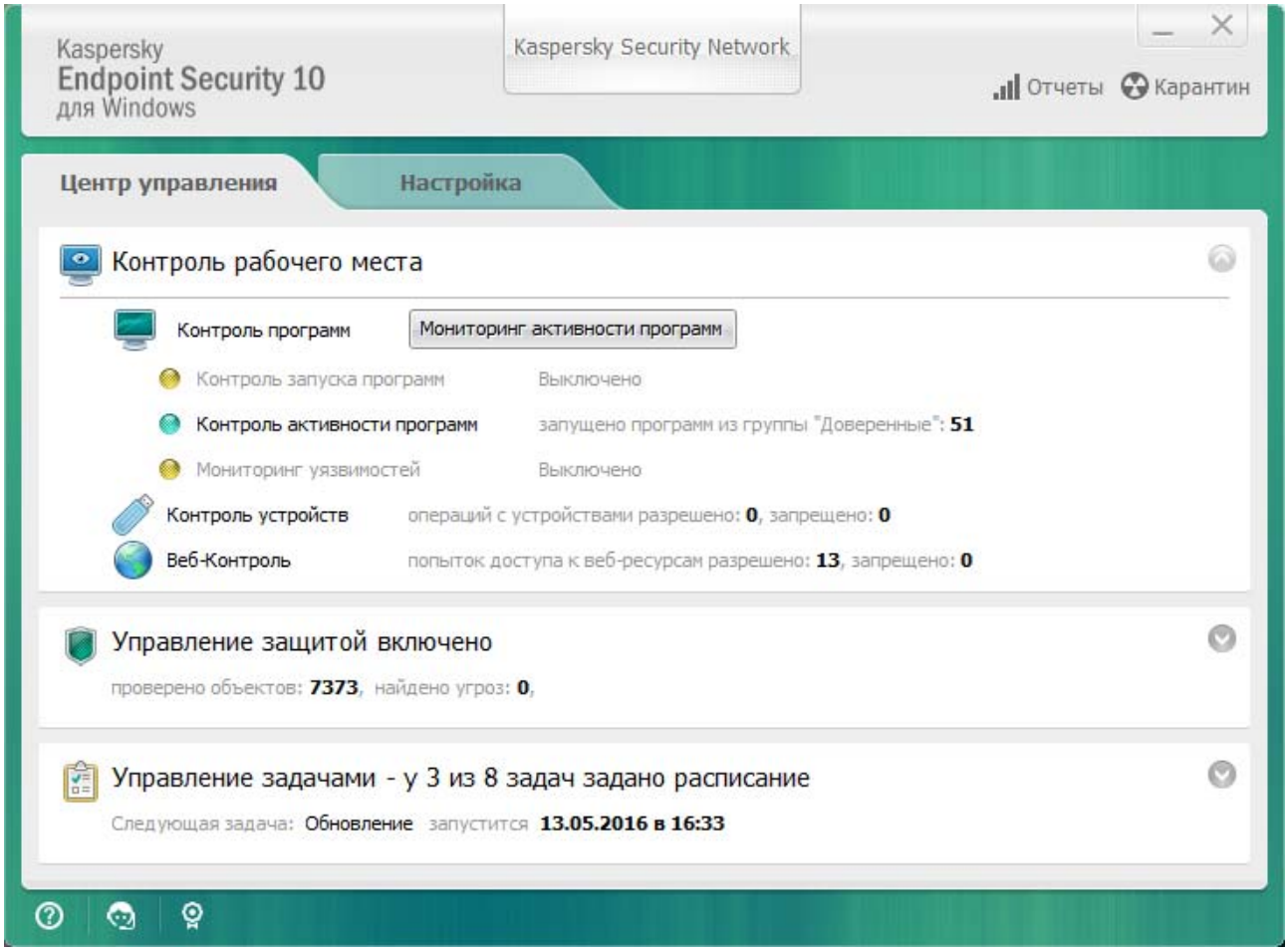
Закладка Центра управления программы

Закладка Центра управления Kaspersky Endpoint Security предназначена для предоставления общей информации о выполнении всех задач и о работе всех компонентов программы. На этой закладке вы также можете регулировать работу компонентов и выполнение задач.

Закладка Центра управления программы состоит из трех частей (см. рис. ниже):

- Блок **Контроль рабочего места** содержит список компонентов контроля.
- Блок **Управление защитой** содержит список компонентов антивирусной защиты.
- Блок **Управление задачами** содержит список локальных задач, выполняемых на компьютере.

В каждом блоке содержатся элементы управления, с помощью которых вы можете включить или выключить работу компонента, перейти в раздел настройки параметров выбранного компонента (задачи), а также просмотреть статистику работы выбранного компонента (задачи).



Чтобы открыть закладку Центра управления программы, выполните одно из следующих действий:

- Выберите закладку **Центр управления** в главном окне программы (см. раздел "Главное окно программы" на стр. 64).
- 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. 63).

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. 27).
- Прочитав документ license.txt. Этот документ включен в комплект поставки программы (см. раздел "Комплект поставки" на стр. 18).

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. 72). 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 антивирусную 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 подписке

Подписка на Kaspersky Endpoint Security – это заказ на использование программы с выбранными параметрами (дата окончания подписки, количество защищаемых устройств). Подписку на Kaspersky Endpoint Security можно зарегистрировать у поставщика услуг (например, у интернет-провайдера). Подписку можно продлевать вручную или в автоматическом режиме или отказаться от нее. Управление подпиской доступно на веб-сайте поставщика услуг (см. раздел "Переход на веб-сайт поставщика услуг" на стр. 80).

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

Если подписка ограничена, по ее истечении может предоставляться буферный период для продления подписки, в течение которого функциональность программы сохраняется. Наличие и длительность буферного периода определяет поставщик услуг.

Чтобы использовать Kaspersky Endpoint Security по подписке, требуется применить код активации, предоставленный поставщиком услуг. После применения кода активации устанавливается активный ключ, определяющий лицензию на использование программы по подписке. При этом дополнительный ключ может быть установлен только с помощью кода активации и не может быть установлен с помощью файла ключа или по подписке.

Функциональность программы, доступная по подписке, может соответствовать функциональности программы для следующих видов коммерческой лицензии: Стандартная,

Kaspersky Business Space Security, Kaspersky Enterprise Space Security. Лицензии этих видов предназначены для защиты файловых серверов, рабочих станций и мобильных устройств, позволяют использовать компоненты контроля на рабочих станциях и мобильных устройствах.

В зависимости от поставщика услуг, набор возможных действий для управления подпиской может различаться. Поставщик услуг может не предоставлять буферный период для продления подписки, в течение которого функциональность программы сохраняется.

Коды активации, приобретенные по подписке, не могут быть использованы для активации предыдущих версий Kaspersky Endpoint Security.

О коде активации

Код активации - это уникальная последовательность из двадцати латинских букв и цифр, которую вы получаете, приобретая коммерческую лицензию на Kaspersky Endpoint Security.

Чтобы активировать программу с помощью кода активации, требуется доступ в интернет для подключения к серверам активации "Лаборатории Касперского".

При активации программы с помощью кода активации устанавливается активный ключ. При этом дополнительный ключ может быть установлен только с помощью кода активации и не может быть установлен с помощью файла ключа или по подписке.

Если код активации был потерян после активации программы, вы можете восстановить код активации. Вам может потребоваться код активации, например, для регистрации в Kaspersky CompanyAccount. Для восстановления кода активации требуется обратиться в Службу технической поддержки "Лаборатории Касперского" (см. раздел "Обращение в Службу технической поддержки" на стр. 552).

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. 71). Kaspersky Security Network и обновления

баз и модулей 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

Принимая условия Лицензионного соглашения, вы соглашаетесь передавать в автоматическом режиме информацию об используемом продукте, а также тип, версию и языковую локализацию установленной программы, уникальный идентификатор установки программы и тип установки, данные об активном и дополнительном ключах (включая тип лицензии, срок действия, дату активации программы и дату окончания срока действия лицензии, номер лицензии, текущее состояние лицензии, версию протокола взаимодействия с сервером активации).

В случае активации программы с помощью кода активации, для целей получения статистической информации о распространении и использовании продуктов Правообладателя вы соглашаетесь предоставлять в автоматическом режиме версию

используемой программы (в том числе информацию об установленных обновлениях программы, идентификаторе установки программы, информацию об используемой лицензии), версию операционной системы, идентификаторы компонентов программы, активных на момент предоставления информации.

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

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

Более подробную информацию о получении, обработке, хранении и уничтожении информации об использовании программы после принятия Лицензионного соглашения и согласия с Положением о KSN вы можете узнать, прочитав тексты этих документов, а также на веб-сайте "Лаборатории Касперского" (http://www.kaspersky.ru/privacy). Файлы license.txt и ksn.txt с текстами Лицензионного соглашения и Положения о KSN входят в комплект поставки (на стр. 18) программы.

Просмотр информации о лицензии

Чтобы просмотреть информацию о лицензии, выполните следующие действия:

1. Откройте главное окно программы (на стр. 64).

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 (см. раздел "О способах активации программы" на стр. 80).

Чтобы приобрести лицензию, выполните следующие действия:

1. Откройте главное окно программы (на стр. 64).
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.

Продление срока действия лицензии

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. 78) новый код активации программы или файл ключа.
2. Добавьте дополнительный ключ (см. раздел "О способах активации программы" на стр. 80) 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".

Продление подписки

При использовании программы по подписке Kaspersky Endpoint Security автоматически обращается к серверу активации через определенные промежутки времени вплоть до даты окончания подписки.

Если вы используете программу по неограниченной подписке, Kaspersky Endpoint Security автоматически в фоновом режиме проверяет наличие обновленного ключа на сервере активации. Если на сервере активации есть ключ, программа добавляет его в режиме замены предыдущего ключа. Таким образом неограниченная подписка на Kaspersky Endpoint Security продлевается без вашего участия.

Если вы используете программу по ограниченной подписке, в день истечения подписки или буферного периода после истечения подписки, во время которого доступно ее продление, Kaspersky Endpoint Security уведомляет вас об этом и прекращает попытки автоматического продления подписки. Поведение Kaspersky Endpoint Security при этом соответствует ситуации, когда истекает срок действия коммерческой лицензии на использование программы (см. раздел "О лицензии" на стр. 71), – программа работает без обновлений и Kaspersky Security Network недоступен.

Вы можете продлить подписку на веб-сайте поставщика услуг (см. раздел "Переход на веб-сайт поставщика услуг" на стр. 80).

Вы можете обновить статус подписки вручную в окне **Лицензирование**. Это может потребоваться, если подписка продлена после истечения буферного периода, и программа автоматически не обновляет статус подписки.

Переход на веб-сайт поставщика услуг

Чтобы перейти на веб сайт поставщика услуг из интерфейса программы, выполните следующие действия:

1. Откройте главное окно программы (на стр. 64).

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

   Откроется окно **Лицензирование**.

3. В окне **Лицензирование** нажмите на кнопку **Связаться с поставщиком подписки**.

О способах активации 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. 46). 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. 81). 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. 524) и последующего запуска (см. раздел "Запуск, остановка, приостановка и возобновление выполнения задачи" на стр. 530) 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. 82).

> 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. 46).

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. 66).

2. В левой части выберите раздел **Антивирусная защита**.

   В правой части окна отобразятся параметры антивирусной защиты.

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. 85) 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. 83).

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. 62):

- 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.

Защита файловой системы компьютера. Файловый Антивирус

Этот раздел содержит информацию о Файловом Антивирусе и инструкции о том, как настроить параметры компонента.

В этом разделе

О Файловом Антивирусе

Файловый Антивирус позволяет избежать заражения файловой системы компьютера. По умолчанию Файловый Антивирус запускается при старте Kaspersky Endpoint Security, постоянно находится в оперативной памяти компьютера и проверяет все открываемые, сохраняемые и запускаемые файлы на компьютере и на всех присоединенных дисках на наличие в них вирусов и других программ, представляющих угрозу.

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. 466) о вредоносном объекте, обнаруженном в файле (если настроены уведомления) и выполняет над файлом действие (см.

раздел "Изменение действия над зараженными файлами" на стр. 418), заданное в параметрах Файлового Антивируса.

Включение и выключение Файлового Антивируса

По умолчанию Файловый Антивирус включен и работает в рекомендованном специалистами "Лаборатории Касперского" режиме. Вы можете выключить Файловый Антивирус при необходимости.

Включить и выключить компонент можно двумя способами:

- на закладке **Центр управления** главного окна программы (см. раздел "Главное окно программы" на стр. 64);
- из окна настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 66).

Чтобы включить или выключить Файловый Антивирус на закладке Центр управления главного окна программы, выполните следующие действия:

1. Откройте главное окно программы.
2. Выберите закладку **Центр управления**.
3. Нажмите клавишей мыши на блок **Управление защитой**.

   Блок **Управление защитой** раскроется.
4. По правой клавише мыши откройте контекстное меню строки с информацией о компоненте Файловый Антивирус.

   Откроется меню действий с компонентом.
5. Выполните одно из следующих действий:
   - Выберите в меню пункт **Включить**, если вы хотите включить Файловый Антивирус.

Значок статуса работы компонента , отображающийся слева в строке **Файловый Антивирус**, изменится на значок .

- Выберите в меню пункт **Выключить**, если вы хотите выключить Файловый Антивирус.

  Значок статуса работы компонента , отображающийся слева в строке **Файловый Антивирус**, изменится на значок .

Чтобы включить или выключить Файловый Антивирус из окна настройки параметров программы, выполните следующие действия:

1. Откройте окно настройки параметров программы.
2. В левой части окна в разделе **Антивирусная защита** выберите подраздел **Файловый Антивирус**.

   В правой части окна отобразятся параметры компонента Файловый Антивирус.
3. Выполните одно из следующих действий:

   - Установите флажок **Включить Файловый Антивирус**, если вы хотите включить Файловый Антивирус.
   - Снимите флажок **Включить Файловый Антивирус**, если вы хотите выключить Файловый Антивирус.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Автоматическая приостановка работы Файлового Антивируса

Вы можете настроить автоматическую приостановку работы Файлового Антивируса в указанное время или во время работы с определенными программами.

Приостановка работы Файлового Антивируса 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 (https://companyaccount.kaspersky.com)). Специалисты помогут вам наладить совместную работу Файлового Антивируса с другими программами на вашем компьютере.

Чтобы настроить автоматическую приостановку работы Файлового Антивируса, выполните следующие действия:

1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 66).

2. В левой части окна в разделе **Антивирусная защита** выберите подраздел **Файловый Антивирус**.

   В правой части окна отобразятся параметры компонента Файловый Антивирус.

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

   Откроется окно **Файловый Антивирус**.

4. В окне **Файловый Антивирус** 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 Файлового Антивируса в указанное время.

     Откроется окно **Приостановка задачи**.

   - Установите флажок **При запуске программ** и нажмите на кнопку **Выбрать**, если вы хотите настроить автоматическую приостановку работы Файлового Антивируса при запуске указанных программ.

     Откроется окно **Программы**.

6. Выполните одно из следующих действий:

- Если вы настраиваете автоматическую приостановку работы Файлового Антивируса в указанное время, то в окне **Приостановка задачи** в полях **Приостановить в** и **Возобновить в** укажите время (в формате ЧЧ:ММ), в течение которого работу Файлового Антивируса следует приостанавливать. Нажмите на кнопку **OK**.

- Если вы настраиваете автоматическую приостановку работы Файлового Антивируса при запуске указанных программ, то в окне **Программы** с помощью кнопок **Добавить**, **Изменить** и **Удалить** сформируйте список программ, во время работы которых работу Файлового Антивируса следует приостанавливать. Нажмите на кнопку **OK**.

7. В окне **Файловый Антивирус** нажмите на кнопку **OK**.

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

Настройка Файлового Антивируса

Вы можете выполнить следующие действия для настройки работы Файлового Антивируса:

- 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 Файловый Антивирус выполняет при обнаружении зараженного файла.

- Сформировать область защиты Файлового Антивируса.

  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 Файловый Антивирус использует метод проверки Машинное обучение и сигнатурный анализ. В процессе сигнатурного анализа Файловый Антивирус 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 Файловый Антивирус 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 Файловым Антивирусом: 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 Файловый Антивирус 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. 66).

2. В левой части окна в разделе **Антивирусная защита** выберите подраздел **Файловый Антивирус**.

   В правой части окна отобразятся параметры компонента Файловый Антивирус.

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 **Файловый Антивирус**.

  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 Файлового Антивируса над зараженными файлами

Чтобы изменить действие Файлового Антивируса над зараженными файлами, выполните следующие действия:

1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 66).

2. В левой части окна в разделе **Антивирусная защита** выберите подраздел **Файловый Антивирус**.

   В правой части окна отобразятся параметры компонента Файловый Антивирус.

3. В блоке **Действие при обнаружении угрозы** выберите нужный вариант:

   - **Выбирать действие автоматически**.

   - **Выполнять действие: Лечить. Удалять, если лечение невозможно**.

   - **Выполнять действие: Лечить**.

Даже если выбран этот вариант, в отношении файлов, являющихся частью приложения Windows Store, Kaspersky Endpoint Security выполняет действие **Удалить**.

- **Выполнять действие: Удалять**.
- **Выполнять действие: Блокировать**.

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

Формирование области защиты Файлового Антивируса

Под областью защиты подразумеваются объекты, которые проверяет компонент во время своей работы. Область защиты разных компонентов имеет разные свойства. Свойствами области защиты Файлового Антивируса являются местоположение и тип проверяемых файлов. По умолчанию Файловый Антивирус 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. 66).
2. В левой части окна в разделе **Антивирусная защита** выберите подраздел **Файловый Антивирус**.

   В правой части окна отобразятся параметры компонента Файловый Антивирус.
3. В блоке **Уровень безопасности** нажмите на кнопку **Настройка**.

   Откроется окно **Файловый Антивирус**.
4. В окне **Файловый Антивирус** выберите закладку **Общие**.
5. В блоке **Типы файлов** укажите тип файлов, которые вы хотите проверять Файловым Антивирусом:

- 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 Файловый Антивирус 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 **Файловый Антивирус**.

     Нажмите на кнопку **OK**.

   - 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 Файловым Антивирусом.

10. В окне **Файловый Антивирус** нажмите на кнопку **OK**.

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

Использование эвристического анализа в работе Файлового Антивируса

Чтобы настроить использование эвристического анализа в работе Файлового Антивируса, выполните следующие действия:

1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 66).

2. В левой части окна в разделе **Антивирусная защита** выберите подраздел **Файловый Антивирус**.

   В правой части окна отобразятся параметры компонента Файловый Антивирус.

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

   Откроется окно **Файловый Антивирус**.

4. В окне **Файловый Антивирус** выберите закладку **Производительность**.

5. В блоке **Методы проверки** выполните следующие действия:

   - Если вы хотите, чтобы Файловый Антивирус использовал эвристический анализ, установите флажок **Эвристический анализ** и при помощи ползунка задайте уровень эвристического анализа: **поверхностный**, **средний** или **глубокий**.

   - Если вы хотите, чтобы Файловый Антивирус 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 Файлового Антивируса

Чтобы настроить использование технологий проверки в работе Файлового Антивируса, выполните следующие действия:

1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 66).

2. В левой части окна в разделе **Антивирусная защита** выберите подраздел **Файловый Антивирус**.

   В правой части окна отобразятся параметры компонента Файловый Антивирус.

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

   Откроется окно **Файловый Антивирус**.

4. В окне **Файловый Антивирус** выберите закладку **Дополнительно**.

5. В блоке **Технологии проверки** выполните следующие действия:

- Установите флажки около названий тех технологий, которые вы хотите использовать в работе Файлового Антивируса.
- Снимите флажки около названий тех технологий, которые вы не хотите использовать в работе Файлового Антивируса.

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. 66).
2. В левой части окна в разделе **Антивирусная защита** выберите подраздел **Файловый Антивирус**.

   В правой части окна отобразятся параметры компонента Файловый Антивирус.
3. Нажмите на кнопку **Настройка**.

   Откроется окно **Файловый Антивирус**.
4. В окне **Файловый Антивирус** выберите закладку **Производительность**.
5. В блоке **Оптимизация проверки** установите флажок **Проверять только новые и измененные файлы**.
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 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.
>
> Файловый Антивирус 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. 66).
2. В левой части окна в разделе **Антивирусная защита** выберите подраздел **Файловый Антивирус**.

   В правой части окна отобразятся параметры компонента Файловый Антивирус.
3. В блоке **Уровень безопасности** нажмите на кнопку **Настройка**.

   Откроется окно **Файловый Антивирус**.
4. В окне **Файловый Антивирус** 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**.

   Файловый Антивирус 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 Файловому Антивирусу распаковывать составные файлы в фоновом режиме, снимите флажок **Распаковывать составные файлы в фоновом режиме**.

   - Чтобы разрешить Файловому Антивирусу 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 Файловому Антивирусу распаковывать составные файлы большого размера, установите флажок **Не распаковывать составные файлы большого размера** и в поле **Максимальный размер файла** укажите нужное значение. Файловый Антивирус не будет распаковывать составные файлы больше указанного размера.

   - Чтобы разрешить Файловому Антивирусу 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**.

   > Файловый Антивирус 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 **Файловый Антивирус** нажмите на кнопку **OK**.

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

Изменение режима проверки файлов

Под *режимом проверки* подразумевается условие, при котором Файловый Антивирус начинает проверять файлы. По умолчанию Kaspersky Endpoint Security использует интеллектуальный режим проверки файлов. Работая в этом режиме проверки файлов, Файловый Антивирус 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. 66).

2. В левой части окна в разделе **Антивирусная защита** выберите подраздел **Файловый Антивирус**.

   В правой части окна отобразятся параметры компонента Файловый Антивирус.

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

   Откроется окно **Файловый Антивирус**.

4. В окне **Файловый Антивирус** выберите закладку **Дополнительно**.

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

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

6. Нажмите на кнопку **OK**.

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

Защита почты. Почтовый Антивирус

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 (см. раздел "Аппаратные и программные требования" на стр. 24).

Этот раздел содержит информацию о Почтовом Антивирусе и инструкции о том, как настроить параметры компонента.

В этом разделе

О Почтовом Антивирусе

Почтовый Антивирус 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 почтовом сообщении не обнаружены, оно становится доступным и / или обрабатывается.

При обнаружении угрозы в почтовом сообщении Почтовый Антивирус выполняет следующие

действия:

1. Определяет тип объекта, обнаруженного в почтовом сообщении (например, *троянская программа*).

2. Присваивает почтовому сообщению один из следующих статусов:

   - *Заражен*. Этот статус присваивается объекту в следующих случаях:

     - Если в результате проверки в почтовом сообщении найден участок кода известного вируса, информация о котором содержится в антивирусных базах Kaspersky Endpoint Security.

     - Если в почтовом сообщении присутствует участок кода, свойственный вирусам и другим программам, представляющим угрозу, или модифицированный код известного вируса.

   - *Не найдено*. Этот статус присваивается объекту, если в результате проверки в почтовом сообщении не обнаружено вирусов или других программ, представляющих угрозу.

После этого программа блокирует почтовое сообщение, выводит на экран уведомление (см. стр. 466) об обнаруженном объекте (если это указано в параметрах уведомлений) и выполняет действие, заданное в параметрах Почтового Антивируса.

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 Почтового Антивируса встраивается в почтовый клиент Microsoft Office Outlook во время установки Kaspersky Endpoint Security.

Процесс работы Почтового Антивируса отображается с помощью значка программы в области уведомлений панели задач. Когда Почтовый Антивирус проверяет почтовое сообщение, значок программы принимает вид  .

Включение и выключение Почтового Антивируса

По умолчанию Почтовый Антивирус включен и работает в рекомендованном специалистами "Лаборатории Касперского" режиме. Вы можете выключить Почтовый Антивирус при необходимости.

Включить и выключить компонент можно двумя способами:

- на закладке **Центр управления** главного окна программы (см. раздел "Главное окно программы" на стр. 64);
- из окна настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 66).

Чтобы включить или выключить Почтовый Антивирус на закладке Центр управления главного окна программы, выполните следующие действия:

1. Откройте главное окно программы.
2. Выберите закладку **Центр управления**.
3. Нажмите клавишей мыши на блок **Управление защитой**.

   Блок **Управление защитой** раскроется.
4. По правой клавише мыши откройте контекстное меню строки с информацией о компоненте Почтовый Антивирус.

   Откроется меню действий с компонентом.
5. Выполните одно из следующих действий:
   - Выберите в меню пункт **Включить**, если вы хотите включить Почтовый Антивирус.

     Значок статуса работы компонента  , отображающийся слева в строке **Почтовый Антивирус**, изменится на значок .

- Выберите в меню пункт **Выключить**, если вы хотите выключить Почтовый Антивирус.

  Значок статуса работы компонента , отображающийся слева в строке **Почтовый Антивирус**, изменится на значок .

Чтобы включить или выключить Почтовый Антивирус из окна настройки параметров программы, выполните следующие действия:

1. Откройте окно настройки параметров программы.
2. В левой части окна в разделе **Антивирусная защита** выберите подраздел **Почтовый Антивирус**.

   В правой части окна отобразятся параметры компонента Почтовый Антивирус.
3. Выполните одно из следующих действий:

   - Установите флажок **Включить Почтовый Антивирус**, если вы хотите включить Почтовый Антивирус.
   - Снимите флажок **Включить Почтовый Антивирус**, если вы хотите выключить Почтовый Антивирус.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Настройка Почтового Антивируса

Вы можете выполнить следующие действия для настройки работы Почтового Антивируса:

- 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 Почтового Антивируса.
- 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™), Почтовый Антивирус проверяет трафик почтовых протоколов SMTP, POP3, IMAP и NNTP.

  > Работая с почтовым клиентом Mozilla Thunderbird, Почтовый Антивирус 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 Почтовый Антивирус 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. 66).

2. В левой части окна в разделе **Антивирусная защита** выберите подраздел **Почтовый Антивирус**.

   В правой части окна отобразятся параметры компонента Почтовый Антивирус.

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 **Почтовый Антивирус**.

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

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. 66).

2. В левой части окна в разделе **Антивирусная защита** выберите подраздел **Почтовый Антивирус**.

   В правой части окна отобразятся параметры компонента Почтовый Антивирус.

3. В блоке **Действие при обнаружении угрозы** выберите вариант действия, которое выполняет Kaspersky Endpoint Security при обнаружении зараженного сообщения:

   - **Выбирать действие автоматически**.
   - **Выполнять действие: Лечить. Удалять, если лечение невозможно**.
   - **Выполнять действие: Лечить**.
   - **Выполнять действие: Удалять**.
   - **Выполнять действие: Блокировать**.

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

Формирование области защиты Почтового Антивируса

Область защиты - это объекты, которые проверяет компонент во время своей работы. Область защиты разных компонентов имеет разные свойства. Свойствами области защиты Почтового Антивируса являются параметры интеграции Почтового Антивируса в почтовые клиенты, тип сообщений электронной почты и почтовые протоколы, трафик которых проверяет Почтовый Антивирус. 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 Почтового Антивируса, выполните следующие действия:

1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 66).

2. В левой части окна в разделе **Антивирусная защита** выберите подраздел **Почтовый Антивирус**.

   В правой части окна отобразятся параметры компонента Почтовый Антивирус.

3. Нажмите на кнопку **Настройка**.

   Откроется окно **Почтовый Антивирус**.

4. Выберите закладку **Общие**.

5. В блоке **Область защиты** выполните одно из следующих действий:

   - Выберите вариант **Входящие и исходящие сообщения**, если вы хотите, чтобы Почтовый Антивирус проверял все входящие и исходящие сообщения на вашем компьютере.

   - Выберите вариант **Только входящие сообщения**, если вы хотите, чтобы Почтовый Антивирус 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 Почтовый Антивирус 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 Почтовый Антивирус не проверял сообщения, передающиеся по протоколам POP3, SMTP, NNTP и IMAP, до их получения на компьютере пользователя. В этом случае сообщения проверяет расширение Почтового Антивируса, 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** Почтовый Антивирус 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 Почтового Антивируса 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 Почтового Антивируса 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 Почтового Антивируса 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. 66).

2. В левой части окна в разделе **Антивирусная защита** выберите подраздел **Почтовый Антивирус**.

   В правой части окна отобразятся параметры компонента Почтовый Антивирус.

3. Нажмите на кнопку **Настройка**.

   Откроется окно **Почтовый Антивирус**.

4. Выберите закладку **Общие**.

5. В блоке **Проверка составных файлов** выполните следующие действия:

   - Снимите флажок **Проверять вложенные архивы**, если вы хотите, чтобы Почтовый Антивирус не выполнял проверку вложенных в сообщения архивов.

   - Установите флажок **Не проверять архивы размером более N МБ**, если вы хотите, чтобы Почтовый Антивирус 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 Почтовый Антивирус 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

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. 66).

2. В левой части окна в разделе **Антивирусная защита** выберите подраздел **Почтовый Антивирус**.

   В правой части окна отобразятся параметры компонента Почтовый Антивирус.

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

   Откроется окно **Почтовый Антивирус**.

4. В окне **Почтовый Антивирус** выберите закладку **Фильтр вложений**.

5. Выполните одно из следующих действий:

- Выберите вариант **Не применять фильтр**, если вы хотите, чтобы Почтовый Антивирус не фильтровал вложения в сообщениях.

- Выберите вариант **Переименовывать вложения указанных типов**, если вы хотите, чтобы Почтовый Антивирус изменял названия вложенных в сообщения файлов указанных типов.

- Выберите вариант **Удалять вложения указанных типов**, если вы хотите, чтобы Почтовый Антивирус 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 Почтового Антивируса. Оно позволяет перейти к настройке параметров Почтового Антивируса из программы Outlook, а также указать, в какой момент проверять сообщения электронной почты на присутствие вирусов и других программ, представляющих угрозу. Расширение Почтового Антивируса для Outlook может проверять входящие и исходящие сообщения, переданные по протоколам POP3, SMTP, NNTP, IMAP и MAPI.

Настройка параметров Почтового Антивируса 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 Почтовый Антивирус (если в интерфейсе программы Kaspersky Endpoint Security установлен флажок **Трафик POP3 / SMTP / NNTP / IMAP**), затем входящие сообщения проверяет расширение Почтового Антивируса для Outlook. Если Почтовый Антивирус обнаруживает в сообщении вредоносный объект, он уведомляет вас об этом.

От выбора действия в окне уведомления зависит, кто устраняет угрозу в сообщении: Почтовый Антивирус или расширение Почтового Антивируса для Outlook:

- Если в окне уведомления пользователь выбирает действие **Лечить** или **Удалить**, то действие по устранению угрозы выполняет Почтовый Антивирус.
- Если в окне уведомления пользователь выбирает действие **Пропустить**, то действие по устранению угрозы выполняет расширение Почтового Антивируса для Outlook.

Исходящие сообщения сначала проверяет расширение Почтового Антивируса для Outlook, а затем проверяет Почтовый Антивирус.

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, 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 Почтового Антивируса 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 https://technet.microsoft.com/ru-ru/library/cc179175.aspx.

Чтобы настроить режим работы расширения Почтового Антивируса 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 **Антивирусная защита** выберите подраздел **Почтовый Антивирус**.
7. В блоке **Уровень безопасности** нажмите на кнопку **Настройка**.

   Откроется окно **Почтовый Антивирус**.
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 Почтового Антивируса для Outlook проверяло входящие сообщения в момент их поступления в почтовый ящик.
   - Установите флажок **Проверять при прочтении**, если вы хотите, чтобы расширение Почтового Антивируса для Outlook проверяло входящие сообщения в тот момент, когда пользователь открывает их для чтения.
   - Установите флажок **Проверять при отправке**, если вы хотите, чтобы расширение Почтового Антивируса 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 **Почтовый Антивирус**.
12. Примените политику.

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

Защита компьютера в интернете. Веб-Антивирус

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 (см. раздел "Аппаратные и программные требования" на стр. 24).

Этот раздел содержит информацию о Веб-Антивирусе и инструкции о том, как настроить параметры компонента.

В этом разделе

О Веб-Антивирусе

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 скачивает 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.

Веб-Антивирус 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, Веб-Антивирус 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 Веб-Антивируса действие.

Включение и выключение Веб-Антивируса

По умолчанию Веб-Антивирус включен и работает в рекомендованном специалистами "Лаборатории Касперского" режиме. Вы можете выключить Веб-Антивирус при необходимости.

Включить и выключить компонент можно двумя способами:

- на закладке **Центр управления** главного окна программы (см. раздел "Главное окно программы" на стр. 64);
- из окна настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 66).

Чтобы включить или выключить Веб-Антивирус на закладке Центр управления главного окна программы, выполните следующие действия:

1. Откройте главное окно программы.
2. Выберите закладку **Центр управления**.
3. Нажмите клавишей мыши на блок **Управление защитой**.

Блок **Управление защитой** раскроется.

4. По правой клавише мыши откройте контекстное меню строки с информацией о компоненте Веб-Антивирус.

   Откроется меню действий с компонентом.

5. Выполните одно из следующих действий:

   - Выберите в меню пункт **Включить**, если вы хотите включить Веб-Антивирус.

     Значок статуса работы компонента , отображающийся слева в строке **Веб-Антивирус**, изменится на значок .

   - Выберите в меню пункт **Выключить**, если вы хотите выключить Веб-Антивирус.

     Значок статуса работы компонента , отображающийся слева в строке **Веб-Антивирус**, изменится на значок .

Чтобы включить или выключить Веб-Антивирус из окна настройки параметров программы, выполните следующие действия:

1. Откройте окно настройки параметров программы.

2. В левой части окна в разделе **Антивирусная защита** выберите подраздел **Веб-Антивирус**.

   В правой части окна отобразятся параметры компонента Веб-Антивирус.

3. Выполните одно из следующих действий:

   - Установите флажок **Включить Веб-Антивирус**, если вы хотите включить Веб-Антивирус.

   - Снимите флажок **Включить Веб-Антивирус**, если вы хотите выключить Веб-Антивирус.

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

Настройка Веб-Антивируса

Вы можете выполнить следующие действия для настройки работы Веб-Антивируса:

- 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-Антивирусом объекта веб-трафика выясняется, что объект содержит вредоносный код, дальнейшие операции Веб-Антивируса с этим объектом зависят от указанного вами действия.

- Настроить проверку Веб-Антивирусом ссылок 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-Антивирусом веб-трафика, исходящего и поступающего по протоколам HTTP и FTP.

- Сформировать список доверенных веб-адресов.

Вы можете сформировать список веб-адресов, содержанию которых вы доверяете. Веб-Антивирус 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 Веб-Антивирус 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, Веб-Антивирус 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. 66).

2. В левой части окна в разделе **Антивирусная защита** выберите подраздел **Веб-Антивирус**.

   В правой части окна отобразятся параметры компонента Веб-Антивирус.

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 **Веб-Антивирус**.

     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

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. 66).

2. В левой части окна в разделе **Антивирусная защита** выберите подраздел **Веб-Антивирус**.

   В правой части окна отобразятся параметры компонента Веб-Антивирус.

3. В блоке **Действие при обнаружении угрозы** выберите вариант действия, которое Kaspersky Endpoint Security выполняет над вредоносными объектами веб-трафика:

   - **Выбирать действие автоматически**.
   - **Запрещать загрузку**.
   - **Разрешать загрузку**.

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

Проверка Веб-Антивирусом 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 почтовое сообщение 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 почтовом сообщении, но и, например, в тексте ICQ-сообщения, Веб-Антивирус 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 Веб-Антивирусом 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. 66).

2. В левой части окна в разделе **Антивирусная защита** выберите подраздел **Веб-Антивирус**.

В правой части окна отобразятся параметры компонента Веб-Антивирус.

3. Нажмите на кнопку **Настройка**.

   Откроется окно **Веб-Антивирус**.

4. В окне **Веб-Антивирус** выберите закладку **Общие**.

5. Выполните следующие действия:

   - В блоке **Методы проверки** установите флажок **Проверять ссылки по базе вредоносных веб-адресов**, если вы хотите, чтобы Веб-Антивирус проверял ссылки по базам вредоносных веб-адресов.

   - В блоке **Параметры антифишинга** установите флажок **Проверять ссылки по базе фишинговых веб-адресов**, если вы хотите, чтобы Веб-Антивирус 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. 544).

6. Нажмите на кнопку **OK**.

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

Использование эвристического анализа в работе Веб-Антивируса

Чтобы настроить использование эвристического анализа, выполните следующие действия:

1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 66).

2. В левой части окна в разделе **Антивирусная защита** выберите подраздел **Веб-Антивирус**.

   В правой части окна отобразятся параметры компонента Веб-Антивирус.

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

   Откроется окно **Веб-Антивирус**.

4. Выберите закладку **Общие**.

5. Если вы хотите, чтобы Веб-Антивирус 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 Веб-Антивирус 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 **ОК**.

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. 66).

2. В левой части окна в разделе **Антивирусная защита** выберите подраздел **Веб-Антивирус**.

   В правой части окна отобразятся параметры компонента Веб-Антивирус.

3. Нажмите на кнопку **Настройка**.

   Откроется окно **Веб-Антивирус**.

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 трафика IM-клиентов. IM-Антивирус

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 (см. раздел "Аппаратные и программные требования" на стр. 24).

Этот раздел содержит информацию об IM-Антивирусе и инструкции о том, как настроить параметры компонента.

В этом разделе

Об IM-Антивирусе

IM-Антивирус предназначен для проверки трафика, передаваемого программами для быстрого обмена сообщениями (так называемыми *IM-клиентами*).

IM-Антивирус не проверяет сообщения, передаваемые по зашифрованному каналу.

Сообщения, переданные через IM-клиенты, могут содержать следующие виды угроз безопасности компьютера:

- Ссылки, при активации которых на компьютер пользователя пытается загрузиться вредоносная программа.
- Ссылки на вредоносные программы и веб-страницы, которые злоумышленники используют для фишинговых атак.

  Целью фишинговых атак является хищение персональных данных пользователей, например: номеров банковских карт, паспортных данных, паролей к платежным системам банков или другим интернет-сервисам (например, социальным сетям или почтовым сервисам).

Через IM-клиенты можно передавать файлы. Во время попытки сохранения этих файлов их проверяет компонент Файловый Антивирус (см. раздел "О Файловом Антивирусе" на стр. 87).

IM-Антивирус перехватывает каждое сообщение, которое пользователь принимает или отправляет с помощью IM-клиента, и проверяет сообщение на наличие в нем ссылок, представляющих угрозу безопасности компьютера:

- Если в сообщении не обнаружены ссылки, представляющие угрозу, сообщение становится доступным для пользователя.
- Если в сообщении обнаружены ссылки, представляющие угрозу, IM-Антивирус заменяет это сообщение информацией об обнаруженной угрозе в окне переписки используемого IM-клиента.

Включение и выключение IM-Антивируса

По умолчанию IM-Антивирус включен и работает в рекомендованном специалистами "Лаборатории Касперского" режиме. Вы можете выключить IM-Антивирус при необходимости.

Включить и выключить компонент можно двумя способами:

- на закладке **Центр управления** главного окна программы;
- из окна настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 66).

Чтобы включить или выключить IM-Антивирус на закладке Центр управления главного окна программы, выполните следующие действия:

1. Откройте главное окно программы.
2. Выберите закладку **Центр управления**.
3. Нажмите клавишей мыши на блок **Управление защитой**.

   Блок **Управление защитой** раскроется.
4. По правой клавише мыши на строке **IM-Антивирус** откройте контекстное меню действий с компонентом.
5. Выполните одно из следующих действий:
   - Выберите в контекстном меню пункт **Включить**, если вы хотите включить IM-Антивирус.

     Значок статуса работы компонента , отображающийся слева в строке **IM-Антивирус**, изменится на значок .
   - Выберите в контекстном меню пункт **Выключить**, если вы хотите выключить IM-Антивирус.

     Значок статуса работы компонента , отображающийся слева в строке **IM-Антивирус**, изменится на значок .

Чтобы включить или выключить IM-Антивирус из окна настройки параметров программы, выполните следующие действия:

1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 66).

2. В левой части окна в разделе **Антивирусная защита** выберите подраздел **IM-Антивирус**.

   В правой части окна отобразятся параметры компонента IM-Антивирус.

3. Выполните одно из следующих действий:

   - Установите флажок **Включить IM-Антивирус**, если вы хотите включить IM-Антивирус.
   - Снимите флажок **Включить IM-Антивирус**, если вы хотите выключить IM-Антивирус.

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

Настройка IM-Антивируса

Вы можете выполнить следующие действия для настройки работы IM-Антивируса:

- Настроить область защиты.

  Вы можете расширить или сузить область защиты, изменив тип проверяемых сообщений, передаваемых через IM-клиенты.

- Настроить проверку IM-Антивирусом ссылок в сообщениях IM-клиентов по базам вредоносных и фишинговых веб-адресов.

В этом разделе

Формирование области защиты IM-Антивируса

Под областью защиты подразумеваются объекты, которые проверяет компонент во время своей работы. Область защиты разных компонентов имеет разные свойства. Свойством области защиты IM-Антивируса является тип проверяемых сообщений, поступающих и отправляемых через IM-клиенты. По умолчанию IM-Антивирус проверяет как входящие, так и исходящие сообщения. Вы можете отказаться от проверки исходящих сообщений.

Чтобы сформировать область защиты, выполните следующие действия:

1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 66).

2. В левой части окна в разделе **Антивирусная защита** выберите подраздел **IM-Антивирус**.

   В правой части окна отобразятся параметры компонента IM-Антивирус.

3. В блоке **Область защиты** выполните одно из следующих действий:

   - Выберите вариант **Входящие и исходящие сообщения**, если вы хотите, чтобы IM-Антивирус проверял все входящие и исходящие сообщения IM-клиентов.

   - Выберите вариант **Только входящие сообщения**, если вы хотите, чтобы IM-Антивирус проверял только входящие сообщения IM-клиентов.

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

Проверка IM-Антивирусом ссылок по базам вредоносных и фишинговых веб-адресов

Чтобы настроить проверку IM-Антивирусом ссылок по базам вредоносных и фишинговых веб-адресов, выполните следующие действия:

1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 66).

2. В левой части окна в разделе **Антивирусная защита** выберите подраздел **IM-Антивирус**.

   В правой части окна отобразятся параметры компонента IM-Антивирус.

3. В блоке **Методы проверки** установите флажки около названий тех методов, которые вы хотите использовать в работе IM-Антивируса:

   - Установите флажок **Проверять ссылки по базе вредоносных веб-адресов**, если вы хотите проверять ссылки в сообщениях IM-клиентов на их принадлежность к базе вредоносных веб-адресов.

   - Установите флажок **Проверять ссылки по базе фишинговых веб-адресов**, если вы хотите проверять ссылки в сообщениях IM-клиентов на их принадлежность к базе фишинговых веб-адресов.

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

Мониторинг системы

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 (см. раздел "Аппаратные и программные требования" на стр. 24).

Этот раздел содержит информацию о Мониторинге системы и инструкции о том, как настроить параметры компонента.

В этом разделе

О Мониторинге системы

Мониторинг системы получает данные о действиях программ на вашем компьютере и предоставляет эту информацию другим компонентам для более эффективной защиты.

Шаблоны опасного поведения программ

Шаблоны опасного поведения программ BSS (Behavior Stream Signatures) (далее также "шаблоны опасного поведения") содержат последовательности действий программ, которые Kaspersky Endpoint Security классифицирует как опасные. Если активность программы совпадает с одним из шаблонов опасного поведения, Kaspersky Endpoint Security выполняет

заданное действие. Функциональность Kaspersky Endpoint Security, основанная на шаблонах опасного поведения, обеспечивает проактивную защиту компьютера.

По умолчанию, если активность программы полностью совпадает с шаблоном опасного поведения, Мониторинг системы удаляет исполняемый файл этой программы и сохраняет копию удаленного файла в Резервном хранилище.

Откат действий, произведенных вредоносными программами

На основе информации, полученной Мониторингом системы, Kaspersky Endpoint Security при лечении вредоносных программ может выполнять откат действий, произведенных вредоносными программами в операционной системе.

Откат действий вредоносной программы может быть инициирован Файловым Антивирусом (см. стр. 87) или при антивирусной проверке (см. раздел «Проверка компьютера» на стр. 412).

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 Мониторинга системы

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

Не рекомендуется выключать Мониторинг системы без необходимости, так как это снижает эффективность работы компонентов защиты. Компоненты защиты могут запрашивать данные, полученные Мониторингом системы, для уточнения обнаруженной угрозы.

Включить и выключить Мониторинг системы можно двумя способами:

- на закладке **Центр управления** главного окна программы (см. раздел "Главное окно программы" на стр. 64);
- из окна настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 66).

*Чтобы включить или выключить Мониторинг системы на закладке **Центр управления** главного окна программы, выполните следующие действия:*

1. Откройте главное окно программы.
2. Выберите закладку **Центр управления**.
3. Нажмите клавишей мыши на блок **Управление защитой**.

   Блок **Управление защитой** раскроется.
4. По правой клавише мыши откройте контекстное меню строки с информацией о компоненте Мониторинг системы.

   Откроется меню действий с компонентом.
5. Выполните одно из следующих действий:
   - Выберите в меню пункт **Включить**, если вы хотите включить Мониторинг системы.

     Значок статуса работы компонента  , отображающийся слева в строке **Мониторинг системы**, изменится на значок  .
   - Выберите в меню пункт **Выключить**, если вы хотите выключить Мониторинг системы.

     Значок статуса работы компонента  , отображающийся слева в строке **Мониторинг системы**, изменится на значок  .

Чтобы включить или выключить Мониторинг системы из окна настройки параметров программы, выполните следующие действия:

1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 66).

2. В левой части окна в разделе **Антивирусная защита** выберите подраздел **Мониторинг системы**.

   В правой части окна отобразятся параметры компонента **Мониторинг системы**.

3. Выполните одно из следующих действий:

   - Установите флажок **Включить Мониторинг системы**, если вы хотите включить Мониторинг системы.

   - Снимите флажок **Включить Мониторинг системы**, если вы хотите выключить Мониторинг системы.

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

Настройка Мониторинга системы

Вы можете выполнить следующие действия для настройки работы Мониторинга системы:

- включить или выключить защиту от эксплойтов;
- выбрать действие при обнаружении вредоносной активности программы;
- включить или выключить откат действий вредоносных программ при лечении.

В этом разделе

Включение и выключение защиты от эксплойтов

Чтобы включить или выключить защиту от эксплойтов, выполните следующие действия:

1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 66).

2. В левой части окна в разделе **Антивирусная защита** выберите подраздел **Мониторинг системы**.

   В правой части окна отобразятся параметры компонента **Мониторинг системы**.

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 он выполняет действие, выбранное в раскрывающемся списке **Действие при обнаружении угрозы**.

   - 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.

Выбор действия при обнаружении вредоносной 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. 66).

2. В левой части окна в разделе **Антивирусная защита** выберите подраздел **Мониторинг системы**.

   В правой части окна отобразятся параметры компонента **Мониторинг системы**.

3. В блоке **Действие при обнаружении угрозы** в раскрывающемся списке **При обнаружении вредоносной активности программы** выберите нужное действие:

   - **Выбирать действие автоматически**;
   - **Завершать работу вредоносной программы**;
   - **Пропускать**.

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

Включение и выключение отката действий вредоносных программ при лечении

Чтобы включить или выключить откат действий вредоносных программ при лечении, выполните следующие действия:

1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 66).

2. В левой части окна в разделе **Антивирусная защита** выберите подраздел **Мониторинг системы**.

   В правой части окна отобразятся параметры компонента **Мониторинг системы**.

3. Выполните одно из следующих действий:

   - Установите флажок **Выполнять откат действий вредоносных программ при лечении**, если вы хотите, чтобы при лечении вредоносных программ Kaspersky Endpoint Security выполнял откат действий, которые эти программы совершили в операционной системе.
   - Снимите флажок **Выполнять откат действий вредоносных программ при лечении**, если вы хотите, чтобы при лечении 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.

Сетевой экран

Этот раздел содержит информацию о Сетевом экране и инструкции о том, как настроить параметры компонента.

В этом разделе

О Сетевом экране

Во время работы в локальных сетях и интернете компьютер подвержен не только заражению вирусами и другими программами, представляющими угрозу, но и различного рода атакам, использующим уязвимости операционных систем и программного обеспечения.

Сетевой экран обеспечивает защиту персональных данных, хранящихся на компьютере пользователя, блокируя большинство возможных для операционной системы угроз в то время, когда компьютер подсоединен к интернету или к локальной сети. Сетевой экран позволяет обнаружить все сетевые соединения на компьютере пользователя и предоставить список их IP-адресов с указанием статуса сетевого соединения по умолчанию.

Компонент Сетевой экран фильтрует всю сетевую активность в соответствии с сетевыми правилами (см. раздел "О сетевых правилах" на стр. 143). Настройка сетевых правил позволяет вам задать нужный уровень защиты компьютера, от полной блокировки доступа в интернет для всех программ до разрешения неограниченного доступа.

Включение и выключение Сетевого экрана

По умолчанию Сетевой экран включен и работает в оптимальном режиме. При необходимости вы можете выключить Сетевой экран.

Включить и выключить компонент можно двумя способами:

- на закладке **Центр управления** главного окна программы (см. раздел "Главное окно программы" на стр. 64);
- из окна настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 66).

Чтобы включить или выключить Сетевой экран на закладке Центр управления главного окна программы, выполните следующие действия:

1. Откройте главное окно программы.
2. Выберите закладку **Центр управления**.
3. Нажмите клавишей мыши на блок **Управление защитой**.

   Блок **Управление защитой** раскроется.
4. По правой клавише мыши на строке **Сетевой экран** откройте контекстное меню действий с компонентом Сетевой экран.

5. Выполните одно из следующих действий:

   - Выберите в контекстном меню пункт **Включить**, если вы хотите включить Сетевой экран.

     Значок статуса работы компонента  , отображающийся слева в строке **Сетевой экран**, изменится на значок  .

   - Выберите в контекстном меню пункт **Выключить**, если вы хотите выключить Сетевой экран.

     Значок статуса работы компонента  , отображающийся слева в строке **Сетевой экран**, изменится на значок  .

Чтобы включить или выключить Сетевой экран из окна настройки параметров программы, выполните следующие действия:

1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 66).

2. В левой части окна в разделе **Антивирусная защита** выберите подраздел **Сетевой экран**.

   В правой части окна отобразятся параметры компонента Сетевой экран.

3. Выполните одно из следующих действий:

   - Установите флажок **Включить Сетевой экран**, если вы хотите включить Сетевой экран.

   - Снимите флажок **Включить Сетевой экран**, если вы хотите выключить Сетевой экран.

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

О сетевых правилах

Сетевое правило представляет собой разрешающее или запрещающее действие, которое Сетевой экран совершает, обнаружив попытку сетевого соединения.

Защиту от сетевых атак различного рода Сетевой экран осуществляет на двух уровнях: сетевом и прикладном. Защита на сетевом уровне обеспечивается за счет применения правил для сетевых пакетов. Защита на прикладном уровне обеспечивается за счет применения правил использования сетевых ресурсов программами, установленными на компьютере пользователя.

Исходя из двух уровней защиты Сетевого экрана, вы можете сформировать:

- *Сетевые пакетные правила*. Используются для ввода ограничений на сетевые пакеты независимо от программы. Такие правила ограничивают входящую и исходящую сетевую активность по определенным портам выбранного протокола передачи данных. Сетевой экран задает по умолчанию некоторые сетевые пакетные правила.

- *Сетевые правила программ*. Используются для ограничения сетевой активности конкретной программы. Учитываются не только характеристики сетевого пакета, но и конкретная программа, которой адресован этот сетевой пакет, либо которая инициировала отправку этого сетевого пакета. Такие правила позволяют тонко настраивать фильтрацию сетевой активности, например, когда определенный тип сетевых соединений запрещен для одних программ, но разрешен для других.

Сетевые пакетные правила имеют более высокий приоритет, чем сетевые правила программ. Если для одного и того же вида сетевой активности заданы и сетевые пакетные правила, и сетевые правила программ, то эта сетевая активность обрабатывается по сетевым пакетным правилам.

Вы можете установить для каждого сетевого пакетного правила и сетевого правила программы свой приоритет выполнения.

О статусах сетевого соединения

Сетевой экран контролирует все сетевые соединения на компьютере пользователя и автоматически присваивает статус каждому из обнаруженных сетевых соединений.

Выделены следующие статусы сетевого соединения:

- **Публичная сеть**. Этот статус разработан для сетей, не защищенных какими-либо антивирусными программами, сетевыми экранами, фильтрами (например, для сети

интернет-кафе). Пользователю компьютера, подключенного к такой сети, Сетевой экран закрывает доступ к файлам и принтерам этого компьютера. Сторонние пользователи также не могут получить доступ к информации через папки общего доступа и удаленный доступ к рабочему столу этого компьютера. Сетевой экран фильтрует сетевую активность каждой программы в соответствии с сетевыми правилами этой программы.

Сетевой экран по умолчанию присваивает статус *Публичная сеть* сети Интернет. Вы не можете изменить статус сети Интернет.

- **Локальная сеть**. Этот статус разработан для сетей, пользователям которых вы доверяете доступ к файлам и принтерам этого компьютера (например, для локальной сети организации или для домашней сети).

- **Доверенная сеть**. Этот статус разработан для безопасной сети, во время работы в которой компьютер не подвергается атакам и попыткам несанкционированного доступа к данным. Для сетей с этим статусом Сетевой экран разрешает любую сетевую активность в рамках этой сети.

Изменение статуса сетевого соединения

Чтобы изменить статус сетевого соединения, выполните следующие действия:

1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 66).

2. В левой части окна в разделе **Антивирусная защита** выберите подраздел **Сетевой экран**.

   В правой части окна отобразятся параметры компонента Сетевой экран.

3. Нажмите на кнопку **Доступные сети**.

   Откроется окно **Сетевой экран**.

4. Выберите сетевое соединение, статус которого вы хотите изменить.

5. В контекстном меню выберите статус сетевого соединения (см. раздел "О статусах сетевого соединения" на стр. 144):

- **Публичная сеть**.
- **Локальная сеть**.
- **Доверенная сеть**.

6. Нажмите на кнопку **ОК** в окне **Сетевой экран**.
7. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Работа с сетевыми пакетными правилами

Вы можете выполнить следующие действия в процессе работы с сетевыми пакетными правилами:

- Создать новое сетевое пакетное правило.

  Вы можете создать новое сетевое пакетное правило, сформировав набор условий и действий над сетевыми пакетами и потоками данных.

- Включить и выключить сетевое пакетное правило.

  Все сетевые пакетные правила, созданные Сетевым экраном по умолчанию, имеют статус *Включено*. Если сетевое пакетное правило включено, Сетевой экран применяет это правило.

  Вы можете выключить любое сетевое пакетное правило, выбранное в списке сетевых пакетных правил. Если сетевое пакетное правило выключено, Сетевой экран временно не применяет это правило.

  > Новое сетевое пакетное правило, созданное пользователем, по умолчанию добавляется в список сетевых пакетных правил со статусом *Включено*.

- Изменить параметры существующего сетевого пакетного правила.

  После того как вы создали новое сетевое пакетное правило, вы всегда можете вернуться к настройке его параметров и изменить нужные.

- Изменить действие Сетевого экрана для сетевого пакетного правила.

  В списке сетевых пакетных правил вы можете изменить действие, которое Сетевой экран выполняет, обнаружив сетевую активность указанного сетевого пакетного правила.

- Изменить приоритет сетевого пакетного правила.

  Вы можете повысить или понизить приоритет выбранного в списке сетевого пакетного правила.

- Удалить сетевое пакетное правило.

  Вы можете удалить сетевое пакетное правило, если вы не хотите, чтобы Сетевой экран применял это правило при обнаружении сетевой активности, и чтобы оно отображалось в списке сетевых пакетных правил со статусом *Выключено*.

В этом разделе

Создание и изменение сетевого пакетного правила

Создавая сетевые пакетные правила, следует помнить, что они имеют приоритет над сетевыми правилами программ.

Чтобы создать или изменить сетевое пакетное правило, выполните следующие действия:

1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 66).

2. В левой части окна в разделе **Антивирусная защита** выберите подраздел **Сетевой экран**.

3. Нажмите на кнопку **Сетевые пакетные правила**.

4. Откроется окно **Сетевой экран** на закладке **Сетевые пакетные правила**.

   На этой закладке представлен список сетевых пакетных правил, установленных Сетевым экраном по умолчанию.

5. Выполните одно из следующих действий:

   - Если хотите создать новое сетевое пакетное правило, нажмите на кнопку **Добавить**.

   - Если хотите изменить сетевое пакетное правило, выберите его в списке сетевых пакетных правил и нажмите на кнопку **Изменить**.

   Откроется окно **Сетевое правило**.

6. В раскрывающемся списке **Действие** выберите действие, которое должен выполнять Сетевой экран, обнаружив этот вид сетевой активности:

   - **Разрешать**.

   - **Запрещать**.

   - **По правилам программы**.

7. В поле **Название** укажите название сетевой службы одним из следующих способов:

   - Нажмите на значок , расположенный справа от поля **Название**, и в раскрывающемся списке выберите название сетевой службы.

     В раскрывающийся список входят сетевые службы, описывающие наиболее часто используемые сетевые соединения.

- В поле **Название** введите название сетевой службы вручную.

8. Укажите протокол передачи данных:

   a. Установите флажок **Протокол**.

   b. В раскрывающемся списке выберите тип протокола, по которому следует контролировать сетевую активность.

      Сетевой экран контролирует соединения по протоколам TCP, UDP, ICMP, ICMPv6, IGMP и GRE.

      Если сетевая служба выбрана в раскрывающемся списке **Название**, то флажок **Протокол** устанавливается автоматически и в раскрывающемся списке рядом с флажком выбирается тип протокола, который соответствует выбранной сетевой службе. По умолчанию флажок **Протокол** снят.

9. В раскрывающемся списке **Направление** выберите направление контролируемой сетевой активности.

   Сетевой экран контролирует сетевые соединения со следующими направлениями:

   - **Входящее (пакет)**.
   - **Входящее**.
   - **Входящее / Исходящее**.
   - **Исходящее (пакет)**.
   - **Исходящее**.

10. Если в качестве протокола выбран протокол ICMP или ICMPv6, вы можете задать тип и код ICMP-пакета:

    a. Установите флажок **ICMP-тип** и в раскрывающемся списке выберите тип ICMP-пакета.

b. Установите флажок **ICMP-код** и в раскрывающемся списке выберите код ICMP-пакета.

11. Если в качестве протокола выбран протокол TCP или UDP, вы можете через запятую указать номера портов компьютера пользователя и удаленного компьютера, соединение между которыми следует контролировать:

    a. В поле **Удаленные порты** введите порты удаленного компьютера.

    b. В поле **Локальные порты** введите порты компьютера пользователя.

12. В таблице **Сетевые адаптеры** укажите параметры сетевых адаптеров, с которых могут быть отправлены или которыми могут быть приняты сетевые пакеты. Для этого воспользуйтесь кнопками **Добавить**, **Изменить** и **Удалить**.

13. Если вы хотите ограничить контроль сетевых пакетов по времени их жизни (TTL, Time to Live), установите флажок **TTL** и в поле рядом укажите диапазон значений времени жизни передаваемых и / или получаемых сетевых пакетов.

    Сетевое правило будет контролировать передачу сетевых пакетов, у которых время жизни не превышает указанного значения.

    В противном случае снимите флажок **TTL**.

14. Укажите сетевые адреса удаленных компьютеров, которые могут передавать и / или получать сетевые пакеты. Для этого в раскрывающемся списке **Удаленные адреса** выберите одно из следующих значений:

    - **Любой адрес**. Сетевое правило контролирует отправку и / или получение сетевых пакетов удаленными компьютерами с любым IP-адресом.

    - **Адреса подсети**. Сетевое правило контролирует отправку и / или получение сетевых пакетов удаленными компьютерами с IP-адресами, относящимися к выбранному типу сети: **Доверенные сети**, **Локальные сети**, **Публичные сети**.

    - **Адреса из списка**. Сетевое правило контролирует отправку и / или получение сетевых пакетов удаленными компьютерами с IP-адресами, которые можно указать в списке ниже с помощью кнопок **Добавить**, **Изменить** и **Удалить**.

15. Укажите сетевые адреса компьютеров с установленной программой Kaspersky Endpoint Security, которые могут передавать и / или получать сетевые пакеты. Для этого в раскрывающемся списке **Локальные адреса** выберите одно из следующих значений:

    - **Любой адрес**. Сетевое правило контролирует отправку и / или получение сетевых пакетов компьютерами с установленной программой Kaspersky Endpoint Security и любым IP-адресом.

    - **Адреса из списка**. Сетевое правило контролирует отправку и / или получение сетевых пакетов компьютерами с установленной программой Kaspersky Endpoint Security и с IP-адресами, которые можно указать в списке ниже с помощью кнопок **Добавить**, **Изменить** и **Удалить**.

    Иногда для программ, работающих с сетевыми пакетами, не удается получить локальный адрес. В этом случае значение параметра **Локальные адреса** игнорируется.

16. Установите флажок **Записывать в отчет**, если вы хотите, чтобы действие сетевого правила было отражено в отчете (см. раздел "Работа с отчетами" на стр. 456).

17. Нажмите на кнопку **ОК** в окне **Сетевое правило**.

    Если вы создали новое сетевое правило, оно отобразится на закладке **Сетевые пакетные правила** окна **Сетевой экран**. По умолчанию новое сетевое правило помещается в конец списка сетевых пакетных правил.

18. Нажмите на кнопку **ОК** в окне **Сетевой экран**.

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

Включение и выключение сетевого пакетного правила

Чтобы включить или выключить сетевое пакетное правило, выполните следующие действия:

1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 66).

2. В левой части окна в разделе **Антивирусная защита** выберите подраздел **Сетевой экран**.

   В правой части окна отобразятся параметры компонента Сетевой экран.

3. Нажмите на кнопку **Сетевые пакетные правила**.

   Откроется окно **Сетевой экран** на закладке **Сетевые пакетные правила**.

4. Выберите в списке нужное сетевое пакетное правило.

5. Выполните одно из следующих действий:

   - Установите флажок рядом с названием сетевого пакетного правила, если вы хотите включить правило.

   - Снимите флажок рядом с названием сетевого пакетного правила, если вы хотите выключить правило.

6. Нажмите на кнопку **ОК**.

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

Изменение действия Сетевого экрана для сетевого пакетного правила

Чтобы изменить действие Сетевого экрана для сетевого пакетного правила, выполните следующие действия:

1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 66).

2. В левой части окна в разделе **Антивирусная защита** выберите подраздел **Сетевой экран**.

   В правой части окна отобразятся параметры компонента Сетевой экран.

3. Нажмите на кнопку **Сетевые пакетные правила**.

   Откроется окно **Сетевой экран** на закладке **Сетевые пакетные правила**.

4. Выберите в списке сетевое пакетное правило, для которого вы хотите изменить действие.

5. В графе **Разрешение** по правой клавише мыши откройте контекстное меню и выберите действие, которое вы хотите назначить:

   - **Разрешать**.
   - **Запрещать**.
   - **По правилу программы**.
   - **Записывать в отчет**.

6. Нажмите на кнопку **ОК** в окне **Сетевой экран**.

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

Изменение приоритета сетевого пакетного правила

Приоритет выполнения сетевого пакетного правила определяется его положением в списке сетевых пакетных правил. Первое сетевое пакетное правило в списке сетевых пакетных правил обладает самым высоким приоритетом.

Каждое сетевое пакетное правило, которое вы создали вручную, добавляется в конец списка сетевых пакетных правил и имеет самый низкий приоритет.

Сетевой экран выполняет правила в порядке их расположения в списке сетевых пакетных правил, сверху вниз. Согласно каждому обрабатываемому сетевому пакетному правилу, применяемому к определенному сетевому соединению, Сетевой экран либо разрешает,

либо блокирует сетевой доступ к адресу и порту, указанным в настройках этого сетевого соединения.

Чтобы изменить приоритет сетевого пакетного правила, выполните следующие действия:

1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 66).

2. В левой части окна в разделе **Антивирусная защита** выберите подраздел **Сетевой экран**.

   В правой части окна отобразятся параметры компонента Сетевой экран.

3. Нажмите на кнопку **Сетевые пакетные правила**.

   Откроется окно **Сетевой экран** на закладке **Сетевые пакетные правила**.

4. Выберите в списке сетевое пакетное правило, приоритет которого вы хотите изменить.

5. С помощью кнопок **Вверх** и **Вниз** переместите сетевое пакетное правило на нужную позицию в списке сетевых пакетных правил.

6. Нажмите на кнопку **ОК**.

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

Работа с сетевыми правилами программ

Kaspersky Endpoint Security по умолчанию группирует все программы, установленные на компьютере пользователя, по названию производителей программного обеспечения, файловую и сетевую активность которого он контролирует. Группы программ, в свою очередь, сгруппированы в группы доверия. Все программы и группы программ наследуют свойства своей родительской группы: правила контроля программ, сетевые правила программы, а также приоритет их выполнения.

Все программы, запускаемые на компьютере, Kaspersky Endpoint Security распределяет на группы доверия. Программы распределяются на группы доверия в зависимости от степени угрозы, которую эти программы могут представлять для операционной системы.

Существуют следующие группы доверия:

- **Доверенные**. В группу входят программы, для которых выполняется одно или более следующих условий:
  - программы обладают цифровой подписью доверенных производителей,
  - о программах есть записи в базе доверенных программ Kaspersky Security Network,
  - пользователь поместил программы в группу "Доверенные".

  Запрещенных операций для таких программ нет.
- **Слабые ограничения**. В группу входят программы, для которых выполняются следующие условия:
  - программы не обладают цифровой подписью доверенных производителей,
  - о программах нет записей в базе доверенных программ Kaspersky Security Network,
  - степень угрозы программ характеризуется индексом меньше 80,
  - 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,

- степень угрозы программ характеризуется индексом в диапазоне 81-90,
- 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,
  - степень угрозы программ характеризуется индексом в диапазоне 91-100,
  - пользователь поместил программы в группу "Недоверенные".

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

Как и компонент Контроль активности программ (см. раздел "Предотвращение вторжений" на стр. 207), компонент Сетевой экран по умолчанию применяет сетевые правила группы программ для фильтрации сетевой активности всех помещенных в группу программ. Сетевые правила группы программ определяют, какими правами доступа к различным сетевым соединениям обладают программы, входящие в эту группу.

Сетевой экран по умолчанию создает набор сетевых правил для каждой группы программ, которые Kaspersky Endpoint Security обнаружил на компьютере. Вы можете изменить действие Сетевого экрана для сетевых правил группы программ, созданных по умолчанию. Вы не можете изменить, удалить или выключить сетевые правила группы программ, созданные по умолчанию, а также изменить их приоритет.

Вы также можете создать сетевое правило для отдельной программы. Такое правило будет иметь более высокий приоритет, чем сетевое правило группы, в которую входит эта программа.

Вы можете выполнить следующие действия в процессе работы с сетевыми правилами программ:

- Создать новое сетевое правило.

  Вы можете создать новое сетевое правило, в соответствии с которым Сетевой экран должен регулировать сетевую активность программы или программ, входящих в выбранную группу программ.

- Включить и выключить сетевое правило.

  Все сетевые правила добавляются в список сетевых правил программ со статусом *Включено*. Если сетевое правило включено, Сетевой экран применяет это правило.

  Вы можете выключить сетевое правило, созданное вручную. Если сетевое правило выключено, Сетевой экран временно не применяет это правило.

- Изменить параметры сетевого правила.

  После того как вы создали новое сетевое правило, вы всегда можете вернуться к настройке его параметров и изменить нужные.

- Изменить действие Сетевого экрана для сетевого правила.

  В списке сетевых правил вы можете изменить действие для сетевого правила, которое Сетевой экран выполняет, обнаружив сетевую активность этой программы или группы программ.

- Изменить приоритет сетевого правила.

  Вы можете повысить или понизить приоритет созданного вручную сетевого правила.

- Удалить сетевое правило.

  Вы можете удалить созданное вручную сетевое правило, если вы не хотите, чтобы Сетевой экран применял это сетевое правило к выбранной программе или группе

программ при обнаружении сетевой активности, и чтобы оно отображалось в списке сетевых правил программ.

В этом разделе

Создание и изменение сетевого правила программ

Чтобы создать или изменить сетевое правило группы программ, выполните следующие действия:

1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 66).
2. В левой части окна в разделе **Антивирусная защита** выберите подраздел **Сетевой экран**.
3. Нажмите на кнопку **Сетевые правила программ**.

   Откроется окно **Сетевой экран** на закладке **Правила контроля программ**.
4. В списке программ выберите программу или группу программ, для которой вы хотите создать или изменить сетевое правило.
5. По правой клавише мыши откройте контекстное меню и в зависимости от того, что вам нужно сделать, выберите пункт **Правила программы** или **Правила группы**.

Откроется окно **Правила контроля программы** или **Правила контроля группы программ**.

6. В открывшемся окне выберите закладку **Сетевые правила**.
7. Выполните одно из следующих действий:
   - Если хотите создать новое сетевое правило, нажмите на кнопку **Добавить**.
   - Если хотите изменить сетевое правило, выберите его в списке сетевых правил и нажмите на кнопку **Изменить**.

   Откроется окно **Сетевое правило**.
8. В раскрывающемся списке **Действие** выберите действие, которое должен выполнять Сетевой экран, обнаружив этот вид сетевой активности:
   - **Разрешать**.
   - **Запрещать**.
9. В поле **Название** укажите название сетевой службы одним из следующих способов:
   - Нажмите на значок  , расположенный справа от поля **Название**, и в раскрывающемся списке выберите название сетевой службы.

     В раскрывающийся список входят сетевые службы, описывающие наиболее часто используемые сетевые соединения.
   - В поле **Название** введите название сетевой службы вручную.
10. Укажите протокол передачи данных:

    a. Установите флажок **Протокол**.

    b. В раскрывающемся списке выберите тип протокола, по которому должен производиться контроль сетевой активности.

    Сетевой экран контролирует соединения по протоколам TCP, UDP, ICMP, ICMPv6, IGMP и GRE.

Если сетевая служба выбрана в раскрывающемся списке **Название**, то флажок **Протокол** устанавливается автоматически и в раскрывающемся списке рядом с флажком выбирается тип протокола, который соответствует выбранной сетевой службе. По умолчанию флажок **Протокол** снят.

11. В раскрывающемся списке **Направление** выберите направление контролируемой сетевой активности.

    Сетевой экран контролирует сетевые соединения со следующими направлениями:

    - **Входящее**.
    - **Входящее / Исходящее**.
    - **Исходящее**.

12. Если в качестве протокола выбран протокол ICMP или ICMPv6, вы можете задать тип и код ICMP-пакета:

    a. Установите флажок **ICMP-тип** и в раскрывающемся списке выберите тип ICMP-пакета.

    b. Установите флажок **ICMP-код** и в раскрывающемся списке выберите код ICMP-пакета.

13. Если в качестве протокола выбран протокол TCP или UDP, вы можете через запятую указать номера портов компьютера пользователя и удаленного компьютера, соединение между которыми следует контролировать:

    a. В поле **Удаленные порты** введите порты удаленного компьютера.

    b. В поле **Локальные порты** введите порты компьютера пользователя.

14. Укажите сетевые адреса удаленных компьютеров, которые могут передавать и / или получать сетевые пакеты. Для этого в раскрывающемся списке **Удаленные адреса** выберите одно из следующих значений:

    - **Любой адрес**. Сетевое правило контролирует отправку и / или получение сетевых пакетов удаленными компьютерами с любым IP-адресом.

- **Адреса подсети**. Сетевое правило контролирует отправку и / или получение сетевых пакетов удаленными компьютерами с IP-адресами, относящимися к выбранному типу сети: **Доверенные сети**, **Локальные сети**, **Публичные сети**.

- **Адреса из списка**. Сетевое правило контролирует отправку и / или получение сетевых пакетов удаленными компьютерами с IP-адресами, которые можно указать в списке ниже с помощью кнопок **Добавить**, **Изменить** и **Удалить**.

15. Укажите сетевые адреса компьютеров с установленной программой Kaspersky Endpoint Security, которые могут передавать и / или получать сетевые пакеты. Для этого в раскрывающемся списке **Локальные адреса** выберите одно из следующих значений:

    - **Любой адрес**. Сетевое правило контролирует отправку и / или получение сетевых пакетов компьютерами с установленной программой Kaspersky Endpoint Security и любым IP-адресом.

    - **Адреса из списка**. Сетевое правило контролирует отправку и / или получение сетевых пакетов компьютерами с установленной программой Kaspersky Endpoint Security и с IP-адресами, которые можно указать в списке ниже с помощью кнопок **Добавить**, **Изменить** и **Удалить**.

    > Иногда для программ, работающих с сетевыми пакетами, не удается получить локальный адрес. В этом случае значение параметра **Локальные адреса** игнорируется.

16. Установите флажок **Записывать в отчет**, если вы хотите, чтобы действие сетевого правила было отражено в отчете (см. раздел "Работа с отчетами" на стр. 456).

17. Нажмите на кнопку **ОК** в окне **Сетевое правило**.

    Если вы создали новое сетевое правило, оно отобразится на закладке **Сетевые правила**.

18. Нажмите на кнопку **ОК** в окне **Правила контроля группы программ**, если правило предназначено для группы программ, или в окне **Правила контроля программы**, если правило предназначено для программы.

19. Нажмите на кнопку **ОК** в окне **Сетевой экран**.

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

Включение и выключение сетевого правила программ

Чтобы включить или выключить сетевое правило программ, выполните следующие действия:

1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 66).

2. В левой части окна в разделе **Антивирусная защита** выберите подраздел **Сетевой экран**.

   В правой части окна отобразятся параметры компонента Сетевой экран.

3. Нажмите на кнопку **Сетевые правила программ**.

   Откроется окно **Сетевой экран** на закладке **Правила контроля программ**.

4. В списке выберите программу или группу программ, для которой вы хотите включить или выключить сетевое правило.

5. По правой клавише мыши откройте контекстное меню и в зависимости от того, что вам нужно сделать, выберите пункт **Правила программы** или **Правила группы**.

   Откроется окно **Правила контроля программы** или **Правила контроля группы программ**.

6. В открывшемся окне выберите закладку **Сетевые правила**.

7. В списке сетевых правил группы программ выберите нужное вам сетевое правило.

8. Выполните одно из следующих действий:

   - Установите флажок рядом с названием сетевого правила, если вы хотите включить правило.

- Снимите флажок рядом с названием сетевого правила, если вы хотите выключить правило.

  Вы не можете выключить сетевое правило группы программ, если оно создано Сетевым экраном по умолчанию.

9. Нажмите на кнопку **ОК** в окне **Правила контроля группы программ**, если правило предназначено для группы программ, или в окне **Правила контроля программы**, если правило предназначено для программы.

10. Нажмите на кнопку **ОК** в окне **Сетевой экран**.

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

Изменение действия Сетевого экрана для сетевого правила программ

Вы можете изменить действие Сетевого экрана для всех сетевых правил программы или группы программ, которые были созданы по умолчанию, а также изменить действие Сетевого экрана для одного сетевого правила программы или группы программ, которое было создано вручную.

Чтобы изменить действие Сетевого экрана для всех сетевых правил программы или группы программ, выполните следующие действия:

1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 66).

2. В левой части окна в разделе **Антивирусная защита** выберите подраздел **Сетевой экран**.

   В правой части окна отобразятся параметры компонента Сетевой экран.

3. Нажмите на кнопку **Сетевые правила программ**.

   Откроется окно **Сетевой экран** на закладке **Правила контроля программ**.

4. В списке выберите программу или группу программ, если вы хотите изменить действие Сетевого экрана для всех ее сетевых правил, созданных по умолчанию. Сетевые правила, созданные вручную, останутся без изменений.

5. В графе **Сеть** по левой клавише мыши откройте контекстное меню и выберите действие, которое вы хотите назначить:

   - **Наследовать**.
   - **Разрешать**.
   - **Запрещать**.

6. Нажмите на кнопку **ОК**.

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

Чтобы изменить действие Сетевого экрана для одного сетевого правила программы или группы программ, выполните следующие действия:

1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 66).

2. В левой части окна в блоке **Антивирусная защита** выберите раздел **Сетевой экран**.

   В правой части окна отобразятся параметры компонента Сетевой экран.

3. Нажмите на кнопку **Сетевые правила программ**.

   Откроется окно **Сетевой экран** на закладке **Правила контроля программ**.

4. В списке выберите программу или группу программ, для которой вы хотите изменить действие одного сетевого правила.

5. По правой клавише мыши откройте контекстное меню и в зависимости от того, что вам нужно сделать, выберите пункт **Правила программы** или **Правила группы**.

   Откроется окно **Правила контроля программы** или **Правила контроля группы программ**.

6. В открывшемся окне выберите закладку **Сетевые правила**.

7. Выберите сетевое правило, для которого вы хотите изменить действие Сетевого экрана.

8. В графе **Разрешение** по правой клавише мыши откройте контекстное меню и выберите действие, которое вы хотите назначить:

   - **Разрешать**.
   - **Запрещать**.
   - **Записывать в отчет**.

9. Нажмите на кнопку **ОК** в окне **Правила контроля группы программ**, если правило предназначено для группы программ, или в окне **Правила контроля программы**, если правило предназначено для программы.

10. Нажмите на кнопку **ОК** в окне **Сетевой экран**.

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

Изменение приоритета сетевого правила программ

Приоритет выполнения сетевого правила определяется его положением в списке сетевых правил. Сетевой экран выполняет правила в порядке их расположения в списке сетевых правил, сверху вниз. Согласно каждому обрабатываемому сетевому правилу, применяемому к определенному сетевому соединению, Сетевой экран либо разрешает, либо блокирует сетевой доступ к адресу и порту, указанным в настройках этого сетевого соединения.

Созданные вручную сетевые правила имеют более высокий приоритет, чем сетевые правила, созданные по умолчанию.

Вы не можете изменить приоритет сетевых правил группы программ, созданных по умолчанию.

Чтобы изменить приоритет сетевого правила, выполните следующие действия:

1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 66).

2. В левой части окна в разделе **Антивирусная защита** выберите подраздел **Сетевой экран**.

   В правой части окна отобразятся параметры компонента Сетевой экран.

3. Нажмите на кнопку **Сетевые правила программ**.

   Откроется окно **Сетевой экран** на закладке **Правила контроля программ**.

4. В списке программ выберите программу или группу программ, для которой вы хотите изменить приоритет сетевого правила.

5. По правой клавише мыши откройте контекстное меню и в зависимости от того, что вам нужно сделать, выберите пункт **Правила программы** или **Правила группы**.

   Откроется окно **Правила контроля программы** или **Правила контроля группы программ**.

6. В открывшемся окне выберите закладку **Сетевые правила**.

7. Выберите сетевое правило, приоритет которого вы хотите изменить.

8. С помощью кнопок **Вверх** и **Вниз** переместите сетевое правило на нужную позицию в списке сетевых правил.

9. Нажмите на кнопку **ОК** в окне **Правила контроля группы программ**, если правило предназначено для группы программ, или в окне **Правила контроля программы**, если правило предназначено для программы.

10. Нажмите на кнопку **ОК** в окне **Сетевой экран**.

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

Мониторинг сети

Этот раздел содержит информацию о мониторинге сети и инструкцию о том, как запустить мониторинг сети.

В этом разделе

О мониторинге сети

Мониторинг сети - это инструмент, предназначенный для просмотра информации о сетевой активности компьютера пользователя в реальном времени.

Запуск мониторинга сети

Чтобы запустить мониторинг сети, выполните следующие действия:

1. Откройте главное окно программы (на стр. 64).
2. Выберите закладку **Центр управления**.
3. Нажмите клавишей мыши на блок **Управление защитой**.

   Блок **Управление защитой** раскроется.
4. По правой клавише мыши на строке **Сетевой экран** откройте контекстное меню действий с компонентом Сетевой экран.
5. В контекстном меню выберите пункт **Мониторинг сети**.

   Откроется окно **Мониторинг сети**. В этом окне информация о сетевой активности компьютера пользователя представлена на четырех закладках:

- На закладке **Сетевая активность** отображаются все активные на текущий момент сетевые соединения с компьютером пользователя. Приводятся как сетевые соединения, инициированные компьютером пользователя, так и входящие сетевые соединения.

- На закладке **Открытые порты** перечислены все открытые сетевые порты на компьютере пользователя.

- На закладке **Сетевой трафик** отображается объем входящего и исходящего сетевого трафика между компьютером пользователя и другими компьютерами сети, в которой пользователь работает в текущий момент.

- На закладке **Заблокированные компьютеры** представлен список IP-адресов удаленных компьютеров, сетевую активность которых компонент Защита от сетевых атак заблокировал, обнаружив попытку сетевой атаки с этого IP-адреса.

Защита от сетевых атак

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

В этом разделе

О Защите от сетевых атак

Компонент Защита от сетевых атак 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.

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 атак, пополняется в процессе обновления баз и модулей программы (см. раздел "Об обновлении баз и модулей программы" на стр. 397).

Включение и выключение Защиты от сетевых атак

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

Включить и выключить компонент можно двумя способами:

- на закладке **Центр управления** главного окна программы (см. раздел "Главное окно программы" на стр. 64);
- из окна настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 66).

Чтобы включить или выключить Защиту от сетевых атак на закладке Центр управления главного окна программы, выполните следующие действия:

1. Откройте главное окно программы.
2. Выберите закладку **Центр управления**.
3. Нажмите клавишей мыши на блок **Управление защитой**.

   Блок **Управление защитой** раскроется.
4. По правой клавише мыши на строке **Защита от сетевых атак** откройте контекстное меню действий с компонентом Защита от сетевых атак.

5. Выполните одно из следующих действий:

   - Выберите в контекстном меню пункт **Включить**, если вы хотите включить Защиту от сетевых атак.

     Значок статуса работы компонента , отображающийся слева в строке **Защита от сетевых атак**, изменится на значок .

   - Выберите в контекстном меню пункт **Выключить**, если вы хотите выключить Защиту от сетевых атак.

     Значок статуса работы компонента , отображающийся слева в строке **Защита от сетевых атак**, изменится на значок .

Чтобы включить или выключить Защиту от сетевых атак из окна настройки параметров программы, выполните следующие действия:

1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 66).

2. В левой части окна в разделе **Антивирусная защита** выберите подраздел **Защита от сетевых атак**.

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

3. Выполните следующие действия:

   - Установите флажок **Включить Защиту от сетевых атак**, если вы хотите включить Защиту от сетевых атак.

   - Снимите флажок **Включить Защиту от сетевых атак**, если вы хотите выключить Защиту от сетевых атак.

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

Настройка Защиты от сетевых атак

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

- 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. 66).

2. В левой части окна в разделе **Антивирусная защита** выберите подраздел **Защита от сетевых атак**.

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

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

   Если этот флажок установлен, то, обнаружив попытку сетевой атаки, компонент Защита от сетевых атак 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 атак 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. 66).

2. В левой части окна в разделе **Антивирусная защита** выберите подраздел **Защита от сетевых атак**.

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

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.

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 программа не находится под политикой 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. 85).

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. 30), 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 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. 66).

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. 66).

2. В левой части окна в разделе **Антивирусная 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**, если вы хотите запретить использование экранной клавиатуры при авторизации.

   - Снимите флажок **Запретить использование экранной клавиатуры для авторизации**, если вы хотите разрешить использование экранной клавиатуры при 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 запуска программ

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

В этом разделе

О Контроле запуска программ

Компонент Контроль запуска программ отслеживает попытки запуска программ пользователями и регулирует запуск программ с помощью *правил Контроля запуска программ* (см. раздел "*О правилах Контроля запуска программ*" на стр. 183).

Запуск программ, параметры которых не удовлетворяют ни одному из правил Контроля запуска программ, регулируется выбранным режимом работы компонента. По умолчанию

выбран *режим Черный список* (см. раздел "*О режимах работы Контроля запуска программ*" на стр. 197). Этот режим разрешает любым пользователям запускать любые программы.

Все попытки запуска программ пользователями фиксируются в отчетах (см. раздел "Работа с отчетами" на стр. 456).

Включение и выключение Контроля запуска программ

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

Включить и выключить компонент можно двумя способами:

- на закладке **Центр управления** главного окна программы (см. раздел "Главное окно программы" на стр. 64);
- из окна настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 66).

Чтобы включить или выключить Контроль запуска программ на закладке Центр управления главного окна программы, выполните следующие действия:

1. Откройте главное окно программы.
2. Выберите закладку **Центр управления**.
3. Нажмите клавишей мыши на блок **Контроль рабочего места**.

   Блок **Контроль рабочего места** раскроется.
4. По правой клавише мыши откройте контекстное меню строки с информацией о компоненте Контроль запуска программ.

   Откроется меню действий с компонентом.
5. Выполните одно из следующих действий:
   - Выберите в меню пункт **Включить**, если вы хотите включить Контроль запуска программ.

Значок статуса работы компонента  , отображающийся слева в строке **Контроль запуска программ**, изменится на значок  .

- Выберите в меню пункт **Выключить**, если вы хотите выключить Контроль запуска программ.

  Значок статуса работы компонента  , отображающийся слева в строке **Контроль запуска программ**, изменится на значок  .

Чтобы включить или выключить Контроль запуска программ из окна настройки параметров программы, выполните следующие действия:

1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 66).

2. В левой части окна в разделе **Контроль рабочего места** выберите подраздел **Контроль запуска программ**.

   В правой части окна отобразятся параметры компонента Контроль запуска программ.

3. Выполните одно из следующих действий:

   - Установите флажок **Включить Контроль запуска программ**, если вы хотите включить Контроль запуска программ.

   - Снимите флажок **Включить Контроль запуска программ**, если вы хотите выключить Контроль запуска программ.

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

Ограничения функциональности Контроля запуска программ

Работа компонента Контроль запуска программ ограничена в следующих случаях:

- При обновлении версии программы импорт параметров компонента Контроль запуска программ не поддерживается.

Для восстановления работоспособности Контроля запуска 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. Если в локальных базах отсутствует информация о программе, то для такой программы не будет определена категория, то есть программа не будет помещена в группу доверия.

  Результат категоризации программ при наличии соединения с серверами KSN может отличаться от результата категоризации, выполненной 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 запуска 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:

- { cCmdLineParser::itCmd, _T("%ComSpec%") };
- { cCmdLineParser::itReg, _T("%SystemRoot%\\system32\\reg.exe") };
- { cCmdLineParser::itRegedit, _T("%SystemRoot%\\system32\\regedit.exe") };
- { cCmdLineParser::itRegedit, _T("%SystemRoot%\\regedit.exe") };
- { cCmdLineParser::itRegedit, _T("%SystemRoot%\\system32\\regedt32.exe") };
- { cCmdLineParser::itCWScript, _T("%SystemRoot%\\system32\\cscript.exe") };
- { cCmdLineParser::itCWScript, _T("%SystemRoot%\\system32\\wscript.exe") };
- { cCmdLineParser::itMsiexec, _T("%SystemRoot%\\system32\\msiexec.exe") };
- { cCmdLineParser::itMmc, _T("%SystemRoot%\\system32\\mmc.exe") };
- { cCmdLineParser::itMshta, _T("%SystemRoot%\\system32\\mshta.exe") };
- { cCmdLineParser::itRundll, _T("%SystemRoot%\\system32\\rundll32.exe") };
- { cCmdLineParser::itMetro, _T("%SystemRoot%\\system32\\wwahost.exe") };
- { cCmdLineParser::itCmd, _T("%SystemRoot%\\syswow64\\cmd.exe") };
- { cCmdLineParser::itReg, _T("%SystemRoot%\\syswow64\\reg.exe") };
- { cCmdLineParser::itRegedit, _T("%SystemRoot%\\syswow64\\regedit.exe") };
- { cCmdLineParser::itRegedit, _T("%SystemRoot%\\syswow64\\regedt32.exe") };
- { cCmdLineParser::itCWScript, _T("%SystemRoot%\\syswow64\\cscript.exe") };
- { cCmdLineParser::itCWScript, _T("%SystemRoot%\\syswow64\\wscript.exe") };
- { cCmdLineParser::itMsiexec, _T("%SystemRoot%\\syswow64\\msiexec.exe") };
- { cCmdLineParser::itMmc, _T("%SystemRoot%\\syswow64\\mmc.exe") };
- { cCmdLineParser::itMshta, _T("%SystemRoot%\\syswow64\\mshta.exe") };
- { cCmdLineParser::itRundll, _T("%SystemRoot%\\syswow64\\rundll32.exe") };

- { cCmdLineParser::itMetro, _T("%SystemRoot%\\syswow64\\wwahost.exe") }.

О правилах Контроля запуска программ

Kaspersky Endpoint Security контролирует запуск программ пользователями с помощью правил. В правиле Контроля запуска программ содержатся условия срабатывания и действие компонента Контроль запуска 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.

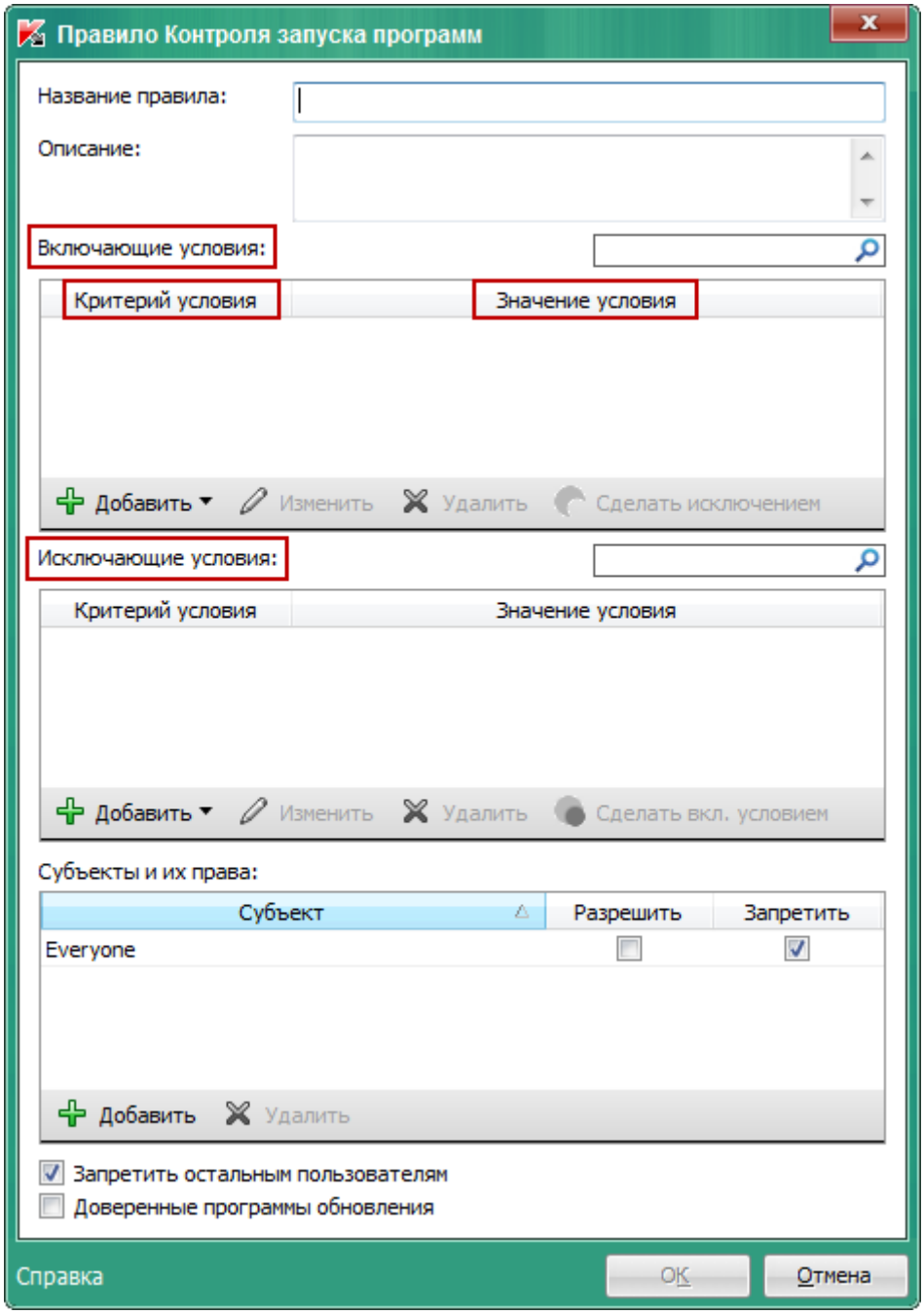


Figure 2: Правило контроля запуска программ. Параметры условия срабатывания правила

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 запуска программ выполняет действие, прописанное в правиле. Если параметры программы соответствуют значениям критериев, указанных в исключающем условии, Контроль запуска программ не контролирует запуск программы.

Решения компонента Контроль запуска программ при срабатывании правила

При срабатывании правила Контроль запуска 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 запуска программы и для одного из пользователей этой группы назначено запрещающее правило Контроля запуска программы, то этому пользователю будет запрещен запуск программы.

Статус работы правила

Правила Контроля запуска программ могут иметь два статуса работы:

- **Вкл.**

  Статус работы правила означает, что правило включено.

- **Выкл.**

  Статус работы правила означает, что правило выключено.

Правила Контроля запуска программ по умолчанию

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

Вы можете выполнить следующие действия с правилами Контроля запуска программ:

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

Правило Контроля запуска программ может быть включено (флажок напротив правила установлен) или выключено (флажок напротив правила снят). По умолчанию после создания правило Контроля запуска программ включено.

- Удалить правило.

В этом разделе

Добавление и изменение правила Контроля запуска программ

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

1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 66).

2. В левой части окна в разделе **Контроль рабочего места** выберите подраздел **Контроль запуска программ**.

   В правой части окна отобразятся параметры компонента Контроль запуска программ.

3. Установите флажок **Включить Контроль запуска 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 запуска 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 запуска программ" на стр. 190) 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 запуска программ (см. раздел "О режимах работы Контроля запуска программ" на стр. 197).

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 запускать другие программы, для которых не определены правила контроля запуска.

6. Нажмите на кнопку **OK**.

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

Добавление условия срабатывания в правило Контроля запуска программ

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

1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 66).

2. В левой части окна в разделе **Контроль рабочего места** выберите подраздел **Контроль запуска программ**.

   В правой части окна отобразятся параметры компонента Контроль запуска программ.

3. Установите флажок **Включить Контроль запуска 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 запуска 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 **ОК**.

   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 запуска 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 запуска 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.

3. Нажмите на кнопку **OK**.

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

1. В раскрывающемся списке кнопки **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 символьные ссылки в поле **Путь к файлу или папке**, рекомендуется развернуть символьные ссылки для корректной работы правила Контроля запуска 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 кнопки **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 запуска программ

Чтобы изменить статус правила Контроля запуска программ, выполните следующие действия:

1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 66).

2. В левой части окна в разделе **Контроль рабочего места** выберите подраздел **Контроль запуска программ**.

   В правой части окна отобразятся параметры компонента Контроль запуска программ.

3. Установите флажок **Включить Контроль запуска программ**, чтобы параметры компонента стали доступными для изменения.

4. Выберите правило, статус которого вы хотите изменить.

5. В графе **Статус** выполните следующие действия:

   - Если вы хотите включить использование правила, установите флажок напротив этого правила.

   - Если вы хотите выключить использование правила, снимите флажок напротив этого правила.

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

Тестирование правил Контроля запуска программ

Чтобы убедиться, что правила Контроля запуска 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 запуска программ требуется изучить события о работе компонента Контроль запуска 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 запуска программ выключен.

Чтобы протестировать правила Контроля запуска программ, выполните следующие действия:

1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 66).

2. В левой части окна в разделе **Контроль рабочего места** выберите подраздел **Контроль запуска программ**.

   В правой части окна отобразятся параметры компонента Контроль запуска программ.

3. Установите флажок **Включить Контроль запуска программ**, чтобы параметры компонента стали доступными для изменения.

4. В раскрывающемся списке **Режим Контроля запуска 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 запуска программ, но будет отправлять уведомления об их запуске на Сервер администрирования.

Изменение шаблонов сообщений Контроля запуска программ

Когда пользователь пытается запустить программу, запрещенную правилом Контроля запуска 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. 66).
2. В левой части окна в разделе **Контроль рабочего места** выберите подраздел **Контроль запуска программ**.

   В правой части окна отобразятся параметры компонента Контроль запуска программ.

3. Установите флажок **Включить Контроль запуска 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 запуска программ

Компонент Контроль запуска программ может работать в двух режимах:

- **Черный список**. Режим, при котором Контроль запуска программ разрешает всем пользователям запуск любых программ, кроме тех, которые указаны в запрещающих правилах Контроля запуска программ (см. раздел "О правилах Контроля запуска программ" на стр. 183).

  Этот режим работы Контроля запуска программ установлен по умолчанию.

- **Белый список**. Режим, при котором Контроль запуска программ запрещает всем пользователям запуск любых программ, кроме тех, которые указаны в разрешающих правилах Контроля запуска программ.

Если разрешающие правила Контроля запуска 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.

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 запуска программ.

Настройка Контроля запуска 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. 203).

  Правила Контроля запуска 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. 202).

Поэтому настройку работы компонента Контроль запуска программ рекомендуется выполнять с помощью Kaspersky Security Center.

Выбор режима Контроля запуска программ

Чтобы выбрать режим Контроля запуска программ, выполните следующие действия:

1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 66).

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.

     При выборе этого режима по умолчанию создается два правила Контроля программ: **Операционная система и ее компоненты** и **Доверенные программы обновления**. Вы не можете удалить эти правила. Параметры этих правил недоступны для изменения. Вы можете включить или выключить работу этих правил, установив или сняв флажок напротив правила. 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 запуска программ**.

5. В раскрывающемся списке **Действие** выберите, какое действие компонент должен выполнять при попытке пользователя запустить программу, запрещенную правилами Контроля запуска 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.

   Если флажок установлен, то контроль DLL-модулей и драйверов также осуществляется до запуска Kaspersky Endpoint Security. Чтобы в дальнейшем контроль всех DLL-модулей и драйверов работал до запуска программы, перезагрузите компьютер после установки флажка **Контролировать DLL и драйверы**. Если у вас нет возможности перезагрузить компьютер, то после установки флажка **Контролировать DLL и драйверы** вы можете загрузить DLL-модули и драйверы при запущенной программе Kaspersky Endpoint Security. В этом случае контроль вступит в действие только для DLL-модулей и драйверов, загруженных при запущенной программе 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. Использование функции **Контролировать DLL и драйверы** при отсутствии таких разрешающих правил может привести к нестабильности системы.

Правила контроля, 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 запуска программ с помощью Kaspersky Security Center

Этот раздел содержит информацию о настройке Контроля запуска программ с помощью Kaspersky Security Center и рекомендации по оптимальному использованию Контроля запуска программ.

В этом разделе

Получение информации о программах, которые установлены на компьютерах пользователей

Для создания оптимальных правил Контроля запуска 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 (см. раздел "О задачах для Kaspersky Endpoint Security" на стр. 524).

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.

Создание категорий программ

Для удобства формирования правил вы можете создать категории программ и использовать их при создании правил Контроля запуска 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.

Создание правил Контроля запуска программ с помощью Kaspersky Security Center

Чтобы создать правило Контроля запуска 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 рабочего места** выберите подраздел **Контроль запуска программ**.

   В правой части окна отобразятся параметры компонента Контроль запуска программ.

7. Нажмите на кнопку **Добавить**.

   Откроется окно **Правило контроля запуска программ**.

8. Из раскрывающегося списка **Категория** выберите созданную категорию программ, на основе которой вы хотите создать правило.

9. Задайте список пользователей и / или групп пользователей, для которых вы хотите настроить возможность запускать программы, принадлежащие к выбранной категории. Для этого в таблице **Субъекты и их права** нажмите на кнопку **Добавить**.

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

10. 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** напротив этих пользователей.
    - Если вы хотите запретить пользователям и / или группам пользователей запуск программ, принадлежащих к выбранной категории, установите флажок **Запретить** напротив этих пользователей.

11. 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**.

12. Установите флажок **Доверенные программы обновления**, если вы хотите, чтобы программы из категории, указанной в правиле, Kaspersky Endpoint Security считал доверенными программами обновления с правом запускать другие программы, для которых не определены правила контроля запуска.

13. Нажмите на кнопку **OK**.

14. Нажмите на кнопку **Применить** в разделе **Контроль запуска программ** окна свойств политики.

Изменение статуса правила Контроля запуска программ с помощью Kaspersky Security Center

Чтобы изменить статус правила Контроля запуска 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 рабочего места** выберите подраздел **Контроль запуска программ**.

   В правой части окна отобразятся параметры компонента Контроль запуска программ.

7. Выберите правило Контроля запуска программ, статус которого вы хотите изменить.
8. В графе **Статус** выполните одно из следующих действий:
    - Если вы хотите включить использование правила, установите флажок напротив этого правила.
    - Если вы хотите выключить использование правила, снимите флажок напротив этого правила.
9. Нажмите на кнопку **Применить**.

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 (см. раздел "Аппаратные и программные требования" на стр. 24).

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 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 программ представляют собой набор ограничений для различных действий программ в операционной системе и прав доступа к ресурсам компьютера.

Сетевую активность программ контролирует компонент Сетевой экран.

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

Для более эффективной работы Контроля активности программ вам рекомендуется принять участие в Kaspersky Security Network (см. раздел "Участие в Kaspersky Security Network" на стр. 544). Данные, полученные с помощью Kaspersky Security Network, позволяют точнее относить программы к той или иной группе доверия, а также применять оптимальные правила контроля программ.

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

Ограничения контроля аудио и видео устройств

О защите аудиосигнала

Функциональность защиты аудиосигнала имеет следующие особенности:

- Для работы функциональности необходимо, чтобы был включен компонент Контроль активности программ.

- Если программа начала получать аудиосигнал до запуска компонента Контроль активности программ, 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 Контроля активности программ) 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 Контроль активности программ включен и работает в рекомендованном специалистами "Лаборатории Касперского" режиме. Вы можете выключить Контроль активности программ при необходимости.

Включить и выключить компонент можно двумя способами:

- на закладке **Центр управления** главного окна программы (см. раздел "Главное окно программы" на стр. 64);
- из окна настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 66).

Чтобы включить или выключить Контроль активности программ на закладке Центр управления главного окна программы, выполните следующие действия:

1. Откройте главное окно программы.
2. Выберите закладку **Центр управления**.
3. Нажмите клавишей мыши на блок **Контроль рабочего места**.

   Блок **Контроль рабочего места** раскроется.
4. По правой клавише мыши откройте контекстное меню строки с информацией о компоненте Контроль активности программ.

   Откроется меню действий с компонентом.
5. Выполните одно из следующих действий:
   - Выберите в меню пункт **Включить**, если вы хотите включить Контроль активности программ.

     Значок статуса работы компонента  , отображающийся слева в строке Контроль активности программ, изменится на значок  .

- Выберите в меню пункт **Выключить**, если вы хотите выключить Контроль активности программ.

  Значок статуса работы компонента  , отображающийся слева в строке Контроль активности программ, изменится на значок  .

Чтобы включить или выключить Контроль активности программ из окна настройки параметров программы, выполните следующие действия:

1. Откройте окно настройки параметров программы.
2. В левой части окна в разделе **Контроль рабочего места** выберите подраздел **Контроль активности программ**.

   В правой части окна отобразятся параметры компонента Контроль активности программ.
3. В правой части окна выполните одно из следующих действий:

   - Установите флажок **Включить Контроль активности программ**, если вы хотите включить Контроль активности программ.
   - Снимите флажок **Включить Контроль активности программ**, если вы хотите выключить Контроль активности программ.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Работа с группами доверия программ

Во время первого запуска каждой программы компонент Контроль активности программ проверяет безопасность программы и помещает программу в одну из групп доверия.

Все программы, запускаемые на компьютере, Kaspersky Endpoint Security распределяет на группы доверия. Программы распределяются на группы доверия в зависимости от степени угрозы, которую эти программы могут представлять для операционной системы.

Существуют следующие группы доверия:

- **Доверенные**. В группу входят программы, для которых выполняется одно или более следующих условий:

- программы обладают цифровой подписью доверенных производителей,
- о программах есть записи в базе доверенных программ Kaspersky Security Network,
- пользователь поместил программы в группу "Доверенные".

Запрещенных операций для таких программ нет.

- **Слабые ограничения**. В группу входят программы, для которых выполняются следующие условия:
  - программы не обладают цифровой подписью доверенных производителей,
  - о программах нет записей в базе доверенных программ Kaspersky Security Network,
  - степень угрозы программ характеризуется индексом меньше 80,
  - 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,
  - степень угрозы программ характеризуется индексом в диапазоне 81-90,
  - 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,
- степень угрозы программ характеризуется индексом в диапазоне 91-100,
- 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. 544) (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 базах KSN изменилась.

Чтобы распределять по группам доверия неизвестные программы, Kaspersky Endpoint Security по умолчанию использует эвристический анализ. В процессе эвристического анализа Kaspersky Endpoint Security определяет степень угрозы программы. На основании степени угрозы программы Kaspersky Endpoint Security помещает программу в ту или иную группу доверия. Вместо использования эвристического анализа вы можете указать 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 пользователем в окне **Выбор группы доверия** (см. раздел "**Выбор группы доверия для программ, запускаемых до Kaspersky Endpoint Security**" на стр. 218).

Контролируется только сетевая активность программ, запущенных до Kaspersky Endpoint Security, согласно сетевым правилам, установленным в параметрах Сетевого экрана.

По умолчанию Kaspersky Endpoint Security проверяет программу в течение 30 секунд. Если по истечении этого времени определение степени угрозы программы не завершено,

Kaspersky Endpoint Security помещает программу в группу доверия "Слабые ограничения" и продолжает определять степень угрозы программы в фоновом режиме. Затем Kaspersky Endpoint Security помещает программу в подходящую группу доверия. Вы можете изменить время, которое отводится для проверки степени угрозы запускаемых программ. Если вы уверены, что все запускаемые на компьютере пользователя программы не представляют угрозы для его безопасности, то время, отведенное для определения степени угрозы программы, можно уменьшить. Если же вы устанавливаете на компьютер пользователя программы, в безопасности которых вы не уверены, время определения степени угрозы программ рекомендуется увеличить.

Если степень угрозы программы высока, то Kaspersky Endpoint Security уведомляет пользователя об этом и предлагает выбрать группу доверия, в которую следует поместить эту программу. Уведомление содержит статистику использования этой программы участниками Kaspersky Security Network. На основании этой статистики, а также зная историю появления программы на компьютере, пользователь может принять более обоснованное решение о том, в какую группу доверия следует поместить эту программу.

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 Контроля активности программ.

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. 66).

2. В левой части окна в разделе **Контроль рабочего места** выберите подраздел **Контроль активности программ**.

   В правой части окна отобразятся параметры компонента Контроль активности программ.

3. Если вы хотите автоматически помещать программы с цифровой подписью в группу доверия "Доверенные", установите флажок **Доверять программам, имеющим цифровую подпись**.

4. Выберите способ распределения неизвестных программ по группам доверия:

   - Если вы хотите использовать эвристический анализ для распределения неизвестных программ по группам доверия, выберите вариант **Использовать эвристический анализ для определения группы** и укажите время, которое отводится для проверки запускаемой программы, в поле **Максимальное время определения группы**.

   - Если вы хотите помещать все неизвестные программы в указанную группу доверия, выберите вариант **Автоматически помещать в группу** и выберите нужную группу доверия из раскрывающегося списка.

     > В целях безопасности группа **Доверенные** не включена в значения параметра **Автоматически помещать в группу**.

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 отдельной программы.

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. 66).

2. В левой части окна в разделе **Контроль рабочего места** выберите подраздел **Контроль активности программ**.

   В правой части окна отобразятся параметры компонента Контроль активности программ.

3. Нажмите на кнопку **Программы**.

   Откроется закладка **Правила контроля программ** окна **Программы**.

4. На закладке **Правила контроля 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 **ОК**.

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

Выбор группы доверия для программ, запускаемых до Kaspersky Endpoint Security

Контролируется только сетевая активность программ, запущенных до Kaspersky Endpoint Security. Контроль осуществляется согласно сетевым правилам, установленным в параметрах Сетевого экрана (см. раздел "Создание и изменение сетевого правила программ" на стр. 158). 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. 66).
2. В левой части окна в разделе **Контроль рабочего места** выберите подраздел **Контроль активности программ**.

   В правой части окна отобразятся параметры компонента Контроль активности программ.
3. Нажмите на кнопку **Изменить**.

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

Работа с правилами контроля программ

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

контроля программ для всей группы доверия, для отдельной программы или группы программ внутри группы доверия.

Правила контроля программ, определенные для отдельных программ или групп программ внутри группы доверия, имеют более высокий приоритет, чем правила контроля 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 Контроль активности программ 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 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. 66).

2. В левой части окна в разделе **Контроль рабочего места** выберите подраздел **Контроль активности программ**.

   В правой части окна отобразятся параметры компонента Контроль активности программ.

3. Нажмите на кнопку **Программы**.

   Откроется закладка **Правила контроля программ** окна **Контроль активности программ**.

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. 66).
2. В левой части окна в разделе **Контроль рабочего места** выберите подраздел **Контроль активности программ**.

   В правой части окна отобразятся параметры компонента Контроль активности программ.

3. Нажмите на кнопку **Программы**.

Откроется закладка **Правила контроля программ** окна **Контроль активности программ**.

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 **Правила контроля 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 **ОК**.
10. В окне **Программы** нажмите на кнопку **ОК**.

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. 66).

2. В левой части окна в разделе **Контроль рабочего места** выберите подраздел **Контроль активности программ**.

   В правой части окна отобразятся параметры компонента Контроль активности программ.

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, Контроль активности программ 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. 66).

2. В левой части окна в разделе **Контроль рабочего места** выберите подраздел **Контроль активности программ**.

   В правой части окна отобразятся параметры компонента Контроль активности программ.

3. Нажмите на кнопку **Программы**.

Откроется закладка **Правила контроля программ** окна **Контроль активности программ**.

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. 66).
2. В левой части окна в разделе **Контроль рабочего места** выберите подраздел **Контроль активности программ**.

   В правой части окна отобразятся параметры компонента Контроль активности программ.
3. Нажмите на кнопку **Программы**.

   Откроется закладка **Правила контроля программ** окна **Контроль активности программ**.

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. 66).
2. В левой части окна в разделе **Контроль рабочего места** выберите подраздел **Контроль активности программ**.

   В правой части окна отобразятся параметры компонента Контроль активности программ.
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 Контроль активности программ 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. 66).

2. В левой части окна в разделе **Контроль рабочего места** выберите подраздел **Контроль активности программ**.

   В правой части окна отобразятся параметры компонента Контроль активности программ.

3. Нажмите на кнопку **Ресурсы**.

   Откроется закладка **Защищаемые ресурсы** окна **Контроль активности программ**.

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 **Контроль активности программ** 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. 66).

2. В левой части окна в разделе **Контроль рабочего места** выберите подраздел **Контроль активности программ**.

   В правой части окна отобразятся параметры компонента Контроль активности программ.

3. Нажмите на кнопку **Ресурсы**.

   Откроется закладка **Защищаемые ресурсы** окна **Контроль активности программ**.

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 **Контроль активности программ** 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. 66).

2. В левой части окна в разделе **Контроль рабочего места** выберите подраздел **Контроль активности программ**.

   В правой части окна отобразятся параметры компонента Контроль активности программ.

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

   Откроется закладка **Защищаемые ресурсы** окна **Контроль активности программ**.

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 Контроль активности программ: **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 Контроль активности программ.

e. Нажмите на кнопку **OK**.

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

В списке ресурсов, исключенных из защиты компонента Контроль активности программ, появится новый элемент.

> После того как вы добавили ресурс в список исключений из защиты компонентом Контроль активности программ, 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 **Контроль активности программ** нажмите на кнопку **OK**.

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

Мониторинг уязвимостей

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 Мониторинге уязвимостей и инструкции о том, как включить или выключить компонент.

В этом разделе

О Мониторинге уязвимостей

Компонент Мониторинг уязвимостей в режиме реального времени проверяет на уязвимости программы, запущенные на компьютере пользователя, а также программы в момент их запуска. Если вы используете компонент Мониторинг уязвимостей, не нужно запускать задачу поиска уязвимостей. Такая проверка актуальна, если задача поиска уязвимостей (см. раздел "О задаче поиска уязвимостей" на стр. 437) в установленных на компьютере пользователя программах не выполнялась или выполнялась давно.

Включение и выключение Мониторинга уязвимостей

По умолчанию компонент Мониторинг уязвимостей выключен. Вы можете включить Мониторинг уязвимостей при необходимости.

Включить и выключить компонент можно двумя способами:

- на закладке **Центр управления** главного окна программы (см. раздел "Главное окно программы" на стр. 64);
- из окна настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 66).

Чтобы включить или выключить Мониторинг уязвимостей на закладке Центр управления главного окна программы, выполните следующие действия:

1. Откройте главное окно программы (на стр. 64).
2. Выберите закладку **Центр управления**.
3. Нажмите клавишей мыши на блок **Контроль рабочего места**.

   Блок **Контроль рабочего места** раскроется.
4. По правой клавише мыши откройте контекстное меню строки с информацией о компоненте Мониторинг уязвимостей.

   Откроется меню действий с компонентом.
5. Выполните одно из следующих действий:
   - Выберите в меню пункт **Включить**, если вы хотите включить Мониторинг уязвимостей.

     Значок статуса работы компонента  , отображающийся слева в строке **Мониторинг уязвимостей**, изменится на значок  .
   - Выберите в меню пункт **Выключить**, если вы хотите выключить Мониторинг уязвимостей.

Значок статуса работы компонента  , отображающийся слева в строке **Мониторинг уязвимостей**, изменится на значок  .

Чтобы включить или выключить Мониторинг уязвимостей из окна настройки параметров программы, выполните следующие действия:

1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 66).

2. В левой части окна в разделе **Контроль рабочего места** выберите подраздел **Мониторинг уязвимостей**.

   В правой части окна отобразятся параметры компонента Мониторинг уязвимостей.

3. В правой части окна выполните одно из следующих действий:

   - Установите флажок **Включить Мониторинг уязвимостей**, если вы хотите, чтобы Kaspersky Endpoint Security проверял на уязвимости программы, запущенные на компьютере пользователя, а также программы в момент их запуска.

   - Снимите флажок **Включить Мониторинг уязвимостей**, если вы хотите, чтобы Kaspersky Endpoint Security не проверял на уязвимости программы, запущенные на компьютере пользователя, а также программы в момент их запуска.

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

Контроль устройств

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 (см. раздел "Аппаратные и программные требования" на стр. 24).

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

В этом разделе

О Контроле устройств

Контроль устройств обеспечивает безопасность конфиденциальных данных путем ограничения доступа пользователей к устройствам, установленным или подключенным к компьютеру:

- устройствам памяти (жесткие диски, съемные диски, ленточные накопители, CD/DVD-приводы);

- инструментам передачи информации (модемы, внешние сетевые карты);
- инструментам превращения информации в твердую копию (принтеры);
- шинам подключения (далее также "шинам") - интерфейсам, с помощью которых устройства подключаются к компьютеру (например, USB, FireWire, Infrared).

Контроль устройств регулирует доступ пользователей к устройствами с помощью *правил доступа к устройствам* (далее также "правил доступа") и *правил доступа к шинам подключения* (далее также "правил доступа к шинам").

Включение и выключение Контроля устройств

По умолчанию Контроль устройств включен. Вы можете выключить Контроль устройств при необходимости.

Включить и выключить компонент можно двумя способами:

- на закладке **Центр управления** главного окна программы (см. раздел "Главное окно программы" на стр. 64);
- из окна настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 66).

*Чтобы включить или выключить Контроль устройств на закладке **Центр управления** главного окна программы, выполните следующие действия:*

1. Откройте главное окно программы.
2. Выберите закладку **Центр управления**.
3. Нажмите клавишей мыши на блок **Контроль рабочего места**.

   Блок **Контроль рабочего места** раскроется.
4. По правой клавише мыши откройте контекстное меню строки с информацией о компоненте Контроль устройств.

   Откроется меню действий с компонентом.

5. Выполните одно из следующих действий:

   - Выберите в меню пункт **Включить**, если вы хотите включить Контроль устройств.
   - Выберите в меню пункт **Выключить**, если вы хотите выключить Контроль устройств.

Чтобы включить или выключить Контроль устройств из окна настройки параметров программы, выполните следующие действия:

1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 66).
2. В левой части окна в разделе **Контроль рабочего места** выберите подраздел **Контроль устройств**.

   В правой части окна отобразятся параметры компонента Контроль устройств.
3. Выполните одно из следующих действий:

   - Установите флажок **Включить Контроль устройств**, если вы хотите включить Контроль устройств.
   - Снимите флажок **Включить Контроль устройств**, если вы хотите выключить Контроль устройств.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

О правилах доступа к устройствам и шинам подключения

Правило доступа к устройствам представляет собой набор параметров, которые определяют следующие функции компонента Контроль устройств:

- Разрешение выбранным пользователям и / или группам пользователей доступа к типам устройств в определенные интервалы времени.

  Вы можете выбрать пользователя и / или группу пользователей и создать для них расписание доступа к устройствам.

- Установка права на чтение содержимого устройств памяти.
- Установка права на изменение содержимого устройств памяти.

По умолчанию для всех типов устройств из классификации компонента Контроль устройств созданы правила доступа, которые разрешают полный доступ к устройствам всем пользователям в любое время, если разрешен доступ к шинам подключения для соответствующих типов устройств.

Правило доступа к шине подключения представляет собой разрешение или запрет на доступ к шине подключения.

Для всех шин подключения из классификации компонента Контроль устройств по умолчанию созданы правила, разрешающие доступ к шинам.

Вы не можете создавать и удалять правила доступа к устройствам и правила доступа к шинам подключения, вы можете только изменять их.

О доверенных устройствах

Доверенные устройства - это устройства, полный доступ к которым разрешен в любое время для пользователей, указанных в параметрах доверенного устройства.

Для работы с доверенными устройствами доступны следующие действия:

- добавление устройства в список доверенных устройств;
- изменение пользователя и / или группы пользователей, которым разрешен доступ к доверенному устройству;
- удаление устройства из списка доверенных устройств.

> Если устройство добавлено в список доверенных устройств, а для устройств этого типа создано правило доступа, запрещающее или ограничивающее доступ, то при принятии решения о доступе к устройству наличие устройства в списке доверенных устройств имеет более высокий приоритет, чем правило доступа.

Типовые решения о доступе к устройствам

Kaspersky Endpoint Security принимает решение о доступе к устройству после того, как пользователь подключил это устройство к компьютеру.

Таблица 1. Типовые решения о доступе к устройствам

№	Исходные условия	Промежуточные шаги до принятия решения о доступе к устройству			Решение о доступе к устройств
		Проверка наличия устройства в списке доверенных устройств	Проверка доступа к устройству на основании правила доступа	Проверка доступа к шине на основании правила доступа к шине	

1	Устройства нет в классификации компонента Контроль устройств.	Нет в списке доверенных устройств.	Нет правила доступа.	Не проверяется.	Доступ разрешен.
2	Устройство является доверенным.	Есть в списке доверенных устройств.	Не проверяется.	Не проверяется.	Доступ разрешен.
3	Доступ к устройству разрешен.	Нет в списке доверенных устройств.	Доступ разрешен.	Не проверяется.	Доступ разрешен.
4	Доступ к устройству зависит от шины.	Нет в списке доверенных устройств.	Доступ зависит от шины.	Доступ разрешен.	Доступ разрешен.
5	Доступ к устройству зависит от шины.	Нет в списке доверенных устройств.	Доступ зависит от шины.	Доступ запрещен.	Доступ запрещен.
6	Доступ к устройству разрешен. Правило доступа к шине отсутствует.	Нет в списке доверенных устройств.	Доступ разрешен.	Нет правила доступа к шине.	Доступ разрешен.
7	Доступ к устройству запрещен.	Нет в списке доверенных устройств.	Доступ запрещен.	Не проверяется.	Доступ запрещен.
8	Правило доступа к устройству и правило доступа к шине отсутствуют.	Нет в списке доверенных устройств.	Нет правила доступа.	Нет правила доступа к шине.	Доступ разрешен.

9	Правило доступа к устройству отсутствует.	Нет в списке доверенных устройств.	Нет правила доступа.	Доступ разрешен.	Доступ разрешен.
10	Правило доступа к устройству отсутствует.	Нет в списке доверенных устройств.	Нет правила доступа.	Доступ запрещен.	Доступ запрещен.

Вы можете изменить правило доступа к устройству после подключения устройства. Если устройство было подключено и правило доступа разрешало доступ к устройству, а после вы изменили правило доступа и запретили доступ к устройству, то при очередном обращении к устройству за какой-либо файловой операцией (просмотр дерева каталогов, чтение, запись) Kaspersky Endpoint Security блокирует доступ. Блокирование устройства без файловой системы произойдет только при последующем подключении устройства.

Если пользователю компьютера с установленной программой Kaspersky Endpoint Security требуется запросить доступ к устройству, которое, по его мнению, было заблокировано ошибочно, передайте ему инструкцию по запросу доступа (см. раздел "Получение доступа к заблокированному устройству" на стр. 257).

Изменение правила доступа к устройствам

В зависимости от типа устройства вы можете изменять разные параметры доступа: список пользователей, получающих доступ к устройству, расписание доступа и разрешение / запрет на доступ.

Чтобы изменить правило доступа к устройствам, выполните следующие действия:

1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 66).

2. В левой части окна в разделе **Контроль рабочего места** выберите подраздел **Контроль устройств**.

В правой части окна отобразятся параметры компонента Контроль устройств.

3. В правой части окна выберите закладку **Типы устройств**.

   На закладке **Типы устройств** находятся правила доступа для всех устройств, которые есть в классификации компонента Контроль устройств.

4. Выберите правило доступа, которое хотите изменить.

5. Нажмите на кнопку **Изменить**. Кнопка доступна только для тех типов устройств, которые имеют файловую систему.

   Откроется окно **Настройка правила доступа к устройствам**.

   По умолчанию правило доступа к устройствам разрешает полный доступ к типу устройств всем пользователям в любое время. Такое правило доступа в списке **Пользователи и / или группы пользователей** содержит группу **Все**, а в таблице **Права выделенной группы пользователей по расписаниям доступа** содержит расписание доступа к устройствам **Расписание по умолчанию** с установленными правами на все возможные операции с устройствами.

6. Измените параметры правила доступа к устройствам:

   a. Выберите пользователя и / или группу пользователей в списке **Пользователи и / или группы пользователей**.

   Для изменения списка **Пользователи и / или группы пользователей** используйте кнопки **Добавить**, **Изменить**, **Удалить**.

   b. В таблице **Права выделенной группы пользователей по расписаниям доступа** настройте расписание доступа к устройствам для выбранного пользователя и / или группы пользователей. Для этого установите флажки около названий тех расписаний доступа к устройствам, которые вы хотите использовать в изменяемом правиле доступа к устройствам.

   Для изменения списка расписаний доступа к устройствам используйте кнопки **Создать**, **Изменить**, **Копировать**, **Удалить** в таблице **Права выделенной группы пользователей по расписаниям доступа**.

c. Для каждого расписания доступа к устройствам, используемого в изменяемом правиле, задайте операции, которые разрешаются при работе с устройствами. Для этого в таблице **Права выделенной группы пользователей по расписаниям доступа** установите флажки в графах с названиями нужных операций.

d. Нажмите на кнопку **ОК**.

После того как вы изменили исходные значения параметров правила доступа к устройствам, параметр доступа к типу устройств в графе **Доступ** в таблице на закладке **Типы устройств** принимает значение *Ограничивать правилами*.

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

Включение и выключение записи событий в журнал

Запись событий в журнал доступна только для операций с файлами на съемных дисках.

Чтобы включить или выключить запись событий в журнал, выполните следующие действия:

1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 66).

2. В левой части окна в разделе **Контроль рабочего места** выберите подраздел **Контроль устройств**.

   В правой части окна отобразятся параметры компонента Контроль устройств.

3. В правой части окна выберите закладку **Типы устройств**.

   На закладке **Типы устройств** находятся правила доступа для всех устройств, которые есть в классификации компонента Контроль устройств.

4. Выберите в таблице устройств **Съемные диски**.

   В верхней части таблицы станет доступной кнопка **Запись событий в журнал**.

5. Нажмите на кнопку **Запись событий в журнал**.

   Откроется окно **Параметры записи событий в журнал**.

6. Выполните одно из следующих действий:

   - Если вы хотите включить запись событий об операциях записи и удаления файлов на съемных дисках, установить флажок **Включить запись событий в журнал**.

     Kaspersky Endpoint Security будет сохранять событие в файл журнала и отправлять сообщение на Сервер администрирования Kaspersky Security Center, когда пользователь совершает операции записи или удаления с файлами на съемных дисках.

   - В противном случае снимите флажок **Включить запись событий в журнал**.

7. Укажите, информация о каких операциях должна записываться в журнал. Для этого выполните одно из следующих действий:

   - Если вы хотите, чтобы Kaspersky Endpoint Security записывал в журнал все события, установите флажок **Сохранять информацию обо всех файлах**.

   - Если вы хотите, чтобы Kaspersky Endpoint Security записывал в журнал только информацию о файлах определенного формата, в блоке **Фильтр по форматам файлов** установите флажки напротив нужных форматов файлов.

8. Укажите, о действиях каких пользователей Kaspersky Endpoint Security будет формировать события журнала. Для этого выполните следующие действия:

   a. В блоке **Пользователи** нажмите на кнопку **Выбрать**.

      Откроется стандартное окно Microsoft Windows **Выбор пользователей или групп**.

   b. Задайте или измените список пользователей и / или групп пользователей.

   Когда пользователи, указанные в блоке **Пользователи**, будут производить запись в файлы, расположенные на съемных дисках, или удалять файлы со съемных дисков, Kaspersky Endpoint Security будет сохранять информацию о совершенной операции в

журнал событий и отправлять сообщение на Сервер администрирования Kaspersky Security Center.

9. Нажмите на кнопку **ОК** в окне **Параметры записи событий в журнал**.

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

Вы можете просмотреть события, связанные с файлами на съемных дисках, в Консоли администрирования Kaspersky Security Center в рабочей области для узла **Сервер администрирования** на закладке **События**. Чтобы события отображались в локальном журнале событий Kaspersky Endpoint Security, требуется установить флажок **Выполнена операция с файлом** в параметрах уведомлений (см. раздел "Настройка параметров журналов событий" на стр. 468) для компонента Контроль устройств.

Добавление сети Wi-Fi в список доверенных

Вы можете разрешить пользователям подключаться к сетям Wi-Fi, которые вы считаете безопасными, например, к корпоративной сети Wi-Fi. Для этого нужно добавить эту сеть в список доверенных сетей Wi-Fi. Контроль устройств будет блокировать доступ ко всем сетям Wi-Fi, кроме тех, которые указаны в списке доверенных.

Чтобы добавить сеть Wi-Fi в список доверенных, выполните следующие действия:

1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 66).

2. В левой части окна в разделе **Контроль рабочего места** выберите подраздел **Контроль устройств**.

   В правой части окна отобразятся параметры компонента Контроль устройств.

3. В правой части окна выберите закладку **Типы устройств**.

   На закладке **Типы устройств** находятся правила доступа для всех устройств, которые есть в классификации компонента Контроль устройств.

4. В графе **Доступ** напротив устройства **Wi-Fi** вызовите контекстное меню по правой клавише мыши.

5. Выберите пункт **Запрещать с исключениями**.

6. В списке устройств выберите **Wi-Fi** и нажмите на кнопку **Изменить**.

   Откроется окно **Доверенные сети Wi-Fi**.

7. Нажмите на кнопку **Добавить**.

   Откроется окно **Доверенная сеть Wi-Fi**.

8. В окне **Доверенная сеть Wi-Fi** выполните следующие действия:

   - В поле **Имя сети** укажите имя сети Wi-Fi, которую вы хотите добавить в список доверенных.
   - В раскрывающемся списке **Тип аутентификации** выберите тип аутентификации, используемый при подключении к доверенной сети Wi-Fi.
   - В раскрывающемся списке **Тип шифрования** выберите тип шифрования, используемый для защиты трафика доверенной сети Wi-Fi.
   - В поле **Комментарий** вы можете указать любую информацию о добавленной сети Wi-Fi.

   > Сеть Wi-Fi считается доверенной, если ее параметры соответствуют всем параметрам, указанным в правиле.

9. Нажмите на кнопку **ОК** в окне **Доверенная сеть Wi-Fi**.

10. Нажмите на кнопку **ОК** в окне **Доверенные сети Wi-Fi**.

Изменение правила доступа к шине подключения

Чтобы изменить правило доступа к шине подключения, выполните следующие действия:

1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 66).

2. В левой части окна в разделе **Контроль рабочего места** выберите подраздел **Контроль устройств**.

   В правой части окна отобразятся параметры компонента Контроль устройств.

3. Выберите закладку **Шины подключения**.

   На закладке **Шины подключения** находятся правила доступа для всех шин подключения, которые есть в классификации компонента Контроль устройств.

4. Выберите правило доступа к шине, которое хотите изменить.

5. Измените значение параметра доступа:

   - Чтобы разрешить доступ к шине подключения, в графе **Доступ** вызовите контекстное меню и выберите пункт **Разрешать**.

   - Чтобы запретить доступ к шине подключения, в графе **Доступ** вызовите контекстное меню и выберите пункт **Запрещать**.

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

Действия с доверенными устройствами

Этот раздел содержит информацию о действиях с доверенными устройствами.

В этом разделе

Добавление устройства в список доверенных из интерфейса программы

По умолчанию при добавлении устройства в список доверенных устройств доступ к устройству разрешается всем пользователям (группе пользователей "Все").

Чтобы добавить устройство в список доверенных из интерфейса программы, выполните следующие действия:

1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 66).

2. В левой части окна в разделе **Контроль рабочего места** выберите подраздел **Контроль устройств**.

   В правой части окна отобразятся параметры компонента Контроль устройств.

3. В правой части окна выберите закладку **Доверенные устройства**.

4. Нажмите на кнопку **Выбрать**.

   Откроется окно **Выбор доверенных устройств**.

5. Установите флажок напротив названия устройства, которое вы хотите добавить в список доверенных устройств.

Список устройств в графе **Устройства** зависит от того, какое значение выбрано в раскрывающемся списке **Отображать подключенные устройства**.

6. Нажмите на кнопку **Выбрать**.

   Откроется окно Microsoft Windows **Выбор пользователей или групп**.

7. В окне Microsoft Windows **Выбор пользователей или групп** задайте пользователей и / или группы пользователей, для которых Kaspersky Endpoint Security распознает выбранные устройства как доверенные.

   Имена пользователей и / или групп пользователей, заданных в окне Microsoft Windows **Выбор пользователей или групп**, отобразятся в поле **Разрешать пользователям и / или группам пользователей**.

8. В окне **Выбор доверенных устройств** нажмите на кнопку **ОК**.

   В таблице на закладке **Доверенные устройства** окна настроек компонента **Контроль устройств** появится строка с параметрами добавленного доверенного устройства.

9. Повторите пункты 4-7 для каждого устройства, которое вы хотите добавить в список доверенных устройств для определенных пользователей и / или групп пользователей.

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

Добавление устройств в список доверенных по их модели или идентификатору

По умолчанию при добавлении устройства в список доверенных устройств доступ к устройству разрешается всем пользователям (группе пользователей "Все").

Чтобы добавить устройства в список доверенных по их модели или идентификатору, 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 сформировать список доверенных устройств.

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 рабочего места** выберите подраздел **Контроль устройств**.

7. В правой части окна выберите закладку **Доверенные устройства**.

8. Нажмите на кнопку **Добавить**.

   Откроется контекстное меню кнопки.

9. В контекстном меню кнопки **Добавить** выполните одно из следующих действий:

   - Выберите пункт **Устройства по идентификатору**, если для добавления в список доверенных устройств вы хотите выбирать устройства, для которых известны их уникальные идентификаторы.

   - Выберите пункт **Устройства по модели**, если вы хотите добавить в список доверенные устройства, для которых известны VID (идентификатор производителя) и PID (идентификатор продукта).

10. В открывшемся окне в раскрывающемся списке **Тип устройств** выберите тип устройств для вывода в таблице ниже.

11. Нажмите на кнопку **Обновить**.

    В таблице отобразится список устройств, для которых известны их идентификаторы и/или модели и которые отнесены к типу, указанному в раскрывающемся списке **Тип устройств**.

12. Установите флажки напротив названий устройств, которые вы хотите добавить в список доверенных устройств.

13. Нажмите на кнопку **Выбрать**.

    Откроется окно Microsoft Windows **Выбор пользователей или групп**.

14. В окне Windows **Выбор пользователей или групп** задайте пользователей и / или группы пользователей, для которых Kaspersky Endpoint Security распознает выбранные устройства как доверенные.

    Имена пользователей и / или групп пользователей, заданных в окне Microsoft Windows **Выбор пользователей или групп**, отобразятся в поле **Разрешать пользователям и / или группам пользователей**.

15. Нажмите на кнопку **OK**.

    В таблице на закладке **Доверенные устройства** отобразятся строки с параметрами добавленных доверенных устройств.

16. Нажмите на кнопку **OK** или **Применить**, чтобы сохранить внесенные изменения.

Добавление устройств в список доверенных по маске их идентификатора

По умолчанию при добавлении устройства в список доверенных устройств доступ к устройству разрешается всем пользователям (группе пользователей "Все").

> Добавление устройств в список доверенных по маске их идентификатора возможно только в Консоли администрирования Kaspersky Security Center.

Чтобы добавить устройства в список доверенных по маске их идентификатора, 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 сформировать список доверенных устройств.

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 рабочего места** выберите подраздел **Контроль устройств**.

7. В правой части окна выберите закладку **Доверенные устройства**.

8. Нажмите на кнопку **Добавить**.

   Откроется контекстное меню кнопки.

9. В контекстном меню кнопки **Добавить** выберите пункт **Устройства по маске идентификатора**.

   Откроется окно **Добавление доверенных устройств по маске идентификатора**.

10. В окне **Добавление доверенных устройств по маске идентификатора** в поле **Маска** введите маску для идентификаторов устройств.

11. Нажмите на кнопку **Выбрать**.

    Откроется окно Microsoft Windows **Выбор пользователей или групп**.

12. В окне Microsoft Windows **Выбор пользователей или групп** задайте пользователей и / или группы пользователей, для которых Kaspersky Endpoint Security распознает устройства, модели или идентификаторы которых удовлетворяют заданной маске, как доверенные.

Имена пользователей и / или групп пользователей, заданных в окне Microsoft Windows **Выбор пользователей или групп**, отобразятся в поле **Разрешать пользователям и / или группам пользователей**.

13. Нажмите на кнопку **OK**.

    В таблице на закладке **Доверенные устройства** окна параметров компонента **Контроль устройств** появится строка с параметрами правила добавления устройств в список доверенных по маске их идентификаторов.

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

Настройка доступа пользователей к доверенному устройству

По умолчанию при добавлении устройства в список доверенных устройств доступ к устройству разрешается всем пользователям (группе пользователей "Все"). Вы можете настроить доступ пользователей (и групп пользователей) к доверенному устройству.

Чтобы настроить доступ пользователей к доверенному устройству, выполните следующие действия:

1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 66).

2. В левой части окна в разделе **Контроль рабочего места** выберите подраздел **Контроль устройств**.

   В правой части окна отобразятся параметры компонента Контроль устройств.

3. В правой части окна выберите закладку **Доверенные устройства**.

4. В списке доверенных устройств выберите устройство, правила доступа к которому вы хотите изменить.

5. Нажмите на кнопку **Изменить**.

   Откроется окно **Настройка правила доступа к доверенным устройствам**.

6. Нажмите на кнопку **Выбрать**.

Откроется окно Microsoft Windows **Выбор пользователей или групп**.

7. В окне Microsoft Windows **Выбор пользователей или групп** задайте пользователей и / или группы пользователей, для которых Kaspersky Endpoint Security распознает выбранные устройства как доверенные.

8. Нажмите на кнопку **OK**.

   Имена пользователей и / или групп пользователей, заданных в окне Microsoft Windows **Выбор пользователей или групп**, отобразятся в поле **Разрешать пользователям и / или группам пользователей** окна **Настройка правила доступа к доверенным устройствам**.

9. Нажмите на кнопку **OK**.

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

Удаление устройства из списка доверенных устройств

Чтобы удалить устройство из списка доверенных устройств, выполните следующие действия:

1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 66).

2. В левой части окна в разделе **Контроль рабочего места** выберите подраздел **Контроль устройств**.

   В правой части окна отобразятся параметры компонента Контроль устройств.

3. В правой части окна выберите закладку **Доверенные устройства**.

4. Выберите устройство, которое вы хотите удалить из списка доверенных устройств.

5. Нажмите на кнопку **Удалить**.

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

Решение о доступе к устройству, которое вы удалили из списка доверенных устройств, Kaspersky Endpoint Security принимает на основании правил доступа к устройствам и правил доступа к шинам подключения.

Изменение шаблонов сообщений Контроля устройств

Когда пользователь пытается обратиться к заблокированному устройству, Kaspersky Endpoint Security выводит сообщение о блокировке доступа к устройству или о запрете операции над содержимым устройства. Если блокировка доступа к устройству или запрет операции с содержимым устройства, по мнению пользователя, произошел ошибочно, пользователь может отправить сообщение администратору локальной сети организации по ссылке из текста сообщения о блокировке.

Для сообщения о блокировке доступа к устройству или запрете операции над содержимым устройства, а также для сообщения администратору предусмотрены шаблоны. Вы можете изменять шаблоны сообщений.

Чтобы изменить шаблоны сообщений Контроля устройств, выполните следующие действия:

1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 66).

2. В левой части окна в разделе **Контроль рабочего места** выберите подраздел **Контроль устройств**.

   В правой части окна отобразятся параметры компонента Контроль устройств.

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 о блокировке доступа к устройству или о запрете операции над содержимым устройства, выберите закладку **Блокировка**.

- Если вы хотите изменить шаблон сообщения администратору локальной сети организации, выберите закладку **Сообщение администратору**.

5. Измените шаблон сообщения. При этом вы можете использовать кнопки **Переменная**, **По умолчанию** и **Ссылка** (кнопка доступна только на закладке **Блокировка**).

6. Нажмите на кнопку **ОК**.

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

Получение доступа к заблокированному устройству

Эта инструкция адресована пользователям клиентских компьютеров с установленной программой Kaspersky Endpoint Security.

Функциональность Kaspersky Endpoint Security для получения временного доступа к устройству доступна только в том случае, если Kaspersky Endpoint Security работает под политикой Kaspersky Security Center и эта функциональность включена в параметрах политики (см. *Руководство администратора Kaspersky Security Center*).

Чтобы запросить доступ к заблокированному устройству из окна настройки компонента Контроль устройств, выполните следующие действия:

1. В главном окне программы выберите закладку **Центр управления**.

2. Нажмите на блок **Контроль рабочего места**.

   Блок **Контроль рабочего места** раскроется.

3. По правой клавише мыши откройте контекстное меню строки с информацией о компоненте Контроль устройств.

   Откроется меню действий с компонентом.

4. Нажмите на кнопку **Доступ к устройству**.

   Откроется окно **Запрос доступа к устройству**.

5. Выберите из списка подключенных устройств то устройство, к которому вы хотите получить доступ.

6. Нажмите на кнопку **Сформировать файл запроса**.

   Откроется окно **Формирование файла запроса**.

7. В поле **Длительность доступа к устройству** укажите, на какое время вы хотите получить доступ к устройству.

8. Нажмите на кнопку **Сохранить**.

   Откроется стандартное окно Microsoft Windows **Сохранение файла запроса**.

9. В окне Microsoft Windows **Сохранение файла запроса** выберите папку, в которую вы хотите сохранить файл запроса доступа к устройству, и нажмите на кнопку **Сохранить**.

10. Передайте файл запроса доступа к устройству администратору локальной сети организации.

11. Получите от администратора локальной сети организации файл с ключом доступа к устройству.

12. В окне **Запрос доступа к устройству** нажмите на кнопку **Активировать ключ доступа**.

    Откроется стандартное окно Microsoft Windows **Загрузка ключа доступа**.

13. В окне Microsoft Windows **Загрузка ключа доступа** выберите файл с ключом доступа к устройству, полученный от администратора локальной сети организации, и нажмите на кнопку **Открыть**.

    Откроется окно **Активация ключа доступа к устройству** с информацией о предоставленном доступе.

14. В окне **Активация ключа доступа к устройству** нажмите на кнопку **ОК**.

Чтобы запросить доступ к заблокированному устройству по ссылке в сообщении о блокировке устройства, выполните следующие действия:

1. Из окна сообщения о блокировке устройства или шины подключения перейдите по ссылке **Запросить доступ**.

   Откроется окно **Формирование файла запроса**.

2. В поле **Длительность доступа к устройству** укажите, на какое время вы хотите получить доступ к устройству.

3. Нажмите на кнопку **Сохранить**.

   Откроется стандартное окно Microsoft Windows **Сохранение файла запроса**.

4. В окне Microsoft Windows **Сохранение файла запроса** выберите папку, в которую вы хотите сохранить файл запроса доступа к устройству, и нажмите на кнопку **Сохранить**.

5. Передайте файл запроса доступа к устройству администратору локальной сети организации.

6. Получите от администратора локальной сети организации файл с ключом доступа к устройству.

7. В окне **Запрос доступа к устройству** нажмите на кнопку **Активировать ключ доступа**.

   Откроется стандартное окно Microsoft Windows **Загрузка ключа доступа**.

8. В окне Microsoft Windows **Загрузка ключа доступа** выберите файл с ключом доступа к устройству, полученный от администратора локальной сети организации, и нажмите на кнопку **Открыть**.

   Откроется окно **Активация ключа доступа к устройству** с информацией о предоставленном доступе.

9. В окне **Активация ключа доступа к устройству** нажмите на кнопку **ОК**.

Период времени, на который предоставляется доступ к устройству, может отличаться от запрашиваемого вами периода времени. Доступ к устройству предоставляется на период времени, который администратор локальной сети организации указывает при формировании ключа доступа к устройству.

Создание ключа доступа к заблокированному устройству с помощью Kaspersky Security Center

Чтобы предоставить пользователю временный доступ к заблокированному устройству, требуется ключ доступа к этому устройству. Вы можете создать ключ доступа с помощью Kaspersky Security Center.

Чтобы создать ключ доступа к заблокированному устройству, 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. В списке клиентских компьютеров выберите компьютер, пользователю которого вы хотите дать временный доступ к заблокированному устройству.
5. В контекстном меню компьютера выберите пункт **Предоставление доступа к устройствам и данным в офлайн-режиме**.

   Откроется окно **Предоставление доступа к устройствам и данным в офлайн-режиме**.
6. Выберите закладку **Контроль устройств**.
7. На закладке **Контроль устройств** нажмите на кнопку **Обзор**.

Откроется стандартное окно Windows **Выбор файла запроса**.

8. В окне Windows **Выбор файла запроса** выберите файл запроса, который вы получили от пользователя, и нажмите на кнопку **Открыть**.

   На закладке **Контроль устройств** отобразится информация о заблокированном устройстве, к которому пользователь запросил доступ.

9. Укажите значение параметра **Длительность доступа к устройству**.

   Параметр содержит период времени, на который вы предоставляете пользователю доступ к заблокированному устройству. По умолчанию выбрано значение, указанное пользователем при формировании файла запроса.

10. Укажите значение параметра **Срок активации**.

    Параметр содержит период времени, в течение которого пользователь может активировать доступ к заблокированному устройству с помощью предоставленного ключа доступа.

11. Нажмите на кнопку **Сохранить**.

    Откроется стандартное окно Windows **Сохранение ключа доступа**.

12. Выберите папку, в которую вы хотите сохранить файл с ключом доступа к заблокированному устройству.

13. Нажмите на кнопку **Сохранить**.

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 (см. раздел "Аппаратные и программные требования" на стр. 24).

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 "Средства интернет-коммуникации").

- 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. 275).

Включение и выключение Веб-Контроля

По умолчанию Веб-Контроль включен. Вы можете выключить Веб-Контроль при необходимости.

Включить и выключить компонент можно двумя способами:

- на закладке **Центр управления** главного окна программы (см. раздел "Главное окно программы" на стр. 64);
- из окна настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 66).

*Чтобы включить или выключить Веб-Контроль на закладке **Центр управления** главного окна программы, выполните следующие действия:*

1. Откройте главное окно программы.
2. Выберите закладку **Центр управления**.
3. Нажмите клавишей мыши на блок **Контроль рабочего места**.

   Блок **Контроль рабочего места** раскроется.
4. По правой клавише мыши откройте контекстное меню строки с информацией о компоненте Веб-Контроль.

   Откроется меню действий с компонентом.
5. Выполните одно из следующих действий:
   - Выберите в меню пункт **Включить**, если вы хотите включить Веб-Контроль.
   - Выберите в меню пункт **Выключить**, если вы хотите выключить Веб-Контроль.

Чтобы включить или выключить Веб-Контроль из окна настройки параметров программы, выполните следующие действия:

1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 66).

2. В левой части окна в разделе **Контроль рабочего места** 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 продуктов 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.

  Пересекается с категорией "Средства интернет-коммуникации".

- 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").

  Пересекается с категорией "Электронная коммерция".

К этой категории не относятся веб-ресурсы с научным, медицинским и учебным содержанием.

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.

  > Пересекается с категорией "Электронная коммерция".

- 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.

  Пересекается с категорией "Электронная коммерция".

- 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.

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.

Пересекается с категорией "Электронная коммерция".

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.

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", "Электронная коммерция".

- **Веб-почта**.

  Подкатегория включает исключительно страницы авторизации в почтовом сервисе и страницы почтового ящика, содержащего почтовые сообщения и сопутствующие данные (например, личные контакты). Остальные веб-страницы интернет-провайдера, предлагающего почтовый сервис, к этой категории не относятся.

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.

Пересекается с категорией "Средства интернет-коммуникации".

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.

  Пересекается с категорией "Средства интернет-коммуникации".

- 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.

  Пересекается с категорией "Электронная коммерция".

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").

> Пересекается с категорией "Средства интернет-коммуникации".

Баннеры

Категория включает веб-ресурсы, содержащие баннеры. Рекламная информация на баннерах может отвлекать пользователей от дел, а загрузка баннеров увеличивает объем трафика.

О правилах доступа к веб-ресурсам

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. 265) и категориям типа данных. Вы можете контролировать доступ пользователей к веб-ресурсам определенных категорий содержания и / или категорий типа 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. 66).

2. В левой части окна в разделе **Контроль рабочего места** 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 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 **OK**.

5. В окне **Правило доступа к веб-ресурсам** нажмите на кнопку **OK**.

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. 66).

2. В левой части окна в разделе **Контроль рабочего места** 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. 66).

2. В левой части окна в разделе **Контроль рабочего места** 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. 66).

2. В левой части окна в разделе **Контроль рабочего места** 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 Service Pack 1 Maintenance Release 1 и с более ранних версий до Kaspersky Endpoint Security 10 Service Pack 2 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 "Форумы и чаты", "Веб-почта", "Социальные сети", становятся основанными на категории содержания веб-ресурсов "Средства интернет-коммуникации".

- 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 "Электронная коммерция".

- 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. 66).

2. В левой части окна в разделе **Контроль рабочего места** 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. 66).

2. В левой части окна в разделе **Контроль рабочего места** 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 **ОК**.

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.
8	http://www.*.example.com	http://123.example.com	Да	См. правила 2, 4, 1.

№	Маска адреса	Проверяемый адрес веб-ресурса	Удовлетворяет ли проверяемый адрес маске адреса	Комментарий
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.

№	Маска адреса	Проверяемый адрес веб-ресурса	Удовлетворяет ли проверяемый адрес маске адреса	Комментарий
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.

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. 66).

2. В левой части окна в разделе **Контроль рабочего места** 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.

KATA Endpoint Sensor

Параметры компонента KATA Endpoint Sensor доступны только в Консоли администрирования Kaspersky Security Center. Для использования компонента требуется установить плагин управления.

Этот раздел содержит информацию о KATA Endpoint Sensor и инструкцию о том, как включить или выключить компонент.

В этом разделе

О KATA Endpoint Sensor

KATA 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.

На компьютерах с компонентом KATA Endpoint Sensor необходимо разрешить входящее соединение с сервером Kaspersky Anti Targeted Attack Platform напрямую, без использования прокси-сервера.

Включение и выключение компонента KATA Endpoint Sensor

Чтобы включить или выключить компонент KATA 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. В разделе **Дополнительные параметры** выберите подраздел **KATA Endpoint Sensor**.
7. Выполните одно из следующих действий:
   - Если вы хотите включить KATA Endpoint Sensor, установите флажок **KATA Endpoint Sensor**.
   - Если вы хотите выключить KATA Endpoint Sensor, снимите флажок **KATA Endpoint Sensor**.
8. Если на предыдущем шаге вы установили флажок **KATA Endpoint Sensor**, в поле **Адрес сервера** укажите адрес сервера Kaspersky Anti Targeted Attack Platform, состоящий из следующих частей:
   a. название протокола;

b. IP-адрес или полное доменное имя (FQDN) сервера;

c. путь к Сборщику событий Windows на сервере.

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.*

Шифрование данных

Если программа Kaspersky Endpoint Security установлена на компьютере под управлением операционной системы Microsoft Windows для рабочих станций, то функциональность шифрования данных доступна в полном объеме. Если программа Kaspersky Endpoint Security установлена на компьютере под управлением операционной системы Microsoft Windows для файловых серверов (см. раздел "Аппаратные и программные требования" на стр. 24), то доступно только шифрование жестких дисков с помощью технологии Шифрование диска BitLocker.

Этот раздел содержит информацию о шифровании и расшифровке жестких и съемных дисков, файлов и папок на локальных дисках компьютера, а также инструкции о том, как настроить и выполнить шифрование и расшифровку данных с помощью Kaspersky Endpoint Security и плагина управления Kaspersky Endpoint Security.

При отсутствии доступа к зашифрованным данным следуйте специальным инструкциям по работе с зашифрованными данными, .

В этом разделе

Включение отображения параметров шифрования в политике Kaspersky Security Center

Чтобы включить отображение параметров шифрования в политике Kaspersky Security Center, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В контекстном меню узла **Сервер администрирования – <Имя компьютера>** дерева Консоли администрирования выберите пункт **Вид** → **Настройка интерфейса**.

   Откроется окно **Настройка интерфейса**.
3. В окне **Настройка интерфейса** установите флажок **Отображать шифрование и защиту данных**.
4. Нажмите на кнопку **OK**.

О шифровании данных

Kaspersky Endpoint Security позволяет шифровать файлы и папки, хранящиеся на локальных дисках компьютера и съемных дисках, съемные и жесткие диски целиком. Шифрование данных снижает риски утечки информации в случае кражи / утери портативного компьютера, съемного диска или жесткого диска, а также при доступе посторонних пользователей и программ к данным.

Если срок действия лицензии истек, то программа не шифрует новые данные, а старые зашифрованные данные остаются зашифрованными и доступными для работы. В этом случае для шифрования новых данных требуется активировать программу по новой лицензии, которая допускает использование шифрования.

В случае истечения срока действия лицензии, нарушения Лицензионного соглашения, удаления ключа, удаления программы Kaspersky Endpoint Security или компонентов шифрования с компьютера пользователя не гарантируется, что файлы, зашифрованные ранее, останутся зашифрованными. Это связано с тем, что некоторые программы, например Microsoft Office Word, при редактировании файлов создают их временную копию, которой подменяют исходный файл при его сохранении. В результате при отсутствии или недоступности на компьютере функциональности шифрования файл остается незашифрованным.

Kaspersky Endpoint Security обеспечивает следующие направления защиты данных:

- **Шифрование файлов на локальных дисках компьютера**. Вы можете сформировать списки из файлов (см. раздел "Запуск шифрования файлов на локальных дисках компьютера" на стр. 311) по расширению или группам расширений и из папок, расположенных на локальных дисках компьютера, а также создать правила шифрования файлов, создаваемых отдельными программами (см. раздел "Шифрование файлов, создаваемых и изменяемых отдельными программами" на стр. 315). После применения политики Kaspersky Security Center программа Kaspersky Endpoint Security шифрует и расшифровывает следующие файлы:

  - файлы, отдельно добавленные в списки для шифрования и расшифровки;
  - файлы, хранящиеся в папках, добавленных в списки для шифрования и расшифровки;
  - файлы, создаваемые отдельными программами.

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

- **Шифрование съемных дисков**. Вы можете указать правило шифрования по умолчанию, в соответствии с которым программа выполняет одинаковое действие по отношению ко всем съемным дискам, и указать правила шифрования отдельных съемных дисков.

  Правило шифрования по умолчанию имеет меньший приоритет, чем правила шифрования, созданные для отдельных съемных дисков. Правила шифрования, созданные для съемных дисков с указанной моделью устройства, имеют меньший

приоритет, чем правила шифрования, созданные для съемных дисков с указанным идентификатором устройства.

Чтобы выбрать правило шифрования файлов на съемном диске, Kaspersky Endpoint Security проверяет, известны ли модель устройства и его идентификатор. Далее программа выполняет одно из следующих действий:

- Если известна только модель устройства, программа применяет правило шифрования, созданное для съемных дисков с данной моделью устройства, если такое правило есть.
- Если известен только идентификатор устройства, программа применяет правило шифрования, созданное для съемных дисков с данным идентификатором устройства, если такое правило есть.
- Если известны и модель устройства, и идентификатор устройства, программа применяет правило шифрования, созданное для съемных дисков с данным идентификатором устройства, если такое правило есть. Если такого правила нет, но есть правило шифрования, созданное для съемных дисков с данной моделью устройства, программа применяет его. Если не заданы правила шифрования ни для данного идентификатора устройства, ни для данной модели устройства, программа применяет правило шифрования по умолчанию.
- Если неизвестны ни модель устройства, ни идентификатор устройства, программа применяет правило шифрования по умолчанию.

Программа позволяет подготовить съемный диск для работы с зашифрованными на нем файлами в портативном режиме. После включения портативного режима становится доступной работа с зашифрованными файлами на съемных дисках, подключенных к компьютеру с недоступной функциональностью шифрования.

Программа выполняет указанное в правиле шифрования действие при применении политики Kaspersky Security Center.

- **Управление правами доступа программ к зашифрованным файлам**. Для любой программы вы можете создать правило доступа к зашифрованным файлам, запрещающее доступ к зашифрованным файлам или разрешающее доступ к зашифрованным файлам только в виде шифротекста - последовательности символов, полученной в результате применения шифрования.

- **Создание зашифрованных архивов**. Вы можете создавать зашифрованные архивы и защищать доступ к этим архивам паролем. Доступ к содержимому зашифрованных архивов можно получить только после ввода паролей, которыми вы защитили доступ к этим архивам. Такие архивы можно безопасно передавать по сети или на съемных дисках.

- **Шифрование жестких дисков**. Вы можете выбрать технологию шифрования: Шифрование диска Kaspersky или Шифрование диска BitLocker (далее также "BitLocker").

  BitLocker - технология, являющаяся частью операционной системы Windows. Если компьютер оснащен доверенным платформенным модулем (TPM, Trusted Platform Module), BitLocker использует его для хранения ключей восстановления, позволяющих получить доступ к зашифрованному жесткому диску. При загрузке компьютера BitLocker запрашивает у доверенного платформенного модуля ключи восстановления жесткого диска и разблокирует его. Вы можете настроить использование пароля и / или PIN-кода для доступа к ключам восстановления.

  Вы можете указать правило шифрования жестких дисков по умолчанию и сформировать список жестких дисков для исключения из шифрования. Kaspersky Endpoint Security выполняет шифрование жестких дисков по секторам после применения политики Kaspersky Security Center. Программа шифрует сразу все логические разделы жестких дисков. Подробнее о применении политики Kaspersky Security Center вы можете прочитать в *Руководстве администратора для Kaspersky Security Center.*

  После шифрования системных жестких дисков при последующем включении компьютера доступ к ним, а также загрузка операционной системы возможны только после прохождения процедуры аутентификации с помощью Агента аутентификации. Для этого требуется ввести пароль токена или смарт-карты, подключенных к компьютеру, или имя и пароль учетной записи Агента аутентификации, созданной системным администратором локальной сети организации с помощью задач управления учетными записями Агента аутентификации. Эти учетные записи основаны на учетных записях пользователей Microsoft Windows, под которыми пользователи выполняют вход в операционную систему. Вы можете управлять учетными записями Агента аутентификации и использовать технологию единого входа (SSO, Single Sign-On), позволяющую осуществлять автоматический вход в

операционную систему с помощью имени и пароля учетной записи Агента аутентификации.

Если для компьютера была создана резервная копия, затем данные компьютера были зашифрованы, после чего была восстановлена резервная копия компьютера и данные компьютера снова были зашифрованы, Kaspersky Endpoint Security формирует дубликаты учетных записей Агента аутентификации. Для удаления дубликатов требуется использовать утилиту klmover с ключом `dupfix`. Утилита klmover поставляется со сборкой Kaspersky Security Center. Подробнее о ее работе вы можете прочитать в *Руководстве администратора для Kaspersky Security Center*.

При обновлении версии программы до Kaspersky Endpoint Security 10 Service Pack 2 для Windows список учетных записей Агента аутентификации не сохраняется.

Доступ к зашифрованным жестким дискам возможен только с компьютеров, на которых установлена программа Kaspersky Endpoint Security с доступной функциональностью шифрования жестких дисков (см. раздел "Работа с зашифрованными устройствами при отсутствии доступа к ним" на стр. 376). Это условие сводит к минимуму вероятность утечки информации, хранящейся на зашифрованном жестком диске, при использовании зашифрованного жесткого диска вне локальной сети организации.

Для шифрования жестких и съемных дисков вы можете использовать функцию **Шифровать только занятое пространство**. Рекомендуется применять эту функцию только для новых, ранее не использовавшихся устройств. Если вы применяете шифрование на уже используемом устройстве, рекомендуется зашифровать все устройство. Это гарантирует защиту всех данных - даже удаленных, но еще содержащих извлекаемые сведения.

Перед началом шифрования Kaspersky Endpoint Security получает карту секторов файловой системы. В первом потоке шифруются секторы, занятые файлами на момент запуска шифрования. Во втором потоке шифруются секторы, в которые выполнялась запись после начала шифрования. После завершения шифрования все секторы, содержащие данные, оказываются зашифрованными.

Если после завершения шифрования пользователь удаляет файл, то секторы, в которых хранился этот файл, становятся свободными для дальнейшей записи информации на уровне файловой системы, но остаются зашифрованными. Таким образом, по мере записи файлов на новом устройстве при регулярном запуске шифрования с включенной функцией **Шифровать только занятое пространство** на компьютере через некоторое время будут зашифрованы все секторы.

Данные, необходимые для расшифровки объектов, предоставляет Сервер администрирования Kaspersky Security Center, под управлением которого находился компьютер в момент шифрования. Если по каким-либо причинам компьютер с зашифрованными объектами попал под управление другого Сервера администрирования и доступ к зашифрованным объектам ни разу не был осуществлен, то получить его возможно одним из следующих способов:

- запросить доступ к зашифрованным объектам у администратора локальной сети организации;
- восстановить данные на зашифрованных устройствах с помощью утилиты восстановления;
- восстановить конфигурацию Сервера администрирования Kaspersky Security Center, под управлением которого находился компьютер в момент шифрования, из резервной копии и использовать эту конфигурацию на Сервере администрирования, под управлением которого оказался компьютер с зашифрованными объектами.

В процессе шифрования программа создает служебные файлы. Для их хранения требуется около двух-трех процентов нефрагментированного свободного пространства на жестком диске компьютера. Если нефрагментированного свободного пространства на жестком диске недостаточно, то шифрование не запускается до тех пор, пока не обеспечено это условие.

Не поддерживается совместимость между функциональностью шифрования Kaspersky Endpoint Security и Антивирусом Касперского для UEFI. Шифрование жестких дисков компьютеров, на которых установлен Антивирус Касперского для UEFI, приводит к неработоспособности Антивируса Касперского для UEFI.

См. также

Получение доступа к зашифрованным файлам при отсутствии связи с Kaspersky Security Center 371

Получение доступа к зашифрованным устройствам через интерфейс программы 379

Восстановление данных на зашифрованных устройствах с помощью утилиты восстановления 385

Ограничения функциональности шифрования

Функциональность шифрования жестких дисков с помощью технологии Шифрование диска Kaspersky недоступна для жестких дисков, которые не отвечают аппаратным и программным требованиям.

Kaspersky Endpoint Security не поддерживает следующие конфигурации:

- схема, при которой загрузчик расположен на одном диске, а операционная система - на другом;

- встроенное программное обеспечение стандарта UEFI 32;
- система с технологией Intel® Rapid Start Technology и диски с разделом гибернации (hibernation partition), даже при отключенном использовании Intel® Rapid Start Technology;
- диски в формате MBR, имеющие более четырех расширенных разделов (extended partitions);
- система, в которой есть файл подкачки, расположенный не на системном диске;
- мультизагрузочная система с несколькими одновременно установленными операционными системами;
- динамические разделы (поддерживаются только разделы основного типа);
- диски, на которых менее 2% свободного нефрагментированного пространства;
- диски с размером сектора, отличным от 512 байт или 4096 байт, которые эмулируют 512 байт;
- гибридные диски.

Смена алгоритма шифрования

Алгоритм шифрования, который Kaspersky Endpoint Security использует для шифрования данных, зависит от библиотек шифрования, входящих в состав дистрибутива.

Чтобы сменить алгоритм шифрования, выполните следующие действия:

1. Расшифруйте объекты, которые программа Kaspersky Endpoint Security зашифровала до начала смены алгоритма шифрования.

   После смены алгоритма шифрования объекты, зашифрованные ранее, становятся недоступны.

2. Удалите Kaspersky Endpoint Security (см. раздел "Удаление программы" на стр. 54).

3. Установите Kaspersky Endpoint Security (см. раздел "Установка программы" на стр. 26) из дистрибутива с библиотеками шифрования другой разрядности.

Включение использования технологии единого входа (SSO)

Технология единого входа (SSO) несовместима со сторонними поставщиками учетных данных.

Чтобы включить использование технологии единого входа (SSO), 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 включить использование технологии единого входа (SSO).
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 **Шифрование данных** выберите подраздел **Общие параметры шифрования**.
7. В подразделе **Общие параметры шифрования** в блоке **Параметры паролей** нажмите на кнопку **Настройка**.

   Откроется закладка **Агент аутентификации** окна **Параметры паролей для шифрования**.

8. Установите флажок **Использовать технологию единого входа (SSO)**.

9. Нажмите на кнопку **OK**.

10. В окне **Свойства: <Название политики>** нажмите на кнопку **OK**, чтобы сохранить внесенные изменения.

11. Примените политику.

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

Особенности шифрования файлов

При использовании функциональности шифрования файлов следует иметь в виду следующие особенности:

- Политика Kaspersky Security Center с заданными параметрами шифрования съемных дисков формируется для определенной группы управляемых компьютеров. Поэтому результат применения политики шифрования / расшифровки съемных дисков зависит от того, к какому компьютеру подключен съемный диск.

- Kaspersky Endpoint Security не выполняет шифрование / расшифровку файлов со статусом доступа "только чтение", хранящихся на съемных дисках.

- Kaspersky Endpoint Security шифрует / расшифровывает стандартные папки только для локальных профилей пользователей (local user profiles) операционной системы. Kaspersky Endpoint Security не шифрует и не расшифровывает стандартные папки для перемещаемых профилей пользователей (roaming user profiles), мандатных профилей пользователей (mandatory user profiles), временных профилей пользователей (temporary user profiles) и перенаправляемых папок (folder redirection). В список стандартных папок, рекомендованных специалистами "Лаборатории Касперского" для шифрования, входят следующие папки:

  - Мои документы.

  - Избранное.

- Файлы Cookies.
- Рабочий стол.
- Временные файлы Internet Explorer.
- Временные файлы.
- Файлы Outlook.

- Kaspersky Endpoint Security не выполняет шифрование файлов и папок, изменение которых может повредить работе операционной системы и установленных программ. Например, в список исключений из шифрования входят следующие файлы и папки со всеми вложенными в них папками:
  - %WINDIR%.
  - %PROGRAMFILES%, %PROGRAMFILES(X86)%.
  - файлы реестра Windows.

  Список исключений из шифрования недоступен для просмотра и изменения. Файлы и папки из списка исключений из шифрования можно добавить в список для шифрования, но при выполнении задачи шифрования файлов и папок они не будут зашифрованы.
- В качестве съемных дисков поддерживаются следующие типы устройств:
  - носители информации, подключаемые по шине USB;
  - жесткие диски, подключаемые по шинам USB и FireWire;
  - SSD-диски, подключаемые по шинам USB и FireWire.

Шифрование файлов на локальных дисках компьютера

Шифрование файлов на локальных дисках компьютера доступно, если программа Kaspersky Endpoint Security установлена на компьютере под управлением операционной системы Microsoft Windows для рабочих станций. Шифрование файлов на локальных дисках компьютера недоступно, если программа Kaspersky Endpoint Security установлена на компьютере под управлением операционной системы Microsoft Windows для файловых серверов (см. раздел "Аппаратные и программные требования" на стр. 24).

Этот раздел содержит информацию о шифровании файлов на локальных дисках компьютера и инструкции о том, как настроить и выполнить шифрование файлов на локальных дисках компьютера с помощью Kaspersky Endpoint Security и плагина управления Kaspersky Endpoint Security.

В этом разделе

Запуск шифрования файлов на локальных дисках компьютера

Чтобы зашифровать файлы на локальных дисках компьютера, 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 шифрование файлов на локальных дисках.
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 **Шифрование данных** выберите подраздел **Шифрование файлов и папок**.
7. В правой части окна выберите закладку **Шифрование**.
8. В раскрывающемся списке **Режим шифрования** выберите элемент **Согласно правилам**.
9. На закладке **Шифрование** нажмите на кнопку **Добавить** и в раскрывающемся списке выберите один из следующих элементов:
   a. Выберите элемент **Стандартные папки**, чтобы добавить в правило шифрования файлы из папок локальных профилей пользователей, предложенных специалистами "Лаборатории Касперского".

   Откроется окно **Выбор стандартных папок**.

b. Выберите элемент **Папку вручную**, чтобы добавить в правило шифрования папку, путь к которой введен вручную.

   Откроется окно **Добавление папки вручную**.

c. Выберите элемент **Файлы по расширению**, чтобы добавить в правило шифрования расширения файлов. Kaspersky Endpoint Security шифрует файлы с указанными расширениями на всех локальных дисках компьютера.

   Откроется окно **Добавление / изменение списка расширений файлов**.

d. Выберите элемент **Файлы по группе(ам) расширений**, чтобы добавить в правило шифрования группы расширений файлов. Kaspersky Endpoint Security шифрует файлы с расширениями, перечисленными в группах расширений, на всех локальных дисках компьютера.

   Откроется окно **Выбор групп расширений файлов**.

10. В окне **Свойства: <Название политики>** нажмите на кнопку **OK**, чтобы сохранить внесенные изменения.

11. Примените политику.

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

Сразу после применения политики Kaspersky Endpoint Security шифрует файлы, включенные в правило шифрования и не включенные в правило расшифровки (см. раздел "Формирование правила расшифровки" на стр. 318).

> Если один и тот же файл добавлен и в правило шифрования, и в правило расшифровки, то Kaspersky Endpoint Security не шифрует этот файл, если он не зашифрован, и расшифровывает, если он зашифрован.

Kaspersky Endpoint Security шифрует незашифрованные файлы, если их свойства (путь к файлу / имя файла / расширение файла) после изменения по-прежнему удовлетворяют критериям правила шифрования.

Kaspersky Endpoint Security откладывает шифрование открытых файлов до тех пор, пока они не будут закрыты.

Когда пользователь создает новый файл, свойства которого удовлетворяют критериям правила шифрования, Kaspersky Endpoint Security шифрует файл сразу же при открытии файла.

Если вы переносите зашифрованный файл в другую папку на локальном диске, файл остается зашифрованным, независимо от того, включена ли эта папка в правило шифрования.

Формирование правил доступа программ к зашифрованным файлам

Чтобы сформировать правила доступа программ к зашифрованным файлам, 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 сформировать правила доступа программ к зашифрованным файлам.
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 **Шифрование данных** выберите подраздел **Шифрование файлов и папок**.
7. В раскрывающемся списке **Режим шифрования** выберите элемент **Согласно правилам**.

Правила доступа действуют только в режиме **Согласно правилам**. Если после применения правил доступа в режиме **Согласно правилам** вы перейдете в режим **Оставлять без изменений**, то Kaspersky Endpoint Security будет игнорировать все правила доступа. Все программы будут иметь доступ ко всем зашифрованным файлам.

8. В правой части окна выберите закладку **Правила для программ**.

9. Если вы хотите выбрать программы исключительно из списка Kaspersky Security Center, нажмите на кнопку **Добавить** и в раскрывающемся списке выберите элемент **Программы из списка Kaspersky Security Center**.

   Откроется окно **Добавление программ из списка Kaspersky Security Center**.

   Выполните следующие действия:

   a. Задайте фильтры для вывода списка программ в таблице. Для этого укажите значения параметров **Программа**, **Производитель**, **Период добавления**, а также флажков из блока **Группа**.

   b. Нажмите на кнопку **Обновить**.

      В таблице отобразится список программ, удовлетворяющих заданным фильтрам.

   c. В графе **Программы** установите флажки напротив тех программ в таблице, для которых вы хотите сформировать правила доступа к зашифрованным файлам.

   d. В раскрывающемся списке **Правило для программ(ы)** выберите правило, которое будет определять доступ программ к зашифрованным файлам.

   e. В раскрывающемся списке **Действие для программ, выбранных ранее** выберите действие, которое выполняет Kaspersky Endpoint Security над правилами доступа к зашифрованным файлам, сформированными для указанных выше программ ранее.

   f. Нажмите на кнопку **OK**.

   Информация о правиле доступа программ к зашифрованным файлам отобразится в таблице на закладке **Правила для программ**.

10. Если вы хотите выбрать программы вручную, нажмите на кнопку **Добавить** и в раскрывающемся списке выберите элемент **Программы вручную**.

    Откроется окно **Добавление / изменение названий исполняемых файлов программ**.

    Выполните следующие действия:

    a. В поле ввода введите имя или список имен исполняемых файлов программ с их расширениями.

    Вы можете также добавить имена исполняемых файлов программ из списка Kaspersky Security Center, нажав на кнопку **Добавить из списка Kaspersky Security Center**.

    b. Если требуется, в поле **Описание** введите описание списка программ.

    c. В раскрывающемся списке **Правило для программ(ы)** выберите правило, которое будет определять доступ программ к зашифрованным файлам.

    d. Нажмите на кнопку **OK**.

    Информация о правиле доступа программ к зашифрованным файлам отобразится в таблице на закладке **Правила для программ**.

11. Нажмите на кнопку **OK**, чтобы сохранить внесенные изменения.

Шифрование файлов, создаваемых и изменяемых отдельными программами

Вы можете создать правило, согласно которому Kaspersky Endpoint Security будет шифровать все файлы, создаваемые и изменяемые указанными в правиле программами.

> Файлы, созданные или измененные указанными программами до применения правила шифрования, не будут зашифрованы.

Чтобы настроить шифрование файлов, создаваемых и изменяемых отдельными программами, 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 настроить шифрование файлов, создаваемых отдельными программами.

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 **Шифрование данных** выберите подраздел **Шифрование файлов и папок**.

7. В раскрывающемся списке **Режим шифрования** выберите элемент **Согласно правилам**.

   Правила шифрования действуют только в режиме **Согласно правилам**. Если после применения правил шифрования в режиме **Согласно правилам** вы перейдете в режим **Оставлять без изменений**, то Kaspersky Endpoint Security будет игнорировать все правила шифрования. Файлы, которые были зашифрованы ранее, по-прежнему останутся зашифрованными.

8. В правой части окна выберите закладку **Правила для программ**.

9. Если вы хотите выбрать программы исключительно из списка Kaspersky Security Center, нажмите на кнопку **Добавить** и в раскрывающемся списке выберите элемент **Программы из списка Kaspersky Security Center**.

   Откроется окно **Добавление программ из списка Kaspersky Security Center**.

Выполните следующие действия:

a. Задайте фильтры для вывода списка программ в таблице. Для этого укажите значения параметров **Программа**, **Производитель**, **Период добавления**, а также флажков из блока **Группа**.

b. Нажмите на кнопку **Обновить**.

   В таблице отобразится список программ, удовлетворяющих заданным фильтрам.

c. В графе **Программы** установите флажки напротив тех программ в таблице, создаваемые файлы которых требуется шифровать.

d. В раскрывающемся списке **Правило для программ(ы)** выберите элемент **Шифровать все создаваемые файлы**.

e. В раскрывающемся списке **Действие для программ, выбранных ранее** выберите действие, которое выполняет Kaspersky Endpoint Security над правилами шифрования файлов, сформированными для указанных выше программ ранее.

f. Нажмите на кнопку **OK**.

Информация о правиле шифрования файлов, создаваемых и изменяемых выбранными программами, отобразится в таблице на закладке **Правила для программ**.

10. Если вы хотите выбрать программы вручную, нажмите на кнопку **Добавить** и в раскрывающемся списке выберите элемент **Программы вручную**.

    Откроется окно **Добавление / изменение названий исполняемых файлов программ**.

    Выполните следующие действия:

    a. В поле ввода введите имя или список имен исполняемых файлов программ с их расширениями.

Вы можете также добавить имена исполняемых файлов программ из списка Kaspersky Security Center, нажав на кнопку **Добавить из списка Kaspersky Security Center**.

b. Если требуется, в поле **Описание** введите описание списка программ.

c. В раскрывающемся списке **Правило для программ(ы)** выберите элемент **Шифровать все создаваемые файлы**.

d. Нажмите на кнопку **OK**.

Информация о правиле шифрования файлов, создаваемых и изменяемых выбранными программами, отобразится в таблице на закладке **Правила для программ**.

11. Нажмите на кнопку **OK**, чтобы сохранить внесенные изменения.

Формирование правила расшифровки

Чтобы сформировать правило расшифровки, 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 сформировать список файлов для расшифровки.
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 **Шифрование данных** выберите подраздел **Шифрование файлов и папок**.

7. В правой части окна выберите закладку **Расшифровка**.

8. В раскрывающемся списке **Режим шифрования** выберите элемент **Согласно правилам**.

9. На закладке **Расшифровка** нажмите на кнопку **Добавить** и в раскрывающемся списке выберите один из следующих элементов:

    a. Выберите элемент **Стандартные папки**, чтобы добавить в правило расшифровки файлы из папок локальных профилей пользователей, предложенных специалистами "Лаборатории Касперского".

    Откроется окно **Выбор стандартных папок**.

    b. Выберите элемент **Папку вручную**, чтобы добавить в правило расшифровки папку, путь к которой введен вручную.

    Откроется окно **Добавление папки вручную**.

    c. Выберите элемент **Файлы по расширению**, чтобы добавить в правило расшифровки расширения файлов. Kaspersky Endpoint Security не шифрует файлы с указанными расширениями на всех локальных дисках компьютера.

    Откроется окно **Добавление / изменение списка расширений файлов**.

    d. Выберите элемент **Файлы по группе(ам) расширений**, чтобы добавить в правило расшифровки группы расширений файлов. Kaspersky Endpoint Security не шифрует файлы с расширениями, перечисленными в группах расширений, на всех локальных дисках компьютеров.

    Откроется окно **Выбор групп расширений файлов**.

10. В окне **Свойства: <Название политики>** нажмите на кнопку **ОК**, чтобы сохранить внесенные изменения.

11. Примените политику.

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

Если один и тот же файл добавлен и в правило шифрования, и в правило расшифровки, то Kaspersky Endpoint Security не шифрует этот файл, если он не зашифрован, и расшифровывает, если он зашифрован.

Расшифровка файлов на локальных дисках компьютера

Чтобы расшифровать файлы на локальных дисках компьютера, 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 расшифровку файлов на локальных дисках.
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 **Шифрование данных** выберите подраздел **Шифрование файлов и папок**.
7. В правой части окна выберите закладку **Шифрование**.
8. Исключите из списка для шифрования файлы и папки, которые вы хотите расшифровать. Для этого в списке выберите файлы и в контекстном меню кнопки **Удалить** выберите пункт **Удалить правило и расшифровать файлы**.

   Вы можете удалять сразу несколько элементов из списка для шифрования. Для этого, удерживая клавишу **CTRL**, левой клавишей мыши выберите нужные элементы

и в контекстном меню кнопки **Удалить** выберите пункт **Удалить правило и расшифровать файлы**.

Удаленные из списка для шифрования файлы и папки автоматически добавляются в список для расшифровки.

9. Сформируйте список файлов для расшифровки (см. раздел "Формирование правила расшифровки" на стр. 318).

10. В окне **Свойства: <Название политики>** нажмите на кнопку **ОК**, чтобы сохранить внесенные изменения.

11. Примените политику.

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

Сразу после применения политики Kaspersky Endpoint Security расшифровывает зашифрованные файлы, добавленные в список для расшифровки.

Kaspersky Endpoint Security расшифровывает зашифрованные файлы, если их параметры (путь к файлу / название файла / расширение файла) изменяются и начинают удовлетворять параметрам объектов, добавленных в список для расшифровки.

Kaspersky Endpoint Security откладывает расшифровку открытых файлов до тех пор, пока они не будут закрыты.

Создание зашифрованных архивов

В процессе создания зашифрованного архива Kaspersky Endpoint Security не выполняет сжатие файлов.

Чтобы создать зашифрованный архив, выполните следующие действия:

1. На компьютере с установленной программой Kaspersky Endpoint Security и доступной функциональностью шифрования файлов в любом файловом менеджере выделите файлы и / или папки, которые вы хотите добавить в зашифрованный архив. По правой клавише мыши откройте их контекстное меню.

2. Выберите пункт **Создать зашифрованный архив** в контекстном меню.

   Откроется стандартное окно Microsoft Windows **Выбор пути для сохранения зашифрованного архива**.

3. В стандартном окне Microsoft Windows **Выбор пути для сохранения зашифрованного архива** выберите место для сохранения зашифрованного архива на съемном диске. Нажмите на кнопку **Сохранить**.

   Откроется окно **Создание зашифрованного архива**.

4. В окне **Создание зашифрованного архива** введите пароль и повторите его.

5. Нажмите на кнопку **Создать**.

   Запустится процесс создания зашифрованного архива. По завершении процесса в указанном месте на съемном диске будет создан самораспаковывающийся защищенный паролем зашифрованный архив.

Если вы отменяете создание зашифрованного архива, то Kaspersky Endpoint Security выполняет следующие действия:

1. Останавливает процессы копирования файлов в архив и завершает все операции шифрования архива, если таковые выполняются.

2. Удаляет все временные файлы, образовавшиеся в процессе создания и шифрования архива, а также сам файл зашифрованного архива.

3. Информирует о принудительной остановке процесса создания зашифрованного архива.

Распаковка зашифрованных архивов

Чтобы распаковать зашифрованный архив, выполните следующие действия:

1. В любом файловом менеджере выделите зашифрованный архив и по левой клавише мыши запустите мастер распаковки зашифрованного архива.

   Откроется окно **Ввод пароля**.

2. Введите пароль, которым защищен зашифрованный архив.
3. В окне **Ввод пароля** нажмите на кнопку **OK**.

   Если введен верный пароль, откроется стандартное окно Microsoft Windows **Обзор папок**.
4. В стандартном окне Microsoft Windows **Обзор папок** выберите папку для распаковки зашифрованного архива и нажмите на кнопку **OK**.

   Запустится процесс распаковки зашифрованного архива в указанную папку.

Если зашифрованный архив уже был распакован в указанную папку, при повторной распаковке файлы зашифрованного архива будут перезаписаны.

Если вы отменяете распаковку зашифрованного архива, то Kaspersky Endpoint Security выполняет следующие действия:

1. Останавливает процесс расшифровки архива и прерывает все операции копирования файлов из зашифрованного архива, если таковые имеются.
2. Удаляет все временные файлы, образовавшиеся в процессе расшифровки и распаковки зашифрованного архива, а также все файлы, которые уже были скопированы из зашифрованного архива в папку назначения.
3. Информирует о принудительной остановке процесса распаковки зашифрованного архива.

Шифрование съемных дисков

Шифрование съемных дисков доступно, если программа Kaspersky Endpoint Security установлена на компьютере под управлением операционной системы Microsoft Windows для рабочих станций. Шифрование съемных дисков недоступно, если программа Kaspersky Endpoint Security установлена на компьютере под управлением операционной системы Microsoft Windows для файловых серверов (см. раздел "Аппаратные и программные требования" на стр. 24).

Этот раздел содержит информацию о шифровании съемных дисков и инструкции о том, как настроить и выполнить шифрование съемных дисков с помощью Kaspersky Endpoint Security и плагина управления Kaspersky Endpoint Security.

В этом разделе

Запуск шифрования съемных дисков

Чтобы зашифровать съемные диски, 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 шифрование съемных дисков.
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 **Шифрование данных** выберите подраздел **Шифрование съемных дисков**.

7. В раскрывающемся списке **Режим шифрования** выберите действие, которое по умолчанию выполняет Kaspersky Endpoint Security со всеми съемными дисками, подключаемыми к компьютерам из выбранной группы администрирования:

   - **Шифровать весь съемный диск**. Если выбран этот элемент, то при применении политики Kaspersky Security Center с заданными параметрами шифрования съемных дисков Kaspersky Endpoint Security посекторно шифрует содержимое съемных дисков. Таким образом, зашифрованными оказываются не только файлы, которые хранятся на съемных дисках, но и файловые системы съемных дисков, включая имена файлов и структуры папок на съемных дисках. Уже зашифрованные съемные диски Kaspersky Endpoint Security повторно не шифрует.

     > Этот вариант шифрования обеспечивается функциональностью шифрования жестких дисков программы Kaspersky Endpoint Security.

   - **Шифровать все файлы**. Если выбран этот элемент, то при применении политики Kaspersky Security Center с заданными параметрами шифрования съемных дисков Kaspersky Endpoint Security шифрует все файлы, которые хранятся на съемных дисках. Уже зашифрованные файлы Kaspersky Endpoint Security повторно не шифрует. Программа не шифрует файловые системы съемных дисков, включая имена зашифрованных файлов и структуры папок.

   - **Шифровать только новые файлы**. Если выбран этот элемент, то при применении политики Kaspersky Security Center с заданными параметрами шифрования съемных дисков Kaspersky Endpoint Security шифрует только те файлы, которые были добавлены на съемные диски или которые хранились на съемных дисках и были изменены после последнего применения политики Kaspersky Security Center.

   - **Расшифровывать весь съемный диск**. Если выбран этот элемент, то при применении политики Kaspersky Security Center с заданными параметрами шифрования съемных дисков Kaspersky Endpoint Security расшифровывает все

зашифрованные файлы, которые хранятся на съемных дисках, а также их файловые системы, если они были зашифрованы.

> Этот вариант шифрования обеспечивается не только функциональностью шифрования файлов, но и функциональностью шифрования жестких дисков программы Kaspersky Endpoint Security.

- **Оставлять без изменений**. Если выбран этот элемент, то при применении политики Kaspersky Security Center с заданными параметрами шифрования съемных дисков Kaspersky Endpoint Security не шифрует и не расшифровывает файлы на съемных дисках.

8. Сформируйте (см. раздел "Добавление правила шифрования для съемных дисков" на стр. 327) правила шифрования файлов на съемных дисках, содержимое которых вы хотите зашифровать.

9. Примените политику.

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

Сразу после применения политики, если пользователь подключает съемный диск или съемный диск уже подключен, Kaspersky Endpoint Security информирует пользователя о том, что к съемному диску применяется правило шифрования, в соответствии с которым данные съемного диска будут зашифрованы.

> Если для шифрования данных на съемном диске задано правило *Оставлять без изменений*, то программа ни о чем не информирует пользователя.

Программа предупреждает пользователя, что процедура шифрования может занять некоторое время.

Программа запрашивает у пользователя подтверждение для выполнения операции шифрования и выполняет следующие действия:

- Шифрует данные в соответствии с параметрами политики, если пользователь подтверждает запрос на шифрование.

- Оставляет данные незашифрованными, если пользователь отклоняет запрос на шифрование, и ограничивает доступ к файлам съемного диска чтением.

- Оставляет данные незашифрованными, если пользователь не дает ответ на запрос на шифрование, ограничивает доступ к файлам съемного диска чтением и повторно запрашивает подтверждение шифрования данных при последующем применении политики Kaspersky Security Center или при последующем подключении съемного диска.

Политика Kaspersky Security Center с заданными параметрами шифрования данных съемных дисков формируется для определенной группы управляемых компьютеров. Поэтому результат шифрования данных съемных дисков зависит от того, к какому компьютеру подключен съемный диск.

Если во время шифрования данных пользователь инициирует безопасное извлечение съемного диска, Kaspersky Endpoint Security прерывает шифрование данных и позволяет извлечь съемный диск до завершения операции шифрования.

Добавление правила шифрования для съемных дисков

Чтобы добавить правило шифрования для съемных дисков, 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 добавить правила шифрования для съемных дисков.

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 **Шифрование данных** выберите подраздел **Шифрование съемных дисков**.

7. По левой кнопке мыши нажмите на кнопку **Добавить** и в раскрывающемся списке выберите один из следующих элементов:

   - Если вы хотите добавить правила шифрования для съемных дисков, которые находятся в списке доверенных устройств компонента Контроль устройств, выберите элемент **Из списка доверенных устройств данной политики**.

     Откроется окно **Добавление устройств из списка доверенных устройств**.

   - Если вы хотите добавить правила шифрования для съемных дисков, которые находятся в списке Kaspersky Security Center, выберите элемент **Из списка устройств Kaspersky Security Center**.

     Откроется окно **Добавление устройств из списка Kaspersky Security Center**.

8. Если на предыдущем шаге вы выбрали элемент **Из списка устройств Kaspersky Security Center**, задайте фильтры для отображения устройств в таблице. Для этого выполните следующие действия:

   a. Укажите значения параметров **Выводить в таблице устройства, для которых определено**, **Тип устройства**, **Название**, **Компьютер**, **Шифрование диска Kaspersky**.

   b. Нажмите на кнопку **Обновить**.

9. В графе **Тип устройств** установите флажки напротив названий тех съемных дисков в таблице, для которых вы хотите создать правила шифрования.

10. В раскрывающемся списке **Режим шифрования для выбранных устройств** выберите действие, которое выполняет Kaspersky Endpoint Security с файлами, хранящимися на выбранных съемных дисках.

11. Установите флажок **Портативный режим**, если вы хотите, чтобы перед шифрованием Kaspersky Endpoint Security выполнял подготовку съемных дисков к работе с зашифрованными на них файлами в портативном режиме.

    Портативный режим позволяет работать с зашифрованными файлами съемных дисков на компьютерах с недоступной функциональностью шифрования (см. стр. 370).

12. Установите флажок **Шифровать только занятое пространство**, если вы хотите, чтобы Kaspersky Endpoint Security шифровал только те сектора диска, которые заняты файлами.

    Если вы применяете шифрование на уже используемом диске, рекомендуется зашифровать весь диск. Это гарантирует защиту всех данных - даже удаленных, но еще содержащих извлекаемые сведения. Функцию **Шифровать только занятое пространство** рекомендуется использовать для новых, ранее не использовавшихся дисков.

    Если устройство было зашифровано ранее с использованием функции **Шифровать только занятое пространство**, после применения политики в режиме **Шифровать весь съемный диск** секторы, не занятые файлами, по-прежнему не будут зашифрованы.

13. В раскрывающемся списке **Действие для устройств, выбранных ранее** выберите действие, выполняемое Kaspersky Endpoint Security с правилами шифрования, которые были определены для съемных дисков ранее:

    - Если вы хотите, чтобы созданное ранее правило шифрования съемного диска осталось без изменений, выберите элемент **Пропустить**.
    - Если вы хотите, чтобы созданное ранее правило шифрования съемного диска было заменено новым правилом, выберите элемент **Обновить**.

14. Нажмите на кнопку **ОК**.

    Строки с параметрами созданных правил шифрования отобразятся в таблице **Правила, заданные вручную**.

15. Нажмите на кнопку **OK**, чтобы сохранить внесенные изменения.

Добавленные правила шифрования съемных дисков будут применены к съемным дискам, подключенным к любым компьютерам, работающим под управлением измененной политики Kaspersky Security Center.

Изменение правила шифрования для съемных дисков

Чтобы изменить правило шифрования для съемного диска, 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 изменить правило шифрования для съемного диска.
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 **Шифрование данных** выберите подраздел **Шифрование съемных дисков**.
7. В списке съемных дисков, для которых определены правила шифрования, выберите запись о нужном вам съемном диске.
8. Нажмите на кнопку **Задать правило**, чтобы изменить правило шифрования для этого съемного диска.

   Откроется контекстное меню кнопки **Задать правило**.

9. В контекстном меню кнопки **Задать правило** выберите действие, которое выполняет Kaspersky Endpoint Security с файлами на выбранном съемном диске.

10. Нажмите на кнопку **OK**, чтобы сохранить внесенные изменения.

Измененные правила шифрования съемных дисков будут применены к съемным дискам, подключенным к любым компьютерам, работающим под управлением измененной политики Kaspersky Security Center.

Включение портативного режима для работы с зашифрованными файлами на съемных дисках

Чтобы включить портативный режим для работы с зашифрованными файлами на съемных дисках, 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 включить портативный режим для работы с зашифрованными файлами на съемных дисках.

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 **Шифрование данных** выберите подраздел **Шифрование съемных дисков**.

7. Установите флажок **Портативный режим**.

Портативный режим доступен только для шифрования всех или только новых файлов.

8. Нажмите на кнопку **ОК**.
9. Примените политику.

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

10. Подключите съемный диск к устройству, на которое была распространена политика Kaspersky Security Center.
11. Подтвердите операцию шифрования съемного диска.

    Откроется окно создания пароля для портативного файлового менеджера.

12. Задайте пароль, соответствующий требованиям к уровню сложности, и подтвердите его.
13. Нажмите на кнопку **ОК**.

Kaspersky Endpoint Security зашифрует файлы на съемном диске согласно правилам шифрования, заданным в политике Kaspersky Security Center. Портативный файловый менеджер для работы с зашифрованными файлами будет также записан на съемный диск.

После включения портативного режима становится доступной работа с зашифрованными файлами на съемных дисках, подключенных к компьютеру с недоступной функциональностью шифрования.

Расшифровка съемных дисков

Чтобы расшифровать съемные диски, 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 расшифровку съемных дисков.

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 **Шифрование данных** выберите подраздел **Шифрование съемных дисков**.

7. Если вы хотите расшифровать все зашифрованные файлы, хранящиеся на съемных дисках, в раскрывающемся списке **Режим шифрования** выберите действие **Расшифровывать весь съемный диск**.

8. Если вы хотите расшифровать данные, хранящиеся на отдельных съемных дисках, измените правила шифрования съемных дисков, данные которых вы хотите расшифровать. Для этого выполните следующие действия:

   a. В списке съемных дисков, для которых определены правила шифрования, выберите запись о нужном вам съемном диске.

   b. Нажмите на кнопку **Задать правило**, чтобы изменить правило шифрования для этого съемного диска.

      Откроется контекстное меню кнопки **Задать правило**.

   c. В контекстном меню кнопки **Задать правило** выберите пункт **Расшифровывать все файлы**.

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

10. Примените политику.

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

Сразу после применения политики, если пользователь подключает съемный диск или он уже подключен, Kaspersky Endpoint Security информирует пользователя о том, что к съемному диску применяется правило шифрования, в соответствии с которым зашифрованные файлы, хранящиеся на съемном диске, а также файловая система съемного диска, если она зашифрована, будут расшифрованы. Программа предупреждает пользователя, что процедура расшифровки может занять некоторое время.

Политика Kaspersky Security Center с заданными параметрами шифрования данных на съемных дисках формируется для определенной группы управляемых компьютеров. Поэтому результат расшифровки данных на съемных дисках зависит от того, к какому компьютеру подключен съемный диск.

Если во время расшифровки данных пользователь инициирует безопасное извлечение съемного диска, Kaspersky Endpoint Security прерывает расшифровку данных и позволяет извлечь съемный диск до завершения операции расшифровки.

Шифрование жестких дисков

Если программа Kaspersky Endpoint Security установлена на компьютере под управлением операционной системы Microsoft Windows для рабочих станций, то для шифрования доступны технологии Шифрование диска BitLocker и Шифрование диска Kaspersky. Если программа Kaspersky Endpoint Security установлена на компьютере под управлением операционной системы Microsoft Windows для файловых серверов (см. раздел "Аппаратные и программные требования" на стр. 24), то доступна только технология Шифрование диска BitLocker.

Этот раздел содержит информацию о шифровании жестких дисков и инструкции о том, как настроить и выполнить шифрование жестких дисков с помощью Kaspersky Endpoint Security и плагина управления Kaspersky Endpoint Security.

В этом разделе

О шифровании жестких дисков

Перед запуском шифрования жестких дисков программа выполняет ряд проверок на возможность шифрования устройства, в том числе и проверку совместимости системного жесткого диска с Агентом аутентификации и с компонентами шифрования BitLocker. Для проверки совместимости требуется выполнить перезагрузку компьютера. После перезагрузки компьютера программа в автоматическом режиме выполняет все необходимые проверки. Если проверка на совместимость проходит успешно, то после загрузки операционной системы и запуска программы запускается шифрование жестких дисков. Если в процессе проверки обнаруживается несовместимость системного жесткого диска с Агентом аутентификации или с компонентами шифрования BitLocker, требуется перезагрузить компьютер с помощью аппаратной кнопки (Reset). Kaspersky Endpoint Security фиксирует информацию о несовместимости, на основе которой не запускает шифрование жестких дисков после старта операционной системы. В отчетах Kaspersky Security Center выводится информация об этом событии.

Если аппаратная конфигурация компьютера изменилась, то для проверки системного жесткого диска на совместимость с Агентом аутентификации и компонентами шифрования BitLocker требуется удалить информацию о несовместимости, полученную программой при предыдущей проверке. Для этого перед шифрованием жестких дисков в командной строке требуется ввести команду `avp pbatestreset`. Если после проверки системного жесткого диска на совместимость с Агентом аутентификации операционная система не может запуститься, требуется удалить объекты и данные, оставшиеся после тестовой работы Агента аутентификации (см. раздел "Удаление объектов и данных, оставшихся после

тестовой работы Агента аутентификации" на стр. 60), с помощью утилиты восстановления, далее запустить Kaspersky Endpoint Security и выполнить команду `avp pbatestreset` повторно.

После запуска шифрования жестких дисков Kaspersky Endpoint Security шифрует все, что записывается на жесткие диски.

Если во время шифрования жестких дисков пользователь выключает или перезагружает компьютер, то перед последующей загрузкой операционной системы загружается Агент аутентификации. После прохождения процедуры аутентификации в агенте и загрузки операционной системы Kaspersky Endpoint Security возобновляет шифрование жестких дисков.

Если во время шифрования жестких дисков операционная система переходит в режим гибернации (hibernation mode), то при выводе операционной системы из режима гибернации загружается Агент аутентификации. После прохождения процедуры аутентификации в агенте и загрузки операционной системы Kaspersky Endpoint Security возобновляет шифрование жестких дисков.

Если во время шифрования жестких дисков операционная система переходит в спящий режим (sleep mode), то при выводе операционной системы из спящего режима Kaspersky Endpoint Security возобновляет шифрование жестких дисков без загрузки Агента аутентификации.

Аутентификация пользователя в Агенте аутентификации может выполняться двумя способами:

- путем ввода имени и пароля учетной записи Агента аутентификации, созданной администратором локальной сети организации средствами Kaspersky Security Center;
- путем ввода пароля подключенного к компьютеру токена или смарт-карты.

Агент аутентификации поддерживает раскладки клавиатуры для следующих языков:

- Английский (Великобритания);
- Английский (США);
- Арабский (Алжир, Марокко, Тунис, раскладка AZERTY);

- Испанский (Латинская Америка);
- Итальянский;
- Немецкий (Германия и Австрия);
- Немецкий (Швейцария);
- Португальский (Бразилия, раскладка ABNT2);
- Русский (для 105-клавишных клавиатур IBM / Windows с раскладкой ЙЦУКЕН);
- Турецкий (раскладка QWERTY);
- Французский (Франция);
- Французский (Швейцария);
- Французский (Бельгия, раскладка AZERTY);
- Японский (для 106-клавишных клавиатур с раскладкой QWERTY).

Раскладка клавиатуры становится доступной в Агенте аутентификации, если она добавлена в настройках языка и региональных стандартов операционной системы и доступна на экране приветствия Microsoft Windows.

Если имя учетной записи Агента аутентификации содержит символы, которые невозможно ввести с помощью доступных в Агенте аутентификации раскладок клавиатуры, то доступ к зашифрованным жестким дискам возможен только после их восстановления с помощью утилиты восстановления (см. раздел "Восстановление данных на зашифрованных устройствах с помощью утилиты восстановления" на стр. 385) или после восстановления имени и пароля учетной записи Агента аутентификации (см. раздел "Восстановление учетных данных Агента аутентификации" на стр. 362).

Kaspersky Endpoint Security работает со следующими токенами, считывателями смарт-карт и смарт-картами:

- SafeNet eToken PRO 64K (4.2b) (USB).
- SafeNet eToken PRO 72K Java (USB).
- SafeNet eToken PRO 72K Java (Smart Card).
- SafeNet eToken 4100 72K Java (Smart Card).
- SafeNet eToken 5100 (USB).
- SafeNet eToken 5105 (USB).
- SafeNet eToken 7300 (USB).
- EMC RSA SecurID 800 (USB).
- Рутокен ЭЦП (USB).
- Рутокен ЭЦП (Flash).
- Aladdin-RD JaCarta PKI (USB).
- Aladdin-RD JaCarta PKI (Smart Card).
- Athena IDProtect Laser (USB).
- Gemalto IDBridge CT40 (Reader).
- Gemalto IDPrime .NET 511.

Шифрование жестких дисков с помощью технологии Шифрование диска Kaspersky

Перед шифрованием жестких дисков компьютера рекомендуется убедиться в том, что компьютер не заражен. Для этого требуется запустить полную проверку или проверку важных областей компьютера (см. раздел "О задачах проверки" на стр. 412). Шифрование жесткого диска компьютера, зараженного руткитом, может привести к неработоспособности компьютера.

Чтобы зашифровать жесткие диски с помощью технологии Шифрование диска Kaspersky, 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 шифрование жестких дисков.
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 **Шифрование данных** выберите подраздел **Шифрование жестких дисков**.
7. В раскрывающемся списке **Технология шифрования** выберите вариант **Шифрование диска Kaspersky**.

   Применение технологии шифрования Шифрование диска Kaspersky невозможно, если на компьютере есть жесткие диски, зашифрованные с помощью BitLocker.

8. В раскрывающемся списке **Режим шифрования** выберите действие **Шифровать все жесткие диски**.

   Если на компьютере установлено несколько операционных систем, то после шифрования всех жестких дисков вы сможете выполнить загрузку только той операционной системы, в которой установлена программа.

Если некоторые жесткие диски нужно исключить из шифрования, сформируйте их список (см. раздел "Формирование списка жестких дисков для исключения из шифрования" на стр. 344).

9. Выберите один из следующих способов шифрования:

   - Если вы хотите применить шифрование только к тем секторам жесткого диска, которые заняты файлами, установите флажок **Шифровать только занятое пространство**.

     Если вы применяете шифрование на уже используемом диске, рекомендуется зашифровать весь диск. Это гарантирует защиту всех данных - даже удаленных, но еще содержащих извлекаемые сведения. Функцию **Шифровать только занятое пространство** рекомендуется использовать для новых, ранее не использовавшихся дисков.

   - Если вы хотите применить шифрование ко всему жесткому диску, снимите флажок **Шифровать только занятое пространство**.

     Эта функция применима только к незашифрованным устройствам. Если устройство было зашифровано ранее с использованием функции **Шифровать только занятое пространство**, после применения политики в режиме **Шифровать все жесткие диски** секторы, не занятые файлами, по-прежнему не будут зашифрованы.

10. Нажмите на кнопку **OK**, чтобы сохранить внесенные изменения.

11. Примените политику.

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

Шифрование жестких дисков с помощью технологии Шифрование диска BitLocker

Перед шифрованием жестких дисков компьютера рекомендуется убедиться в том, что компьютер не заражен. Для этого требуется запустить полную проверку или проверку важных областей компьютера (см. раздел "О задачах проверки" на стр. 412). Шифрование жесткого диска компьютера, зараженного руткитом, может привести к неработоспособности компьютера.

Для работы технологии Шифрование диска BitLocker на компьютерах с серверной операционной системой может потребоваться установка компонента **Шифрование диска BitLocker** с помощью мастера добавления ролей.

Чтобы зашифровать жесткие диски с помощью технологии Шифрование диска BitLocker, 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 шифрование жестких дисков.
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 **Шифрование данных** выберите подраздел **Шифрование жестких дисков**.

7. В раскрывающемся списке **Технология шифрования** выберите вариант **Шифрование диска BitLocker**.

8. В раскрывающемся списке **Режим шифрования** выберите пункт **Шифровать все жесткие диски**.

9. Если вы хотите использовать сенсорную клавиатуру для ввода информации в предзагрузочной среде, установите флажок **Разрешить использование аутентификации, требующей предзагрузочного ввода с клавиатуры на планшетах**.

   Рекомендуется использовать этот параметр только для устройств, у которых во время предварительной загрузки имеются альтернативные средства ввода данных, например USB-клавиатура.

10. Выберите один из следующих типов шифрования:

    - Если вы хотите использовать аппаратное шифрование, установите флажок **Использовать аппаратное шифрование**.
    - Если вы хотите использовать программное шифрование, снимите флажок **Использовать аппаратное шифрование**.

11. Выберите один из следующих способов шифрования:

    - Если вы хотите применить шифрование только к тем секторам жесткого диска, которые заняты файлами, установите флажок **Шифровать только занятое пространство**.
    - Если вы хотите применить шифрование ко всему жесткому диску, снимите флажок **Шифровать только занятое пространство**.

      Эта функция применима только к незашифрованным устройствам. Если устройство было зашифровано ранее с использованием функции **Шифровать только занятое пространство**, после применения политики в режиме **Шифровать все жесткие диски** секторы, не занятые файлами, по-прежнему не будут зашифрованы.

12. Выберите способ получения доступа к жестким дискам, зашифрованным с помощью BitLocker:

    - Если вы хотите использовать для хранения ключей шифрования доверенный платформенный модуль (TPM), выберите вариант **Использовать доверенный платформенный модуль (TPM)**.

    - Если вы не используете доверенный платформенный модуль (TPM) для шифрования жестких дисков, выберите вариант **Использовать пароль** и в поле **Минимальная длина пароля** укажите, какое минимальное количество символов должен содержать пароль.

    > Наличие доверенного платформенного модуля (TPM) является обязательным для операционных систем Windows 7 и Windows 2008 R2, а также более ранних версий.

13. Если на предыдущем шаге вы выбрали вариант **Использовать доверенный платформенный модуль (TPM)**, выполните следующие действия:

    - Если вы хотите установить PIN-код, который будет запрашиваться у пользователя при попытке доступа к ключу шифрования, установите флажок **Использовать PIN-код** и в поле **Минимальная длина PIN-кода** укажите, какое минимальное количество цифр должен содержать PIN-код.

    - Если вы хотите, чтобы в случае отсутствия на компьютере доверенного платформенного модуля доступ к зашифрованным жестким дискам можно было получить с помощью пароля, установите флажок **Использовать пароль, если доверенный платформенный модуль (TPM) недоступен** и в поле **Минимальная длина пароля** укажите, какое минимальное количество символов должен содержать пароль.

      В такой ситуации доступ к ключам шифрования будет осуществляться с помощью заданного пароля так же, как при установленном флажке **Использовать пароль**.

Если флажок **Использовать пароль, если доверенный платформенный модуль (TPM) недоступен** снят и доверенный платформенный модуль недоступен, то шифрование жестких дисков не запускается.

14. Нажмите на кнопку **OK**, чтобы сохранить внесенные изменения.

15. Примените политику.

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

После применения политики на клиентском компьютере с установленной программой Kaspersky Endpoint Security появляются следующие запросы:

- Если политика шифрования применяется к системному жесткому диску, то появится окно запроса ПИН-кода, если используется доверенный платформенный модуль, или окно запроса пароля для предзагрузочной аутентификации в противном случае.
- Если в операционной системе включен режим совместимости с Федеральным стандартом обработки информации (FIPS), то в операционных системах Windows 8 и выше появится окно запроса на подключение USB-устройства для сохранения файла ключа восстановления.

При отсутствии доступа к ключам шифрования пользователь может запросить у администратора локальной сети организации ключ восстановления (см. раздел "Передача пользователю ключа восстановления для жестких дисков, зашифрованных с помощью BitLocker" на стр. 382) (если ключ восстановления не был сохранен ранее на USB-устройстве или был утерян).

Формирование списка жестких дисков для исключения из шифрования

Вы можете сформировать список исключений из шифрования только для технологии Шифрование диска Kaspersky.

Чтобы сформировать список жестких дисков для исключения из шифрования, 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 сформировать список жестких дисков для исключения из шифрования.

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 **Шифрование данных** выберите подраздел **Шифрование жестких дисков**.

7. В раскрывающемся списке **Технология шифрования** выберите вариант **Шифрование диска Kaspersky**.

   В таблице **Не шифровать следующие жесткие диски** отобразятся записи о жестких дисках, которые программа не будет шифровать. Если вы ранее не сформировали список жестких дисков для исключения из шифрования, эта таблица пуста.

8. Если вы хотите добавить жесткие диски в список жестких дисков, которые программа не будет шифровать, выполните следующие действия:

   a. Нажмите на кнопку **Добавить**.

      Откроется окно **Добавление устройств из списка Kaspersky Security Center**.

   b. В окне **Добавление устройств из списка Kaspersky Security Center** укажите значения параметров **Название**, **Компьютер**, **Тип диска**, **Шифрование диска Kaspersky**.

c. Нажмите на кнопку **Обновить**.

d. В графе **Название** установите флажки в строках таблицы, соответствующих тем жестким дискам, которые вы хотите добавить в список жестких дисков для исключения из шифрования.

e. Нажмите на кнопку **OK**.

Выбранные жесткие диски отобразятся в таблице **Не шифровать следующие жесткие диски**.

9. Если вы хотите удалить жесткие диски из таблицы исключений, выберите одну или несколько строк в таблице **Не шифровать следующие жесткие диски** и нажмите на кнопку **Удалить**.

> Чтобы выбрать несколько строк в таблице, выделяйте их, удерживая клавишу **CTRL**.

10. Нажмите на кнопку **OK**, чтобы сохранить внесенные изменения.

Расшифровка жестких дисков

> Вы можете расшифровать жесткие диски даже при отсутствии действующей лицензии, допускающей шифрование данных.

Чтобы расшифровать жесткие диски, 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 расшифровку жестких дисков.
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 **Шифрование данных** выберите подраздел **Шифрование жестких дисков**.

7. В раскрывающемся списке **Технология шифрования** выберите ту технологию, с помощью которой были зашифрованы жесткие диски.

8. Выполните одно из следующих действий:

   - В раскрывающемся списке **Режим шифрования** выберите элемент **Расшифровывать все жесткие диски**, если вы хотите расшифровать все зашифрованные жесткие диски.
   - В таблицу **Не шифровать следующие жесткие диски** добавьте (см. раздел "Формирование списка жестких дисков для исключения из шифрования" на стр. 344) те зашифрованные жесткие диски, которые вы хотите расшифровать.

     > Этот вариант доступен только для технологии шифрования Шифрование диска Kaspersky.

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

10. Примените политику.

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

Если во время расшифровки жестких дисков, зашифрованных с помощью технологии Шифрование диска Kaspersky, пользователь выключает или перезагружает компьютер, то перед последующей загрузкой операционной системы загружается Агент аутентификации. После прохождения процедуры аутентификации в агенте и загрузки операционной системы Kaspersky Endpoint Security возобновляет расшифровку жестких дисков.

Если во время расшифровки жестких дисков, зашифрованных с помощью технологии Шифрование диска Kaspersky, операционная система переходит в режим гибернации (hibernation mode), то при выводе операционной системы из режима гибернации загружается Агент аутентификации. После прохождения процедуры аутентификации в агенте и загрузки операционной системы Kaspersky Endpoint Security возобновляет расшифровку жестких дисков. После расшифровки жестких дисков режим гибернации недоступен до первой перезагрузки операционной системы.

Если во время расшифровки жестких дисков операционная система переходит в спящий режим (sleep mode), то при выводе операционной системы из спящего режима Kaspersky Endpoint Security возобновляет расшифровку жестких дисков без загрузки Агента аутентификации.

Работа с Агентом аутентификации

Если системные жесткие диски зашифрованы, перед загрузкой операционной системы загружается Агент аутентификации. С помощью Агента аутентификации требуется пройти процедуру аутентификации для получения доступа к зашифрованным системным жестким дискам и загрузки операционной системы.

После успешного прохождения процедуры аутентификации загружается операционная система. При последующих перезагрузках операционной системы требуется повторно проходить процедуру аутентификации.

Возможны случаи, когда пользователь не может пройти процедуру аутентификации. Например, аутентификация невозможна, если пользователь забыл учетные данные Агента аутентификации, пароль от токена или смарт-карты или потерял токен или смарт-карту.

Если пользователь забыл учетные данные Агента аутентификации или пароль от токена или смарт-карты, то для восстановления требуется обратиться к администратору локальной сети организации.

Если пользователь потерял токен или смарт-карту, администратору требуется добавить файл электронного сертификата (см. раздел "Использование токена и смарт-карты при работе с Агентом аутентификации" на стр. 349) нового токена или новой смарт-карты в команду для создания учетной записи Агента аутентификации. После этого пользователю требуется пройти процедуру восстановления данных на зашифрованных устройствах (см.

раздел "Работа с зашифрованными устройствами при отсутствии доступа к ним" на стр. 376).

В этом разделе

Использование токена и смарт-карты при работе с Агентом аутентификации

При аутентификации для доступа к зашифрованным жестким дискам можно использовать токен или смарт-карту. Для этого необходимо добавить файл электронного сертификата токена или смарт-карты в команду для создания учетной записи Агента аутентификации.

Использование токена или смарт-карты доступно, только если жесткие диски компьютера зашифрованы с помощью алгоритма шифрования AES256. Если жесткие диски компьютера зашифрованы с помощью алгоритма шифрования AES56, то в добавлении файла электронного сертификата в команду будет отказано.

Чтобы добавить файл электронного сертификата токена или смарт-карты в команду для создания учетной записи Агента аутентификации, его требуется предварительно сохранить с помощью стороннего программного обеспечения, предназначенного для управления сертификатами.

Сертификат токена или смарт-карты должен обладать следующими свойствами:

- Сертификат удовлетворяет стандарту X.509, а файл сертификата имеет кодировку DER.

  Если электронный сертификат токена или смарт-карты не удовлетворяет этому требованию, плагин управления не загружает файл такого сертификата в команду для создания учетной записи Агента аутентификации и выводит ошибку.

- Параметр `KeyUsage`, определяющий назначение сертификата, должен иметь значение `keyEncipherment` или `dataEncipherment`.

  Если электронный сертификат токена или смарт-карты не удовлетворяет этому требованию, плагин управления загружает файл такого сертификата в команду для создания учетной записи Агента аутентификации с предупреждением.

- Сертификат содержит RSA-ключ длиной не менее 1024 бит.

  Если электронный сертификат токена или смарт-карты не удовлетворяет этому требованию, плагин управления не загружает файл такого сертификата в команду для создания учетной записи Агента аутентификации и выводит ошибку.

Изменение справочных текстов Агента аутентификации

Перед изменением справочных текстов Агента аутентификации ознакомьтесь со списком поддерживаемых символов в предзагрузочной среде (см. раздел "Ограничения поддержки символов в справочных текстах Агента аутентификации" на стр. 352).

Чтобы изменить справочные тексты Агента аутентификации, 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 изменить справочные тексты Агента аутентификации.

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 **Шифрование данных** выберите подраздел **Общие параметры шифрования**.

7. Нажмите на кнопку **Справка** в блоке **Шаблоны**.

   Откроется окно **Справочные тексты Агента аутентификации**.

8. Выполните следующие действия:

   - Выберите закладку **Аутентификация**, если вы хотите изменить справочный текст, отображающийся в окне Агента аутентификации на этапе ввода учетных данных.

   - Выберите закладку **Смена пароля**, если вы хотите изменить справочный текст, отображающийся в окне Агента аутентификации на этапе смены пароля для учетной записи Агента аутентификации.

   - Выберите закладку **Восстановление пароля**, если вы хотите изменить справочный текст, отображающийся в окне Агента аутентификации на этапе восстановления пароля для учетной записи Агента аутентификации.

9. Измените справочные тексты.

   Если вы хотите восстановить исходный текст, нажмите на кнопку **По умолчанию**.

> Вы можете ввести справочный текст, содержащий 16 или менее строк. Максимальная длина строки составляет 64 символа.

10. Нажмите на кнопку **OK**.
11. В окне **Свойства: <Название политики>** нажмите на кнопку **OK**, чтобы сохранить внесенные изменения.

Ограничения поддержки символов в справочных текстах Агента аутентификации

В предзагрузочной среде поддерживаются следующие символы Unicode:

- основная латиница (0000 - 007F);
- дополнительные символы Latin-1 (0080 - 00FF);
- расширенная латиница-A (0100 - 017F);
- расширенная латиница-B (0180 - 024F);
- некомбинируемые протяженные символы-идентификаторы (02B0 - 02FF);
- комбинируемые диакритические знаки (0300 - 036F);
- греческий и коптский алфавиты (0370 - 03FF);
- кириллица (0400 - 04FF);
- иврит (0590 - 05FF);
- арабское письмо (0600 - 06FF);
- дополнительная расширенная латиница (1E00 - 1EFF);
- знаки пунктуации (2000 - 206F);
- символы валют (20A0 - 20CF);

- буквоподобные символы (2100 - 214F);
- геометрические фигуры (25A0 - 25FF);
- формы представления арабских букв-B (FE70 - FEFF).

Символы, не указанные в этом списке, не поддерживаются в предзагрузочной среде. Не рекомендуется использовать такие символы в справочных текстах Агента аутентификации.

Выбор уровня трассировки Агента аутентификации

Программа записывает служебную информацию о работе Агента аутентификации, а также информацию о действиях, которые выполняет пользователь в Агенте аутентификации, в файл трассировки. Файл трассировки Агента аутентификации может быть полезен для восстановления данных на зашифрованных жестких дисках (см. раздел "Работа с зашифрованными устройствами при отсутствии доступа к ним" на стр. 376).

Чтобы выбрать уровень трассировки Агента аутентификации, выполните следующие действия:

1. Сразу после запуска компьютера с зашифрованными жесткими дисками по кнопке **F3** вызовите окно для настройки параметров Агента аутентификации.
2. В окне настройки параметров Агента аутентификации выберите уровень трассировки:
   - **Disable debug logging (default)**. Если выбран этот вариант, то программа не записывает информацию о событиях работы Агента аутентификации в файл трассировки.
   - **Enable debug logging**. Если выбран этот вариант, то программа записывает информацию о работе Агента аутентификации и действиях, которые выполняет пользователь в Агенте аутентификации, в файл трассировки.
   - **Enable verbose logging**. Если выбран этот вариант, то программа записывает детальную информацию о работе Агента аутентификации и действиях, которые выполняет пользователь в Агенте аутентификации, в файл трассировки.

Уровень детализации записей для этого варианта выше, чем при выборе уровня **Enable debug logging**. Высокий уровень детализации записей может замедлять загрузку Агента аутентификации и операционной системы.

- **Enable debug logging and select serial port**. Если выбран этот вариант, то программа записывает информацию о работе Агента аутентификации и действиях, которые выполняет пользователь в Агенте аутентификации, в файл трассировки, а также передает ее через COM-порт.

  Если компьютер с зашифрованными жесткими дисками соединен с другим компьютером через COM-порт, то события работы Агента аутентификации можно исследовать с помощью этого компьютера.

- **Enable verbose debug logging and select serial port**. Если выбран этот вариант, то программа записывает детальную информацию о работе Агента аутентификации и действиях, которые выполняет пользователь в Агенте аутентификации, в файл трассировки, а также передает ее через COM-порт.

  Уровень детализации записей для этого варианта выше, чем при выборе уровня **Enable debug logging and select serial port**. Высокий уровень детализации записей может замедлять загрузку Агента аутентификации и операционной системы.

Запись в файл трассировки Агента аутентификации выполняется в случае, если на компьютере есть зашифрованные жесткие диски или выполняется шифрование жестких дисков.

Файл трассировки Агента аутентификации не передается в "Лабораторию Касперского", как другие файлы трассировки программы. При необходимости системный администратор может самостоятельно отправить файл трассировки Агента аутентификации в "Лабораторию Касперского" для анализа.

Управление учетными записями Агента аутентификации

Для управления учетными записями Агента аутентификации вы можете использовать следующие инструменты Kaspersky Security Center:

- Групповая задача управления учетными записями Агента аутентификации. С помощью этой задачи вы можете управлять учетными записями Агента аутентификации для группы клиентских компьютеров.

- Локальная задача **Шифрование (управление учетными записями)**. С помощью этой задачи вы можете управлять учетными записями Агента аутентификации для отдельных клиентских компьютеров.

Чтобы настроить параметры задачи для управления учетными записями Агента аутентификации, выполните следующие действия:

1. Создайте (см. раздел "Создание локальной задачи" на стр. 528, "Создание групповой задачи" на стр. 529) задачу управления учетными записями Агента аутентификации.

2. Откройте (см. раздел "Изменение параметров задачи" на стр. 533) раздел **Параметры** окна **Свойства: <название задачи управления учетными записями Агента аутентификации>**.

3. Добавьте команды для создания учетных записей Агента аутентификации (см. раздел "Добавление команды для создания учетной записи Агента аутентификации" на стр. 356).

4. Добавьте команды для изменения учетных записей Агента аутентификации (см. раздел "Добавление команды для изменения учетной записи Агента аутентификации" на стр. 359).

5. Добавьте команды для удаления учетных записей Агента аутентификации (см. раздел "Добавление команды для удаления учетной записи Агента аутентификации" на стр. 361).

6. Если требуется, измените добавленные команды для управления учетными записями Агента аутентификации. Для этого в таблице **Команды для управления учетными**

записями Агента аутентификации выберите команду и нажмите на кнопку **Изменить**.

7. Если требуется, удалите добавленные команды для управления учетными записями Агента аутентификации. Для этого в таблице **Команды для управления учетными записями Агента аутентификации** выберите одну или несколько команд и нажмите на кнопку **Удалить**.

   > Чтобы выбрать несколько строк в таблице, выделяйте их, удерживая клавишу **CTRL**.

8. В окне свойств задачи нажмите на кнопку **OK**, чтобы сохранить внесенные изменения.

9. Запустите задачу (см. раздел "Запуск, остановка, приостановка и возобновление выполнения задачи" на стр. 530).

Команды по управлению учетными записями Агента аутентификации, добавленные в задачу, будут выполнены.

Добавление команды для создания учетной записи Агента аутентификации

Чтобы добавить команду для создания учетной записи Агента аутентификации, выполните следующие действия:

1. Откройте (см. раздел "Изменение параметров задачи" на стр. 533) раздел **Параметры** окна **Свойства: <название задачи управления учетными записями Агента аутентификации>**.

2. Нажмите на кнопку **Добавить** и в раскрывающемся списке выберите элемент **Команду для добавления учетной записи**.

   Откроется окно **Добавление учетной записи пользователя**.

3. В окне **Добавление учетной записи пользователя** в поле **Учетная запись Windows** укажите имя учетной записи Microsoft Windows, на основе которой будет создана учетная запись для Агента аутентификации.

Для этого введите имя учетной записи вручную или воспользуйтесь кнопкой **Выбрать**.

4. Если вы ввели имя учетной записи Microsoft Windows вручную, нажмите на кнопку **Разрешить**, чтобы определить идентификатор безопасности (SID, Security Identifier) учетной записи.

   Если вы не определяете идентификатор безопасности по кнопке **Разрешить**, то он будет определен в момент выполнения задачи на компьютере.

   > Определение идентификатора безопасности учетной записи Microsoft Windows на этапе добавления команды для создания учетной записи Агента аутентификации может быть удобно для того, чтобы проверить корректность введенного вручную имени учетной записи Microsoft Windows. В случае если введенная учетная запись Microsoft Windows не существует, находится в недоверенном домене или не на компьютере, для которого изменяется локальная задача **Шифрование (управление учетными записями)**, то задача управления учетными записями Агента аутентификации будет завершена с ошибкой.

5. Установите флажок **Заменить существующую учетную запись**, если хотите, чтобы уже заведенная для Агента аутентификации учетная запись с таким же именем была заменена на добавляемую.

   > Этот шаг доступен, если вы добавляете команду для создания учетной записи Агента аутентификации в свойствах групповой задачи управления учетными записями Агента аутентификации. Этот шаг недоступен, если вы добавляете команду для создания учетной записи Агента аутентификации в свойствах локальной задачи **Шифрование (управление учетными записями)**.

6. В поле **Имя пользователя** введите имя учетной записи Агента аутентификации, которое требуется вводить при аутентификации для доступа к зашифрованным жестким дискам.

7. Установите флажок **Разрешать вход по паролю**, если вы хотите, чтобы при аутентификации для получения доступа к зашифрованным жестким дискам программа требовала пароль учетной записи Агента аутентификации.

8. Если на предыдущем шаге вы установили флажок **Разрешать вход по паролю**, выполните следующие действия:

    a. В поле **Пароль** введите пароль учетной записи Агента аутентификации, который требуется вводить при аутентификации для доступа к зашифрованным жестким дискам.

    b. В поле **Подтверждение пароля** повторите введенный на предыдущем шаге пароль учетной записи Агента аутентификации.

    c. Выполните одно из следующих действий:

    - Выберите вариант **Сменить пароль при первой аутентификации**, если вы хотите, чтобы программа требовала сменить пароль от пользователя, в первый раз проходящего процедуру аутентификации под учетной записью, указанной в команде.
    - В противном случае выберите вариант **Не требовать смену пароля**.

9. Установите флажок **Разрешать вход по сертификату**, если вы хотите, чтобы при аутентификации для доступа к зашифрованным жестким дискам программа требовала подключения токена или смарт-карты к компьютеру.

10. Если на предыдущем шаге вы установили флажок **Разрешать вход по сертификату**, нажмите на кнопку **Обзор** и в окне **Выбор файла сертификата** укажите файл электронного сертификата токена или смарт-карты.

11. Если требуется, в поле **Описание команды** введите информацию об учетной записи Агента аутентификации, необходимую вам для работы с командой.

12. Выполните одно из следующих действий:

    - Установите флажок **Разрешать аутентификацию**, если вы хотите, чтобы программа разрешала доступ к аутентификации в Агенте аутентификации пользователю, работающему под учетной записью, указанной в команде.

    - Установите флажок **Запрещать аутентификацию**, если вы хотите, чтобы программа запрещала доступ к аутентификации в Агенте аутентификации пользователю, работающему под учетной записью, указанной в команде.

13. В окне **Добавление учетной записи пользователя** нажмите на кнопку **OK**.

Добавление команды для изменения учетной записи Агента аутентификации

Чтобы добавить команду для изменения учетной записи Агента аутентификации, выполните следующие действия:

1. В разделе **Параметры** окна **Свойства: <название задачи управления учетными записями Агента аутентификации>** в контекстном меню кнопки **Добавить** выберите пункт **Команду для изменения учетной записи**.

   Откроется окно **Изменение учетной записи пользователя**.

2. В окне **Изменение учетной записи пользователя** в поле **Учетная запись Windows** укажите имя учетной записи пользователя Microsoft Windows, на основе которой создана учетная запись для Агента аутентификации, которую вы хотите изменить. Для этого введите имя учетной записи вручную или воспользуйтесь кнопкой **Выбрать**.

3. Если вы ввели имя учетной записи пользователя Microsoft Windows вручную, нажмите на кнопку **Разрешить**, чтобы определить идентификатор безопасности (SID, Security Identifier) учетной записи пользователя.

   Если вы не определяете идентификатор безопасности по кнопке **Разрешить**, то он будет определен в момент выполнения задачи на компьютере.

   > Определение идентификатора безопасности учетной записи пользователя Microsoft Windows на этапе добавления команды для изменения учетной записи Агента аутентификации может быть удобно для того, чтобы проверить корректность введенного вручную имени учетной записи пользователя Microsoft Windows. В случае если введенная учетная запись пользователя Microsoft Windows не существует или находится в недоверенном домене, то групповая задача управления учетными записями Агента аутентификации будет завершена с ошибкой.

4. Установите флажок **Изменить имя пользователя** и введите новое имя учетной записи Агента аутентификации, если вы хотите, чтобы для всех учетных записей Агента аутентификации, созданных на основе учетной записи пользователя Microsoft Windows с именем, указанным в поле **Учетная запись Windows**, программа Kaspersky Endpoint Security изменила имя пользователя на указанное в поле ниже.

5. Установите флажок **Изменить параметры входа по паролю**, если вы хотите сделать доступными для изменения параметры входа по паролю.

6. Установите флажок **Разрешать вход по паролю**, если вы хотите, чтобы при аутентификации для получения доступа к зашифрованным жестким дискам программа требовала пароль учетной записи Агента аутентификации.

7. Если на предыдущем шаге вы установили флажок **Разрешать вход по паролю**, выполните следующие действия:

    a. В поле **Пароль** введите новый пароль учетной записи Агента аутентификации.

    b. В поле **Подтверждение пароля** повторите введенный на предыдущем шаге пароль.

8. Установите флажок **Изменить правило смены пароля при аутентификации в Агенте аутентификации**, если вы хотите, чтобы для всех учетных записей Агента аутентификации, созданных на основе учетной записи пользователя Microsoft Windows с именем, указанным в поле **Учетная запись Windows**, программа Kaspersky Endpoint Security изменила значение параметра смены пароля на установленное ниже.

9. Установите значение параметра смены пароля при аутентификации в Агенте аутентификации.

10. Установите флажок **Изменить параметры входа по сертификату**, если вы хотите сделать доступными для изменения параметры входа по электронному сертификату токена или смарт-карте.

11. Установите флажок **Разрешать вход по сертификату**, если вы хотите, чтобы при аутентификации для доступа к зашифрованным жестким дискам программа требовала ввод пароля к подключенному к компьютеру токену или смарт-карте.

12. Если на предыдущем шаге вы установили флажок **Разрешать вход по сертификату**, нажмите на кнопку **Обзор** и в окне **Выбор файла сертификата** укажите файл электронного сертификата токена или смарт-карты.

13. Установите флажок **Изменить описание команды** и измените описание команды, если вы хотите, чтобы для всех учетных записей Агента аутентификации, созданных на основе учетной записи пользователя Microsoft Windows с именем, указанным в поле **Учетная запись Windows**, программа Kaspersky Endpoint Security изменила описание команды.

14. Установите флажок **Изменить правило доступа к аутентификации в Агенте аутентификации**, если вы хотите, чтобы для всех учетных записей Агента аутентификации, созданных на основе учетной записи пользователя Microsoft Windows с именем, указанным в поле **Учетная запись Windows**, программа Kaspersky Endpoint Security изменила правило доступа пользователя к аутентификации в Агенте аутентификации на установленное ниже.

15. Установите правило доступа к аутентификации в Агенте аутентификации.

16. В окне **Изменение учетной записи пользователя** нажмите на кнопку **OK**.

Добавление команды для удаления учетной записи Агента аутентификации

Чтобы добавить команду для удаления учетной записи Агента аутентификации, выполните следующие действия:

1. В разделе **Параметры** окна **Свойства: <название задачи управления учетными записями Агента аутентификации>** в контекстном меню кнопки **Добавить** выберите пункт **Команду для удаления учетной записи**.

   Откроется окно **Удаление учетной записи пользователя**.

2. В окне **Удаление учетной записи пользователя** в поле **Учетная запись Windows** укажите имя учетной записи пользователя Microsoft Windows, на основе которой создана учетная запись для Агента аутентификации, которую вы хотите удалить. Для этого введите имя учетной записи вручную или воспользуйтесь кнопкой **Выбрать**.

3. Если вы ввели имя учетной записи пользователя Microsoft Windows вручную, нажмите на кнопку **Разрешить**, чтобы определить идентификатор безопасности (SID, Security Identifier) учетной записи пользователя.

   Если вы не определяете идентификатор безопасности по кнопке **Разрешить**, то он будет определен в момент выполнения задачи на компьютере.

   > Определение идентификатора безопасности учетной записи пользователя Microsoft Windows на этапе добавления команды для удаления учетной записи Агента аутентификации может быть удобно для того, чтобы проверить корректность введенного вручную имени учетной записи пользователя Microsoft Windows. В случае если введенная учетная запись пользователя Microsoft Windows не существует или находится в недоверенном домене, то групповая задача управления учетными записями Агента аутентификации будет завершена с ошибкой.

4. В окне **Удаление учетной записи пользователя** нажмите на кнопку **OK**.

Восстановление учетных данных Агента аутентификации

> Эта инструкция адресована пользователям клиентских компьютеров с установленной программой Kaspersky Endpoint Security.

Чтобы восстановить имя и пароль учетной записи Агента аутентификации, выполните следующие действия:

1. Перед загрузкой операционной системы на компьютере с зашифрованными жесткими дисками загружается Агент аутентификации. В интерфейсе Агента аутентификации нажмите на кнопку **Forgot your password**, чтобы инициировать процедуру восстановления имени и пароля учетной записи Агента аутентификации.

2. Следуйте указаниям Агента аутентификации, чтобы получить блоки запроса для восстановления имени и пароля учетной записи Агента аутентификации.

3. Продиктуйте содержимое блоков запроса администратору локальной сети организации вместе с именем компьютера.

4. Введите блоки ответа на запрос о восстановлении имени и пароля учетной записи Агента аутентификации, сформированные и переданные (см. раздел "Ответ на запрос пользователя о восстановлении учетных данных Агента аутентификации" на стр. 363) вам администратором локальной сети организации.

5. Введите новый пароль для учетной записи Агента аутентификации и его подтверждение.

   Имя учетной записи Агента аутентификации определяется с помощью блоков ответа на запрос о восстановлении имени и пароля учетной записи Агента аутентификации.

После ввода и подтверждения нового пароля учетной записи Агента аутентификации пароль будет сохранен, а доступ к зашифрованным жестким дискам будет предоставлен.

Ответ на запрос пользователя о восстановлении учетных данных Агента аутентификации

Чтобы сформировать и передать пользователю блоки ответа на запрос о восстановлении имени и пароля учетной записи Агента аутентификации, 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 восстановление имени и пароля учетной записи Агента аутентификации.

3. В рабочей области выберите закладку **Устройства**.

4. На закладке **Устройства** выделите компьютер пользователя, запросившего восстановление имени и пароля учетной записи Агента аутентификации, и по правой клавише мыши откройте контекстное меню.

5. В контекстном меню выберите пункт **Предоставление доступа к устройствам и данным в офлайн-режиме**.

   Откроется окно **Предоставление доступа к устройствам и данным в офлайн-режиме**.

6. В окне **Предоставление доступа к устройствам и данным в офлайн-режиме** выберите закладку **Агент аутентификации**.

7. В блоке **Используемый алгоритм шифрования** выберите тип алгоритма шифрования.

8. В раскрывающемся списке **Учетная запись** выберите имя учетной записи Агента аутентификации, созданной для пользователя, запросившего восстановление имени и пароля учетной записи Агента аутентификации.

9. В раскрывающемся списке **Жесткий диск** выберите зашифрованный жесткий диск, доступ к которому необходимо восстановить.

10. В блоке **Запрос пользователя** введите блоки запроса, продиктованные пользователем.

    Содержимое блоков ответа на запрос пользователя о восстановлении имени и пароля учетной записи Агента аутентификации отобразится в поле **Ключ доступа**.

11. Продиктуйте содержимое блоков ответа пользователю.

Просмотр информации о шифровании данных

Этот раздел содержит инструкции о том, как просматривать информацию о шифровании данных.

В этом разделе

О статусах шифрования

В процессе шифрования и расшифровки данных Kaspersky Endpoint Security отправляет на Kaspersky Security Center информацию о статусах применения параметров шифрования на клиентских компьютерах.

Возможны следующие статусы шифрования:

- *Политика не определена*. Для компьютера не назначена политика Kaspersky Security Center.
- *Идет шифрование / расшифровка*. На компьютере выполняется шифрование и / или расшифровка данных.
- *Ошибка*. Во время шифрования и / или расшифровки данных на компьютере возникла ошибка.
- *Требуется перезагрузка*. Для инициализации или завершения шифрования или расшифровки данных на компьютере требуется перезагрузка операционной системы.
- *Соответствует политике*. Шифрование и / или расшифровка данных на компьютере выполнена в соответствии с параметрами шифрования, указанными в примененной к компьютеру политике Kaspersky Security Center.

- *Отменено пользователем*. Пользователь отказался подтвердить выполнение операции шифрования файлов на съемном диске.

- *Не поддерживается*. На компьютере недоступна функциональность шифрования данных.

Просмотр статусов шифрования

Чтобы просмотреть статус шифрования данных компьютера, 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 компьютер.

3. В рабочей области выберите закладку **Устройства**.

   На закладке **Устройства** в рабочей области отображаются свойства компьютеров выбранной группы администрирования.

4. На закладке **Устройства** рабочей области сдвиньте полосу прокрутки до упора вправо.

   В графе **Статус шифрования** отображаются статусы шифрования данных для компьютеров выбранной группы администрирования. Этот статус формируется на основе информации о шифровании файлов на локальных дисках компьютера, шифровании жестких дисков компьютера и шифровании съемных дисков, подключенных к компьютеру.

Просмотр статистики шифрования на информационных панелях Kaspersky Security Center

Чтобы просмотреть статусы шифрования на информационных панелях Kaspersky Security Center, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве консоли выберите узел **Сервер администрирования – <Имя компьютера>**.
3. В рабочей области, расположенной справа от дерева Консоли администрирования, выберите закладку **Статистика**.
4. Создайте новую страницу с информационными панелями со статистикой шифрования данных. Для этого выполните следующие действия:
    a. На закладке **Статистика** нажмите на кнопку **Настроить вид**.

    Откроется окно **Свойства: Статистика**.

    b. В окне **Свойства: Статистика** нажмите на кнопку **Добавить**.

    Откроется окно **Свойства: Новая страница**.

    c. В разделе **Общие** окна **Свойства: Новая страница** введите название страницы.

    d. В разделе **Информационные панели** нажмите на кнопку **Добавить**.

    Откроется окно **Новая информационная панель**.

    e. В окне **Новая информационная панель** в группе **Состояние защиты** выберите элемент **Шифрование устройств**.

    f. Нажмите на кнопку **OK**.

    Откроется окно **Свойства: Шифрование устройств**.

g. Измените при необходимости параметры информационной панели. Для этого воспользуйтесь разделами **Вид** и **Устройства** окна **Свойства: Шифрование устройств**.

h. Нажмите на кнопку **OK**.

i. Повторите пункты d – h инструкции, при этом в окне **Новая информационная панель** в группе **Состояние защиты** выберите элемент **Шифрование съемных дисков**.

Добавленные информационные панели отобразятся в списке **Информационные панели** окна **Свойства: Новая страница**.

j. В окне **Свойства: Новая страница** нажмите на кнопку **OK**.

Название созданной на предыдущих шагах страницы с информационными панелями отобразится в списке **Страницы** окна **Свойства: Статистика**.

k. В окне **Свойства: Статистика** нажмите на кнопку **Закрыть**.

5. На закладке **Статистика** откройте страницу, созданную на предыдущих шагах инструкции.

Отобразятся информационные панели, на которых вы можете просмотреть статусы шифрования компьютеров и съемных дисков.

Просмотр ошибок шифрования файлов на локальных дисках компьютера

Чтобы просмотреть ошибки шифрования файлов на локальных дисках компьютера, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.

2. В папке **Управляемые устройства** дерева Консоли администрирования откройте папку с названием группы администрирования, где находится компьютер пользователя, для которого вы хотите просмотреть список ошибок шифрования файлов.

3. В рабочей области выберите закладку **Устройства**.

4. На закладке **Устройства** выделите в списке компьютер и по правой клавише мыши вызовите контекстное меню.

5. Выполните одно из следующих действий:

   - В контекстном меню компьютера выберите пункт **Защита**.

   - В контекстном меню компьютера выберите пункт **Свойства**. В открывшемся окне **Свойства: <название компьютера>** выберите раздел **Защита**.

6. В разделе **Защита** окна **Свойства: <название компьютера>** по ссылке **Просмотреть ошибки шифрования данных** откройте окно **Ошибки шифрования данных**.

   В этом окне отображается информация об ошибках шифрования файлов на локальных дисках компьютера. Если ошибка исправлена, то Kaspersky Security Center удаляет информацию о ней из окна **Ошибки шифрования данных**.

Просмотр отчета о шифровании данных

Чтобы просмотреть отчет о шифровании данных, 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. В окне **Выбор типа шаблона отчета** в разделе **Прочее** выберите один из следующих пунктов:

   - **Отчет о статусе шифрования управляемых устройств**.

   - **Отчет о шифровании устройств хранения данных**.

- **Отчет об ошибках шифрования**.
- **Отчет о блокировании доступа к зашифрованным файлам**.

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.

Запустится процесс формирования отчета. Отчет отобразится в новом окне.

Работа с зашифрованными файлами при ограниченной функциональности шифрования файлов

При применении политики Kaspersky Security Center и последующем шифровании файлов Kaspersky Endpoint Security получает ключ шифрования, необходимый для прямого доступа к зашифрованным файлам. С помощью ключа шифрования пользователь, работающий под любой из учетных записей Windows, которая была активной во время шифрования файлов, может получать прямой доступ к зашифрованным файлам. Пользователям, работающим под учетными записями Windows, которые были неактивны во время шифрования файлов, требуется связь с Kaspersky Security Center для доступа к зашифрованным файлам.

Зашифрованные файлы могут быть недоступны в следующих случаях:

- На компьютере пользователя присутствуют ключи шифрования, но нет связи с Kaspersky Security Center для работы с ними. В этом случае пользователю требуется запросить доступ к зашифрованным файлам у администратора локальной сети организации.

  При отсутствии связи с Kaspersky Security Center требуется:

  - для доступа к зашифрованным файлам на жестких дисках компьютера запросить один ключ доступа;
  - для доступа к зашифрованным файлам на съемных дисках запросить ключ доступа к зашифрованным файлам для каждого съемного диска.

- С компьютера пользователя удалены компоненты шифрования. В этом случае пользователь может открыть зашифрованные файлы на локальных дисках и съемных дисках, но содержимое файлов отображается как зашифрованное.

  Пользователь может работать с зашифрованными файлами при следующих условиях:

  - Файлы помещены в зашифрованные архивы (см. раздел "Создание зашифрованных архивов" на стр. 321), созданные на компьютере с установленной программой Kaspersky Endpoint Security.
  - Файлы хранятся на съемных дисках, для которых разрешена работа в портативном режиме (см. раздел "Включение портативного режима для работы с зашифрованными файлами на съемных дисках" на стр. 331).

В этом разделе

Получение доступа к зашифрованным файлам при отсутствии связи с Kaspersky Security Center

Эта инструкция адресована пользователям клиентских компьютеров с установленной программой Kaspersky Endpoint Security.

Чтобы получить доступ к зашифрованным файлам при отсутствии связи с Kaspersky Security Center, выполните следующие действия:

1. Обратитесь к зашифрованному файлу, доступ к которому вы хотите получить.

   Если связь с Kaspersky Security Center в момент обращения к зашифрованному файлу отсутствует, Kaspersky Endpoint Security формирует файл запроса доступа ко всем зашифрованным файлам, хранящимся на локальных дисках компьютера, если вы обратились к файлу, хранящемуся на локальном диске компьютера. Kaspersky Endpoint Security формирует файл запроса доступа ко всем зашифрованным файлам, хранящимся на съемном диске, если вы обратились к файлу, хранящемуся на съемном диске. Откроется окно **Доступ к файлу запрещен**.

2. Отправьте файл запроса доступа к зашифрованным файлам администратору локальной сети организации. Для этого выполните одно из следующих действий:

   - Нажмите на кнопку **Отправить по почте**, чтобы отправить администратору локальной сети организации созданный файл запроса доступа к зашифрованным файлам по электронной почте.

   - Нажмите на кнопку **Сохранить**, чтобы сохранить файл запроса доступа к зашифрованным файлам и передать его администратору локальной сети организации каким-либо другим способом.

3. Получите файл ключа доступа к зашифрованным файлам, созданный и переданный (см. раздел "Предоставление пользователю доступа к зашифрованным файлам при отсутствии связи с Kaspersky Security Center" на стр. 374) вам администратором локальной сети организации.

4. Активируйте ключ доступа к зашифрованным файлам одним из следующих способов:

   - В любом файловом менеджере выделите файл ключа доступа к зашифрованным файлам и откройте его двойным щелчком мыши.

   - Выполните следующие действия:

     a. Откройте главное окно Kaspersky Endpoint Security.

     b. Нажмите на кнопку  .

Откроется окно **События**.

c. Выберите закладку **Статус доступа к файлам и устройствам**.

На закладке отображается список всех запросов доступа к зашифрованным файлам.

d. Выберите запрос, по которому вы получили файл ключа доступа к зашифрованным файлам.

e. Нажмите на кнопку **Обзор**, чтобы загрузить полученный файл ключа доступа к зашифрованным файлам.

Откроется стандартное окно Microsoft Windows **Выбор файла ключа доступа**.

f. В стандартном окне Microsoft Windows **Выбор файла ключа доступа** выберите полученный от администратора локальной сети организации файл с расширением kesdr и именем, совпадающим с именем соответствующего файла запроса доступа.

g. Нажмите на кнопку **Открыть**.

h. В окне **События** нажмите на кнопку **OK**.

В результате Kaspersky Endpoint Security предоставит доступ ко всем зашифрованным файлам, хранящимся на локальных дисках компьютера, если файл запроса доступа к зашифрованным файлам был сформирован при обращении к файлу, хранящемуся на локальном диске компьютера. Kaspersky Endpoint Security предоставит доступ ко всем зашифрованным файлам, хранящимся на съемном диске, если файл запроса доступа к зашифрованным файлам был сформирован при обращении к файлу, хранящемуся на съемном диске. Для получения доступа к зашифрованным файлам, хранящимся на других съемных дисках, требуется получить отдельные ключи доступа для этих съемных дисков.

Предоставление пользователю доступа к зашифрованным файлам при отсутствии связи с Kaspersky Security Center

Чтобы предоставить пользователю доступ к зашифрованным файлам при отсутствии связи с 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, к которой принадлежит компьютер пользователя, запросившего доступ к зашифрованным файлам.

3. В рабочей области выберите закладку **Устройства**.

4. На закладке **Устройства** выделите компьютер пользователя, запросившего доступ к зашифрованным файлам, и по правой клавише мыши откройте контекстное меню.

5. В контекстном меню выберите пункт **Предоставление доступа к устройствам и данным в офлайн-режиме**.

   Откроется окно **Предоставление доступа к устройствам и данным в офлайн-режиме**.

6. В окне **Предоставление доступа к устройствам и данным в офлайн-режиме** выберите закладку **Шифрование**.

7. На закладке **Шифрование** нажмите на кнопку **Обзор**.

   Откроется стандартное окно Microsoft Windows **Выбор файла запроса**.

8. В окне **Выбор файла запроса** укажите путь к файлу запроса, полученного от пользователя, и нажмите на кнопку **Открыть**.

   Kaspersky Security Center сформирует файл ключа доступа к зашифрованным файлам. На закладке **Шифрование** отобразится информация о запросе пользователя.

9. Выполните одно из следующих действий:

- Нажмите на кнопку **Отправить по почте**, чтобы отправить пользователю созданный файл ключа доступа к зашифрованным файлам по электронной почте.

- Нажмите на кнопку **Сохранить**, чтобы сохранить файл ключа доступа к зашифрованным файлам и передать его пользователю каким-либо другим способом.

Изменение шаблонов сообщений для получения доступа к зашифрованным файлам

Чтобы изменить шаблоны сообщений для получения доступа к зашифрованным файлам, 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 изменить шаблоны сообщений для получения доступа к зашифрованным файлам.

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 **Шифрование данных** выберите подраздел **Общие параметры шифрования**.

7. В блоке **Шаблоны** нажмите на кнопку **Шаблоны**.

   Откроется окно **Шаблоны**.

8. Выполните следующие действия:

- Если вы хотите изменить шаблон сообщения пользователя, выберите закладку **Сообщение пользователя**. Когда пользователь обращается к зашифрованному файлу при отсутствии на компьютере ключа доступа к зашифрованным файлам, открывается окно **Доступ к файлу запрещен**. При нажатии на кнопку **Отправить по почте** окна **Доступ к файлу запрещен** автоматически формируется сообщение пользователя. Это сообщение отправляется администратору локальной сети организации вместе с файлом запроса доступа к зашифрованным файлам.

- Если вы хотите изменить шаблон сообщения администратора, выберите закладку **Сообщение администратора**. Это сообщение автоматически формируется при нажатии на кнопку **Отправить по почте** окна **Предоставление доступа к зашифрованным файлами** и приходит к пользователю после предоставления ему доступа к зашифрованным файлам.

9. Измените шаблоны сообщений.

   Вы можете использовать кнопку **По умолчанию** и раскрывающийся список **Переменная**.

10. Нажмите на кнопку **OK**.

11. В окне **Свойства: <Название политики>** нажмите на кнопку **OK**, чтобы сохранить внесенные изменения.

Работа с зашифрованными устройствами при отсутствии доступа к ним

Получение доступа к зашифрованным устройствам

Пользователю может потребоваться запросить доступ к зашифрованным устройствам в следующих случаях:

- Жесткий диск был зашифрован на другом компьютере.

- На компьютере нет ключа шифрования для устройства (например, в момент первого обращения к зашифрованному съемному диску на этом компьютере), и связь с Kaspersky Security Center отсутствует.

  После того как пользователь применил ключ доступа к зашифрованному устройству, Kaspersky Endpoint Security сохраняет ключ шифрования на компьютере пользователя и предоставляет доступ к этому устройству при последующих обращениях, даже если связь с Kaspersky Security Center отсутствует.

Получение доступа к зашифрованным устройствам осуществляется следующим образом:

1. Пользователь создает через интерфейс программы Kaspersky Endpoint Security файл запроса доступа с расширением kesdc и передает его администратору локальной сети организации.

2. Администратор создает в Консоли администрирования Kaspersky Security Center файл ключа доступа (см. раздел "Предоставление пользователю доступа к зашифрованным устройствам" на стр. 381) с расширением kesdr и передает его пользователю.

3. Пользователь применяет ключ доступа.

Восстановление данных на зашифрованных устройствах

Для работы с зашифрованными устройствами пользователь может использовать утилиту восстановления зашифрованных устройств (далее - "утилита восстановления"). Это может потребоваться в следующих случаях:

- процедура получения доступа с помощью ключа доступа прошла неуспешно;

- на компьютере с зашифрованным устройством не установлены компоненты шифрования.

Данные, необходимые для восстановления доступа к зашифрованным устройствам с помощью утилиты восстановления, в течение некоторого времени находятся в памяти компьютера пользователя в открытом виде. Чтобы снизить вероятность несанкционированного доступа к этим данным, рекомендуется выполнять восстановление доступа к зашифрованным устройствам на доверенных компьютерах.

Восстановление данных на зашифрованных устройствах осуществляется следующим способом:

1. Пользователь создает с помощью утилиты восстановления файл запроса доступа с расширением fdertc и передает его администратору локальной сети организации.

2. Администратор создает в Консоли администрирования Kaspersky Security Center файл ключа доступа (см. раздел "Ответ на запрос пользователя о восстановлении данных на зашифрованных устройствах" на стр. 388) с расширением fdertr и передает его пользователю.

3. Пользователь применяет ключ доступа.

Для восстановления данных на зашифрованных системных жестких дисках пользователь также может указать в утилите восстановления учетные данные Агента аутентификации. Если метаданные учетной записи Агента аутентификации повреждены, то пользователю потребуется пройти процедуру восстановления с помощью файла запроса доступа.

Перед восстановлением данных на зашифрованных устройствах рекомендуется вывести компьютер, на котором будет выполняться процедура, из-под действия политики шифрования Kaspersky Security Center. Это позволяет предотвратить повторное шифрование устройства.

В этом разделе

Получение доступа к зашифрованным устройствам через интерфейс программы

Эта инструкция адресована пользователям клиентских компьютеров с установленной программой Kaspersky Endpoint Security.

Чтобы получить доступ к зашифрованным устройствам через интерфейс программы, выполните следующие действия:

1. Обратитесь к зашифрованному устройству, доступ к которому вы хотите получить.

   Откроется окно **Доступ к данным запрещен**.

2. Отправьте файл запроса доступа к зашифрованному устройству с расширением kesdc администратору локальной сети организации. Для этого выполните одно из следующих действий:

   - Нажмите на кнопку **Отправить по почте**, чтобы отправить администратору локальной сети организации созданный файл запроса доступа к зашифрованному устройству по электронной почте.

   - Нажмите на кнопку **Сохранить**, чтобы сохранить файл запроса доступа к зашифрованному устройству и передать его администратору локальной сети организации каким-либо другим способом.

   > Если вы закрыли окно **Доступ к данным запрещен**, не сохранив или не отправив администратору локальной сети организации файл запроса доступа, вы можете сделать это в любой момент в окне **События** на закладке **Статус доступа к файлам и устройствам**. Чтобы открыть это окно, нажмите на кнопку  в главном окне программы.

3. Получите и сохраните файл ключа доступа к зашифрованному устройству, созданный и переданный (см. раздел "Предоставление пользователю доступа к зашифрованным устройствам" на стр. 381) вам администратором локальной сети организации.

4. Примените ключ доступа к зашифрованному устройству одним из следующих способов:

   - В любом файловом менеджере найдите файл ключа доступа к зашифрованному устройству и откройте его двойным щелчком мыши.

   - Выполните следующие действия:

     a. Откройте главное окно Kaspersky Endpoint Security.

     b. По кнопке  откройте окно **События**.

     c. Выберите закладку **Статус доступа к файлам и устройствам**.

     На закладке отображается список всех запросов доступа к зашифрованным файлам и устройствам.

d. Выберите запрос, по которому вы получили файл ключа доступа к зашифрованному устройству.

e. Нажмите на кнопку **Обзор**, чтобы загрузить полученный файл ключа доступа к зашифрованному устройству.

Откроется стандартное окно Microsoft Windows **Выбор файла ключа доступа**.

f. В стандартном окне Microsoft Windows **Выбор файла ключа доступа** выберите полученный от администратора локальной сети организации файл с расширением kesdr и названием, совпадающим с названием соответствующего файла запроса доступа к зашифрованному устройству.

g. Нажмите на кнопку **Открыть**.

h. В окне **Статус доступа к файлам и устройствам** нажмите на кнопку **OK**.

В результате Kaspersky Endpoint Security предоставит доступ к зашифрованному устройству.

Предоставление пользователю доступа к зашифрованным устройствам

Чтобы предоставить пользователю доступ к зашифрованному устройству, 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 доступ к зашифрованному устройству.

3. В рабочей области выберите закладку **Устройства**.

4. На закладке **Устройства** выделите компьютер пользователя, запросившего доступ к зашифрованному устройству, и по правой клавише мыши откройте контекстное меню.

5. В контекстном меню выберите пункт **Предоставление доступа к устройствам и данным в офлайн-режиме**.

Откроется окно **Предоставление доступа к устройствам и данным в офлайн-режиме**.

6. В окне **Предоставление доступа к устройствам и данным в офлайн-режиме** выберите закладку **Шифрование**.

7. На закладке **Шифрование** нажмите на кнопку **Обзор**.

   Откроется стандартное окно Microsoft Windows **Выбор файла запроса**.

8. В окне **Выбор файла запроса** укажите путь к файлу запроса, полученного от пользователя, с расширением kesdc.

9. Нажмите на кнопку **Открыть**.

   Kaspersky Security Center сформирует файл ключа доступа к зашифрованному устройству с расширением kesdr. На закладке **Шифрование** отобразится информация о запросе пользователя.

10. Выполните одно из следующих действий:

    - Нажмите на кнопку **Отправить по почте**, чтобы отправить пользователю созданный файл ключа доступа к зашифрованному устройству по электронной почте.

    - Нажмите на кнопку **Сохранить**, чтобы сохранить файл ключа доступа к зашифрованному устройству и передать его пользователю каким-либо другим способом.

Передача пользователю ключа восстановления для жестких дисков, зашифрованных с помощью BitLocker

Чтобы передать пользователю ключ восстановления для системного жесткого диска, зашифрованного с помощью BitLocker, 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 доступ к зашифрованному диску.

3. В рабочей области выберите закладку **Устройства**.

4. На закладке **Устройства** выберите компьютер пользователя, запросившего доступ к зашифрованному диску.

5. По правой клавише мыши откройте контекстное меню и выберите пункт **Предоставление доступа к устройствам и данным в офлайн-режиме**.

   Откроется окно **Предоставление доступа к устройствам и данным в офлайн-режиме**.

6. В окне **Предоставление доступа к устройствам и данным в офлайн-режиме** выберите закладку **Доступ к системному диску с защитой BitLocker**.

7. Запросите у пользователя идентификатор ключа восстановления, указанный в окне ввода пароля BitLocker, и сравните его с идентификатором в поле **Идентификатор ключа восстановления**.

   > Если идентификаторы не совпадают, то этот ключ не подходит для восстановления доступа к указанному системному диску. Убедитесь, что имя выбранного компьютера совпадает с именем компьютера пользователя.

8. Передайте пользователю ключ, указанный в поле **Ключ восстановления**.

Чтобы передать пользователю ключ восстановления для несистемного жесткого диска, зашифрованного с помощью BitLocker, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.

2. В дереве Консоли администрирования выберите папку **Дополнительно** → **Шифрование и защита данных** → **Зашифрованные устройства**.

   В рабочей области отобразится список зашифрованных устройств.

3. В рабочей области выберите зашифрованное устройство, доступ к которому требуется восстановить.

4. По правой клавише мыши откройте контекстное меню и выберите пункт **Получить ключ доступа к указанному зашифрованному устройству**.

   Откроется окно **Восстановление доступа к диску, зашифрованному с помощью BitLocker**.

5. Запросите у пользователя идентификатор ключа восстановления, указанный в окне ввода пароля BitLocker, и сравните его с идентификатором в поле **Идентификатор ключа восстановления**.

   > Если идентификаторы не совпадают, то этот ключ не подходит для восстановления доступа к указанному диску. Убедитесь, что имя выбранного компьютера совпадает с именем компьютера пользователя.

6. Передайте пользователю ключ, указанный в поле **Ключ восстановления**.

Создание исполняемого файла утилиты восстановления

> Эта инструкция адресована пользователям клиентских компьютеров с установленной программой Kaspersky Endpoint Security.

Чтобы создать исполняемый файл утилиты восстановления, выполните следующие действия:

1. Откройте главное окно программы (на стр. 64).

2. По кнопке  , расположенной в левом нижнем углу главного окна программы, откройте окно **Поддержка**.

3. В окне **Поддержка** нажмите на кнопку **Восстановление зашифрованного устройства**.

   Запустится утилита восстановления зашифрованных устройств.

4. В окне утилиты восстановления нажмите на кнопку **Создать автономную утилиту восстановления**.

   Откроется окно **Создание автономной утилиты восстановления**.

5. В поле **Сохранить в** введите вручную путь к папке для сохранения исполняемого файла утилиты восстановления или воспользуйтесь кнопкой **Обзор**.

6. В окне **Создание автономной утилиты восстановления** нажмите на кнопку **OK**.

   Исполняемый файл утилиты восстановления fdert.exe будет сохранен в указанной папке.

Восстановление данных на зашифрованных устройствах с помощью утилиты восстановления

Эта инструкция адресована пользователям клиентских компьютеров с установленной программой Kaspersky Endpoint Security.

Чтобы восстановить доступ к зашифрованному устройству с помощью утилиты восстановления, выполните следующие действия:

1. Запустите утилиту восстановления одним из следующих способов:

   - По кнопке  в главном окне программы Kaspersky Endpoint Security откройте окно **Поддержка** и нажмите на кнопку **Восстановление зашифрованного устройства**.

   - Запустите исполняемый файл утилиты восстановления fdert.exe, созданный с помощью программы Kaspersky Endpoint Security (см. раздел "Создание исполняемого файла утилиты восстановления" на стр. 384).

2. В окне утилиты восстановления в раскрывающемся списке **Выберите устройство** выберите зашифрованное устройство, доступ к которому вы хотите восстановить.

3. Нажмите на кнопку **Диагностировать**, чтобы утилита могла определить, какое действие следует выполнить с зашифрованным устройством: разблокировать или расшифровать.

   Если на компьютере доступна функциональность шифрования Kaspersky Endpoint Security, то утилита восстановления предлагает разблокировать устройство. При разблокировке устройство не расшифровывается, но к нему в результате предоставляется прямой доступ. Если на компьютере недоступна функциональность шифрования Kaspersky Endpoint Security, то утилита восстановления предлагает расшифровать устройство.

4. Нажмите на кнопку **Исправить MBR**, если в результате диагностики зашифрованного системного жесткого диска вы получили сообщение о каких-либо проблемах, связанных с главной загрузочной записью (MBR) устройства.

   Исправление главной загрузочной записи устройства может ускорить получение информации, необходимой для разблокировки или расшифровки устройства.

5. Нажмите на кнопку **Разблокировать** или **Расшифровать** в зависимости от результатов диагностики.

   Откроется окно **Параметры разблокировки устройства** или **Параметры расшифровки устройства**.

6. Если вы хотите восстановить данные с помощью учетной записи Агента аутентификации, выполните следующие действия:

   a. Выберите вариант **Использовать параметры учетной записи Агента аутентификации**.

   b. В полях **Имя** и **Пароль** укажите учетные данные Агента аутентификации.

   Этот способ возможен только при восстановлении данных на системном жестком диске. Если системный жесткий диск был поврежден и данные об учетной записи Агента аутентификации потеряны, то для восстановления данных на зашифрованном устройстве необходимо получить ключ доступа у администратора локальной сети организации.

7. Если вы хотите восстановить данные с помощью ключа доступа, выполните следующие действия:

    a. Выберите вариант **Указать ключ доступа к устройству вручную**.

    b. Нажмите на кнопку **Получить ключ доступа**.

    c. Откроется окно **Получение ключа доступа к устройству**.

    d. Нажмите на кнопку **Сохранить** и выберите папку, чтобы сохранить файл запроса доступа с расширением fdertc.

    e. Передайте файл запроса доступа администратору локальной сети организации.

    > Не закрывайте окно **Получение ключа доступа к устройству**, пока вы не получите ключ доступа. При повторном открытии этого окна созданный администратором ранее ключ доступа будет невозможно применить.

    f. Получите и сохраните файл ключа доступа, созданный и переданный (см. раздел "Ответ на запрос пользователя о восстановлении данных на зашифрованных устройствах" на стр. 388) вам администратором локальной сети организации.

    g. Нажмите на кнопку **Загрузить** и в открывшемся окне выберите файл ключа доступа с расширением fdertr.

8. Если вы выполняете расшифровку устройства, то в окне **Параметры расшифровки устройства** вам также требуется указать остальные параметры расшифровки. Для этого выполните следующие действия:

    - Укажите область для расшифровки:

        - Если вы хотите расшифровать все устройство, выберите вариант **Расшифровать все устройство**.
        - Если вы хотите расшифровать часть данных на устройстве, выберите вариант **Расшифровать отдельные области устройства** и задайте границы области для расшифровки с помощью полей **Начало** и **Конец**.

    - Выберите место записи расшифрованных данных:

- Если вы хотите, чтобы данные на исходном устройстве были перезаписаны расшифрованными данными, снимите флажок **Сохранять в файл данные после расшифровки**.
- Если вы хотите сохранить расшифрованные данные отдельно от исходных зашифрованных данных, установите флажок **Сохранять в файл данные после расшифровки** и с помощью кнопки **Обзор** укажите путь, по которому данные должны быть сохранены.

9. Нажмите на кнопку **OK**.

Запустится процесс разблокировки / расшифровки устройства.

Ответ на запрос пользователя о восстановлении данных на зашифрованных устройствах

Чтобы создать и передать пользователю файл ключа доступа к зашифрованному устройству, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В дереве Консоли администрирования выберите папку **Дополнительно** → **Шифрование и защита данных** → **Зашифрованные устройства**.
3. В рабочей области выберите зашифрованное устройство, для которого вы хотите создать файл ключа доступа, и в контекстном меню устройства выберите пункт **Получить ключ доступа к указанному зашифрованному устройству**.

   Если вы не уверены, для какого компьютера был сформирован файл запроса доступа, в дереве Консоли администрирования выберите папку **Дополнительно** → **Шифрование и защита данных** и в рабочей области нажмите на ссылку **Получить ключ шифрования устройства**.

   Откроется окно **Предоставление доступа к устройству**.
4. Выберите используемый алгоритм шифрования. Для этого выберите один из следующих вариантов:

- **AES256**, если на компьютере, на котором было зашифровано устройство, программа Kaspersky Endpoint Security установлена из дистрибутива, расположенного в папке aes256;

- **AES56**, если на компьютере, на котором было зашифровано устройство, программа Kaspersky Endpoint Security установлена из дистрибутива, расположенного в папке aes56.

5. Нажмите на кнопку **Обзор**.

   Откроется стандартное окно Microsoft Windows **Выбор файла запроса**.

6. В окне **Выбор файла запроса** укажите путь к файлу запроса, полученного от пользователя, с расширением fdertc.

7. Нажмите на кнопку **Открыть**.

   Kaspersky Security Center сформирует файл ключа доступа к зашифрованному устройству с расширением fdertr.

8. Выполните одно из следующих действий:

   - Нажмите на кнопку **Отправить по почте**, чтобы отправить пользователю созданный файл ключа доступа к зашифрованному устройству по электронной почте.

   - Нажмите на кнопку **Сохранить**, чтобы сохранить файл ключа доступа к зашифрованному устройству и передать его пользователю каким-либо другим способом.

Восстановление доступа к зашифрованным данным в случае выхода из строя операционной системы

Чтобы восстановить доступ к зашифрованным файлам и съемным дискам в случае выхода из строя операционной системы, выполните следующие действия:

1. Переустановите операционную систему, не форматируя жесткий диск.

2. Установите Kaspersky Endpoint Security (см. раздел "Установка и удаление программы" на стр. 26).

3. Установите связь между компьютером и Сервером администрирования Kaspersky Security Center, под управлением которого находился компьютер во время шифрования данных (см. *Руководство администратора Kaspersky Security Center*).

Доступ к зашифрованным данным будет предоставлен на тех же условиях, что были до выхода операционной системы из строя.

Создание диска аварийного восстановления операционной системы

Диск аварийного восстановления операционной системы может быть полезен в ситуации, когда по каким-либо причинам доступ к зашифрованному системному жесткому диску невозможен и операционная система не может быть загружена.

Вы можете загрузить образ операционной системы Windows с помощью диска аварийного восстановления и восстановить доступ к зашифрованному системному диску с помощью утилиты восстановления, включенной в состав образа операционной системы.

Чтобы создать диск аварийного восстановления операционной системы, выполните следующие действия:

1. Создайте исполняемый файл утилиты восстановления зашифрованных устройств (см. раздел "Создание исполняемого файла утилиты восстановления" на стр. 384).

2. Создайте пользовательский образ среды предустановки Windows. В процессе создания пользовательского образа среды предустановки Windows добавьте в образ исполняемый файл утилиты восстановления зашифрованных устройств.

3. Поместите пользовательский образ среды предустановки Windows на загрузочный носитель, например компакт-диск или съемный диск.

   Инструкцию о создании пользовательского образа среды предустановки Windows вы можете прочитать в справочной документации Microsoft (например, на ресурсе Microsoft TechNet).

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 Почтовый Антивирус (см. раздел "Защита почты. Почтовый Антивирус" на стр. 104) и Веб-Антивирус (см. раздел "Защита компьютера в интернете. Веб-Антивирус" на стр. 119) контролируют потоки данных, передаваемые по определенным протоколам и проходящие через определенные открытые TCP- и UDP-порты компьютера пользователя. Так, например, Почтовый Антивирус анализирует информацию, передаваемую по SMTP-протоколу, а Веб-Антивирус 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 Почтовый Антивирус и Веб-Антивирус 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. 66).

2. В левой части окна выберите раздел **Антивирусная защита**.

   В правой части окна отобразятся параметры антивирусной защиты.

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. 66).

2. В левой части окна выберите раздел **Антивирусная защита**.

   В правой части окна отобразятся параметры антивирусной защиты.

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. 395), 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. 66).

2. В левой части окна выберите раздел **Антивирусная защита**.

   В правой части окна отобразятся параметры антивирусной защиты.

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 **ОК**.

      Окно **Программа** закроется. Добавленная вами программа отобразится в конце списка программ.

8. Нажмите на кнопку **ОК** в окне **Сетевые порты**.

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

Обновление баз и модулей программы

Этот раздел содержит информацию об обновлении баз и модулей программы (далее также "обновления") и инструкции о том, как настроить параметры обновления.

В этом разделе

Об обновлении баз и модулей программы

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

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

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

Для успешной загрузки пакета обновлений с серверов обновлений "Лаборатории Касперского" компьютер должен быть подключен к интернету. По умолчанию параметры подключения к интернету определяются автоматически. Если вы используете прокси-сервер, требуется настроить параметры прокси-сервера (см. раздел "Настройка параметров прокси-сервера" на стр. 411).

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

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

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

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

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

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

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

Информация о текущем состоянии баз Kaspersky Endpoint Security отображается в разделе **Обновление** блока **Управление задачами** на закладке **Центр управления** главного окна программы (см. раздел "Главное окно программы" на стр. 64).

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. 456).

Об источниках обновлений

Источник обновлений - это ресурс, содержащий обновления баз и модулей 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.

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

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. 66).

2. В левой части окна в разделе **Задачи по расписанию** выберите подраздел **Обновление**.

   В правой части окна отобразятся параметры обновления баз и модулей 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 **OK**.

7. В окне **Обновление** нажмите на кнопку **OK**.

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

См. также

Об источниках обновлений.....399

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. 66).

2. В левой части окна в разделе **Задачи по расписанию** выберите подраздел **Обновление**.

   В правой части окна отобразятся параметры обновления баз и модулей 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.

См. также

Об источниках обновлений.....399

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. 66).

2. В левой части окна в разделе **Задачи по расписанию** выберите подраздел **Обновление**.

   В правой части окна отобразятся параметры обновления баз и модулей 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 **OK**.

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. 66).

2. В левой части окна в разделе **Задачи по расписанию** выберите подраздел **Обновление**.

   В правой части окна отобразятся параметры обновления баз и модулей 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.

См. также

Об источниках обновлений.....399

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. 66).

2. В левой части окна в разделе **Задачи по расписанию** выберите подраздел **Обновление**.

   В правой части окна отобразятся параметры обновления баз и модулей 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.

См. также

Запуск и остановка задачи обновления 409

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 нет прав авторизованного пользователя прокси-сервера. 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. 66).

2. В левой части окна в разделе **Задачи по расписанию** выберите подраздел **Обновление**.

   В правой части окна отобразятся параметры обновления баз и модулей 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 **ОК**.

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

Настройка обновления модулей программы

Чтобы настроить обновление модулей программы, выполните следующие действия:

1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 66).

2. В левой части окна в разделе **Задачи по расписанию** выберите подраздел **Обновление**.

   В правой части окна отобразятся параметры обновления баз и модулей программы.

3. В блоке **Дополнительно** выполните одно из следующих действий:

   - Установите флажок **Загружать обновления модулей программы**, если вы хотите, чтобы программа включала обновления модулей программы в пакеты обновлений.

   - В противном случае снимите флажок **Загружать обновления модулей программы**.

4. Если на предыдущем шаге установлен флажок **Загружать обновления модулей программы**, укажите, при каких условиях программа будет устанавливать обновления модулей программы:

   - Выберите вариант **Устанавливать критические и одобренные обновления**, если вы хотите, чтобы программа устанавливала критические обновления модулей программы автоматически, а остальные обновления модулей программы

– после одобрения их установки, локально через интерфейс программы или с помощью Kaspersky Security Center.

- Выберите вариант **Устанавливать только одобренные обновления**, если вы хотите, чтобы программа устанавливала обновления модулей программы только после одобрения их установки, локально через интерфейс программы или с помощью Kaspersky Security Center.

5. 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.
2. Выберите закладку **Центр управления**.
3. Нажмите клавишей мыши на блок **Управление задачами**.

   Блок **Управление задачами** раскроется.
4. По правой клавише мыши откройте контекстное меню строки с названием задачи обновления.

   Откроется меню действий с задачей обновления.
5. Выполните одно из следующих действий:

   - Выберите в меню пункт **Запустить обновление**, если вы хотите запустить задачу обновления.

Статус выполнения задачи обновления, отображающийся справа от кнопки **Обновление**, изменится на *Выполняется*.

- Выберите в меню пункт **Остановить обновление**, если вы хотите остановить задачу обновления.

  Статус выполнения задачи обновления, отображающийся справа от кнопки **Обновление**, изменится на *Остановлено*.

Откат последнего обновления

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

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

Чтобы откатить последнее обновление, выполните следующие действия:

1. Откройте главное окно программы.
2. Выберите закладку **Центр управления**.
3. Нажмите клавишей мыши на блок **Управление задачами**.

   Блок **Управление задачами** раскроется.
4. Правой клавишей мыши вызовите контекстное меню задачи **Обновление**.
5. Выберите пункт **Откатить обновление**.

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. 66).
2. В левой части окна в разделе **Задачи по расписанию** выберите подраздел **Обновление**.

   В правой части окна отобразятся параметры обновления баз и модулей программы.
3. В блоке **Прокси-сервер** нажмите на кнопку **Настройка**.

   Откроется окно **Параметры прокси-сервера**.
4. В окне **Параметры прокси-сервера** установите флажок **Использовать прокси-сервер**.
5. Задайте параметры прокси-сервера.
6. Нажмите на кнопку **OK**.
7. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Вы также можете настроить параметры прокси-сервера в блоке **Дополнительные параметры** на закладке **Настройка** главного окна программы.

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. 414) процесс выполнения проверки отображается в поле напротив названия запущенной задачи проверки в блоке **Управление задачами** на закладке **Центр управления** главного окна Kaspersky Endpoint Security.

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. 64).
2. Выберите закладку **Центр управления**.
3. Нажмите клавишей мыши на блок **Управление задачами**.

   Блок **Управление задачами** раскроется.
4. По правой клавише мыши откройте контекстное меню строки с названием задачи проверки.

   Откроется меню действий с задачей проверки.
5. Выполните одно из следующих действий:

   - Выберите в меню пункт **Запустить проверку**, если вы хотите запустить задачу проверки.

     Статус выполнения задачи, отображающийся справа от кнопки с названием задачи проверки, изменится на *Выполняется*.
   - Выберите в меню пункт **Остановить проверку**, если вы хотите остановить задачу проверки.

     Статус выполнения задачи, отображающийся справа от кнопки с названием задачи проверки, изменится на *Остановлено*.

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. 66).

2. В левой части окна в разделе **Задачи по расписанию** 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

Чтобы изменить действие над зараженными файлами, выполните следующие действия:

1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 66).

2. В левой части окна в разделе **Задачи по расписанию** 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 **Действие при обнаружении угрозы** выберите нужный вариант:

- **Выбирать действие автоматически**.
- **Выполнять действие**.

4. Если на предыдущем шаге вы выбрали вариант **Выполнять действие**, установите следующие флажки:
   - Установите флажок **Лечить**, если вы хотите, чтобы Kaspersky Endpoint Security лечил объекты, в которых были обнаружены угрозы.

     > Даже если выбран этот вариант, в отношении файлов, являющихся частью приложения Windows Store, Kaspersky Endpoint Security выполняет действие **Удалить**.

   - Установите флажок **Удалять**, если вы хотите, чтобы Kaspersky Endpoint Security удалял объекты, в которых обнаружены угрозы.
   - Установите оба флажка **Лечить** и **Удалять**, если вы хотите, чтобы Kaspersky Endpoint Security пытался вылечить объекты, в которых обнаружены угрозы, и удалял те объекты, которые невозможно вылечить.
   - Снимите оба флажка **Лечить** и **Удалять**, если вы хотите, чтобы Kaspersky Endpoint Security не производил никаких действий над объектами, в которых обнаружена угроза, но информировал пользователя о результатах проверки этих объектов.
5. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Формирование списка проверяемых объектов

Сформировать список проверяемых объектов можно двумя способами:

- на закладке **Центр управления** главного окна программы (см. раздел "Главное окно программы" на стр. 64);

- из окна настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 66).

> Этот способ доступен только для задач **Полная проверка** и **Проверка важных областей**. Список проверяемых объектов для задачи **Выборочная проверка** можно сформировать только на закладке **Центр управления**.

Чтобы сформировать список проверяемых объектов на закладке Центр управления главного окна программы, выполните следующие действия:

1. Откройте главное окно программы.
2. Выберите закладку **Центр управления**.
3. Нажмите клавишей мыши на блок **Управление задачами**.

   Блок **Управление задачами** раскроется.
4. По правой клавише мыши откройте контекстное меню строки с названием задачи и выберите пункт **Область проверки**.

   Откроется окно **Область проверки**.
5. 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 **OK**.
6. 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**.

7. 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.

8. 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.

9. Нажмите на кнопку **ОК**.

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

Чтобы сформировать список проверяемых объектов из окна настройки параметров программы, выполните следующие действия:

1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 66).

2. В левой части окна в разделе **Задачи по расписанию** выберите подраздел с названием нужной задачи проверки: **Полная проверка** или **Проверка важных областей**.

   В правой части окна отобразятся параметры выбранной задачи проверки.

3. Нажмите на кнопку **Область проверки**.

   Откроется окно **Область проверки**.

4. Сформируйте список проверяемых объектов согласно пунктам 5 - 10 предыдущей инструкции.

Выбор типа проверяемых файлов

Выбрать тип проверяемых файлов можно двумя способами:

- на закладке **Центр управления** главного окна программы (см. раздел "Главное окно программы" на стр. 64);
- из окна настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 66).

> Этот способ доступен только для задач **Полная проверка** и **Проверка важных областей**. Тип проверяемых файлов для задачи **Выборочная проверка** можно выбрать только на закладке **Центр управления**.

Чтобы выбрать тип проверяемых файлов на закладке Центр управления главного окна программы, выполните следующие действия:

1. Откройте главное окно программы.
2. Выберите закладку **Центр управления**.
3. Нажмите клавишей мыши на блок **Управление задачами**.

   Блок **Управление задачами** раскроется.

4. По правой клавише мыши откройте контекстное меню строки с названием задачи и выберите пункт **Настройка**.

   Откроется окно с названием выбранной задачи проверки.

5. В окне с названием выбранной задачи проверки выберите закладку **Область действия**.

6. 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 или могут содержать исполняемый код (например, форматы EXE, DLL, 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 Файловый Антивирус анализирует заголовок файла. Если в результате выясняется, что файл имеет формат EXE, то программа проверяет его.

7. В окне с названием задачи проверки нажмите на кнопку **OK**.

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

Чтобы выбрать тип проверяемых файлов из окна настройки параметров программы, выполните следующие действия:

1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 66).

2. В левой части окна в разделе **Задачи по расписанию** выберите подраздел с названием нужной задачи проверки: **Полная проверка** или **Проверка важных областей**.

   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. Выполните пункты 5 - 7 предыдущей инструкции.

Оптимизация проверки файлов

Чтобы оптимизировать проверку файлов, выполните следующие действия:

1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 66).

2. В левой части окна в разделе **Задачи по расписанию** 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 **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. 66).
2. В левой части окна в разделе **Задачи по расписанию** 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 **OK**.
10. В окне с названием задачи проверки нажмите на кнопку **OK**.
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. 66).

2. В левой части окна в разделе **Задачи по расписанию** 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 **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 **ОК**.

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. 66).

2. В левой части окна в разделе **Задачи по расписанию** 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 **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. 66).

2. В левой части окна в разделе **Задачи по расписанию** 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. 66).

2. В левой части окна в разделе **Задачи по расписанию** 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 **OK**.

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. 66).

2. В левой части окна выберите раздел **Задачи**.

   В правой части окна отобразятся параметры задач.

3. В блоке **Проверка съемных дисков при подключении** 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 окно выполнения проверки**.
   - Если вы хотите, чтобы Kaspersky Endpoint Security запускал проверку съемных дисков в фоновом режиме, снимите флажок **Отображать окно выполнения проверки**.

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

Работа с необработанными файлами

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

О необработанных файлах

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

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.

Зараженный файл считается *необработанным*, если Kaspersky Endpoint Security в процессе проверки компьютера на вирусы и другие программы, представляющие угрозу, 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 необработанных файлов после обновления баз и модулей 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 необработанных файлов*" на стр. 435);
- восстановить те зараженные файлы, в которых содержится важная информация, а также восстановить файлы со статусом *Вылечен* и *Не заражен.*

Работа со списком необработанных файлов

Список необработанных файлов представлен в виде таблицы.

Вы можете выполнять следующие действия с необработанными файлами:

- просматривать список необработанных файлов;
- проверять необработанные файлы, используя текущую версию баз и модулей Kaspersky Endpoint Security;
- восстанавливать файлы из списка необработанных файлов в исходные папки или в другую выбранную вами папку (в случае, если исходная папка размещения файла недоступна для записи);
- удалять файлы из списка необработанных файлов;
- открыть папку исходного размещения необработанного файла.

Кроме того, вы можете выполнять следующие действия, работая с табличными данными:

- фильтровать события о необработанных файлах по значениям граф или по условиям сложного фильтра;
- использовать функцию поиска событий о необработанных файлах;
- сортировать события о необработанных файлах;

- изменять порядок и набор граф, отображаемых в списке необработанных файлов;
- группировать события о необработанных файлах.

Если требуется, вы можете скопировать выбранные события о необработанных файлах в буфер обмена.

В этом разделе

Запуск задачи выборочной проверки необработанных файлов

Вы можете вручную запустить задачу выборочной проверки необработанных файлов. Проверку можно запустить, например, если по какой-либо причине последняя проверка была прервана или если вы хотите повторно проверить необработанные файлы после очередного обновления баз и модулей программы.

Чтобы запустить задачу выборочной проверки необработанных файлов, выполните следующие действия:

1. Откройте главное окно программы (на стр. 64).
2. По ссылке **Хранилище**, расположенной в верхней части главного окна программы, откройте окно **Хранилище**.
3. В окне **Хранилище** выберите закладку **Необработанные файлы**.
4. В таблице на закладке **Необработанные файлы** выберите одно или несколько событий, относящихся к файлам, которые вы хотите проверить.

   Чтобы выбрать несколько событий, выделяйте их, удерживая клавишу **CTRL**.
5. 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 необработанных файлов

Чтобы удалить файлы из списка необработанных файлов, выполните следующие действия:

1. Откройте главное окно программы (на стр. 64).
2. По ссылке **Хранилище**, расположенной в верхней части главного окна программы, откройте окно **Хранилище**.
3. В окне **Хранилище** выберите закладку **Необработанные файлы**.
4. В таблице на закладке **Необработанные файлы** выберите одно или несколько событий, относящихся к файлам, которые вы хотите удалить.

   Чтобы выбрать несколько событий, выделяйте их, удерживая клавишу **CTRL**.
5. Удалите файлы одним из следующих способов:
   - Нажмите на кнопку **Удалить**.
   - По правой клавише мыши откройте контекстное меню и выберите пункт **Удалить**.

Поиск уязвимостей

Этот раздел содержит информацию об особенностях и настройке задачи поиска уязвимостей, а также инструкции по работе со списком уязвимостей, которые обнаружила программа Kaspersky Endpoint Security в результате выполнения задачи поиска уязвимостей.

В этом разделе

Просмотр информации об уязвимостях запущенных программ

Информация об уязвимостях запущенных программ доступна, если программа Kaspersky Endpoint Security установлена на компьютере под управлением операционной системы Microsoft Windows для рабочих станций. Эта информация недоступна, если программа Kaspersky Endpoint Security установлена на компьютере под управлением операционной системы Microsoft Windows для файловых серверов (см. раздел "Аппаратные и программные требования" на стр. 24).

Чтобы просмотреть информацию об уязвимостях запущенных программ, выполните следующие действия:

1. Откройте главное окно программы (на стр. 64).

2. Выберите закладку **Центр управления**.

3. Раскройте блок **Контроль рабочего места**.

4. Нажмите на кнопку **Мониторинг активности программ**.

Откроется окно **Контроль активности программ** на закладке **Мониторинг активности программ**. В таблице **Мониторинг активности программ** представлена сводная информация об активности запущенных программ в операционной системе. Степень уязвимости запущенных программ, которую определил компонент Мониторинг уязвимостей, отображается в графе **Степень уязвимости**.

О задаче поиска уязвимостей

Уязвимости в операционной системе могут быть результатом, например, ошибок программирования или проектирования, ненадежных паролей, действий вредоносных программ. В рамках поиска уязвимостей проводится изучение операционной системы, поиск аномалий и повреждений в параметрах программ компании Microsoft и других производителей.

Задача поиска уязвимостей заключается в диагностике безопасности операционной системы и обнаружении в программном обеспечении особенностей, которые могут быть использованы злоумышленниками для распространения вредоносных объектов и для доступа к персональным данным.

После запуска задачи поиска уязвимостей (см. раздел "Запуск и остановка задачи поиска уязвимостей" на стр. 438) процесс ее выполнения отображается в поле напротив названия задачи **Поиск уязвимостей** в блоке **Управление задачами** на закладке **Центр управления** главного окна Kaspersky Endpoint Security.

Информация о результатах выполнения задачи поиска уязвимостей фиксируется в отчетах (см. раздел "Работа с отчетами" на стр. 456).

Запуск и остановка задачи поиска уязвимостей

Независимо от выбранного режима запуска задачи поиска уязвимостей вы можете запустить или остановить задачу поиска уязвимостей.

Чтобы запустить или остановить задачу поиска уязвимостей, выполните следующие действия:

1. Откройте главное окно программы (на стр. 64).
2. Выберите закладку **Центр управления**.
3. Нажмите клавишей мыши на блок **Управление задачами**.

   Блок **Управление задачами** раскроется.
4. По правой клавише мыши откройте контекстное меню строки с названием задачи поиска уязвимостей.

   Откроется меню действий с задачей поиска уязвимостей.
5. Выполните одно из следующих действий:

   - Выберите в меню пункт **Запустить проверку**, если вы хотите запустить задачу поиска уязвимостей.

     Статус выполнения задачи, отображающийся справа от кнопки с названием задачи поиска уязвимостей, изменится на *Выполняется*.

   - Выберите в меню пункт **Остановить проверку**, если вы хотите остановить задачу поиска уязвимостей.

     Статус выполнения задачи, отображающийся справа от кнопки с названием задачи поиска уязвимостей, изменится на *Остановлено*.

Настройка параметров поиска уязвимостей

Для настройки параметров поиска уязвимостей вы можете выполнить следующие действия:

- Сформировать область поиска уязвимостей.

  Вы можете расширить или сузить область поиска, добавив или удалив программы, проверяемые на наличие уязвимостей.

- Выбрать режим запуска для задачи поиска уязвимостей.

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

- Настроить запуск задачи 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 и запускать задачу от имени этого пользователя.

В этом разделе

Формирование области для поиска уязвимостей

Под областью для поиска уязвимостей подразумевается производитель программного обеспечения или местоположение папки, в которую установлено программное обеспечение (например, все программы компании Microsoft или программы, установленные в папку Program Files).

Чтобы сформировать область для поиска уязвимостей, выполните следующие действия:

1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 66).

2. В левой части окна в разделе **Задачи по расписанию** выберите подраздел **Поиск уязвимостей**.

   В правой части окна отобразятся параметры задачи поиска уязвимостей.

3. В блоке **Область проверки** выполните следующие действия:

   a. Установите флажок **Microsoft**, если вы хотите, чтобы Kaspersky Endpoint Security искала уязвимости в установленных на компьютере пользователя программах компании Microsoft.

   b. Установите флажок **Другие производители**, если вы хотите чтобы Kaspersky Endpoint Security искала уязвимости в установленных на компьютере пользователя программах, произведенных не компанией Microsoft.

   c. В блоке **Дополнительная область для поиска уязвимостей** нажмите на кнопку **Настройка**.

      Откроется окно **Область для поиска уязвимостей**.

   d. Сформируйте область для поиска уязвимостей. Для этого используйте кнопки **Добавить** и **Удалить**.

   e. В окне **Область для поиска уязвимостей** нажмите на кнопку **OK**.

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

Выбор режима запуска для задачи поиска уязвимостей

Чтобы выбрать режим запуска для задачи поиска уязвимостей, выполните следующие действия:

1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 66).

2. В левой части окна в разделе **Задачи по расписанию** выберите подраздел **Поиск уязвимостей**.

   В правой части окна отобразятся параметры задачи поиска уязвимостей.

3. Нажмите на кнопку **Режим запуска**.

   Откроется закладка **Режим запуска** окна **Поиск уязвимостей**.

4. В блоке **Режим запуска** выберите один из следующих вариантов режима запуска задачи поиска уязвимостей:

   - Выберите вариант **Вручную**, если вы хотите запускать задачу поиска уязвимостей вручную.

   - Выберите вариант **По расписанию**, если вы хотите настроить расписание запуска задачи поиска уязвимостей.

5. Выполните одно из следующих действий:

   - Если вы выбрали вариант **Вручную**, перейдите к пункту 6 инструкции.

   - Если вы выбрали вариант **По расписанию**, задайте параметры расписания запуска задачи поиска уязвимостей. Для этого выполните следующие действия:

     a. В раскрывающемся списке **Периодичность** укажите, когда следует запускать задачу поиска уязвимостей. Выберите один из следующих вариантов: **Дни**, **Каждую неделю**, **В указанное время**, **Каждый месяц**, **После запуска программы**, **После каждого обновления**.

     b. В зависимости от выбранного в раскрывающемся списке **Периодичность**

элемента задайте значение параметров, которые уточняют время запуска задачи поиска уязвимостей.

c. Установите флажок **Запускать пропущенные задачи**, если вы хотите, чтобы Kaspersky Endpoint Security запускал при первой возможности не запущенную вовремя задачу поиска уязвимостей.

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

6. Нажмите на кнопку **OK**.

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

Запуск задачи поиска уязвимостей с правами другого пользователя

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

Чтобы настроить запуск задачи поиска уязвимостей с правами другого пользователя, выполните следующие действия:

1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 66).

2. В левой части окна в разделе **Задачи по расписанию** выберите подраздел **Поиск уязвимостей**.

   В правой части окна отобразятся параметры задачи поиска уязвимостей.

3. Нажмите на кнопку **Режим запуска**.

   Откроется закладка **Режим запуска** окна **Поиск уязвимостей**.

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 запуска задачи поиска уязвимостей.
6. В поле **Пароль** введите пароль пользователя, права которого требуется использовать для запуска задачи поиска уязвимостей.
7. Нажмите на кнопку **OK**.
8. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Работа со списком уязвимостей

Работая со списком уязвимостей, вы можете выполнить следующие действия:

- просмотреть список уязвимостей;
- запустить повторно задачу поиска уязвимостей после обновления баз и модулей программы;
- просмотреть подробную информацию об уязвимости и рекомендации по ее исправлению в отдельном блоке;
- скрыть выбранные записи в списке уязвимостей;
- фильтровать список уязвимостей по уровню важности уязвимостей;
- фильтровать список уязвимостей по статусам уязвимостей *Исправленные* и *Скрытые*.

Кроме того, вы можете выполнять следующие действия, работая с табличными данными:

- фильтровать список уязвимостей по значениям граф или по условиям сложного фильтра;
- использовать функцию поиска уязвимостей;
- сортировать записи в списке уязвимостей;

- изменять порядок и набор граф, отображаемых в списке уязвимостей;
- группировать записи в списке уязвимостей.

В этом разделе

О списке уязвимостей

Kaspersky Endpoint Security записывает сведения о результатах выполнения задачи поиска уязвимостей (см. раздел "О задаче поиска уязвимостей" на стр. 437) в список уязвимостей.

Если вы просмотрели какие-либо уязвимости и выполнили рекомендуемые действия для их устранения, то Kaspersky Endpoint Security присваивает таким уязвимостям статус *Исправленные*.

Если вам нужно, чтобы в списке уязвимостей не отображались записи о каких-либо уязвимостях, то вы можете их скрыть. Kaspersky Endpoint Security присваивает таким уязвимостям статус *Скрытые.*

Список уязвимостей представлен в виде таблицы. Каждая строка таблицы содержит следующие сведения:

- Значок, который обозначает уровень критичности уязвимости. Существуют следующие уровни критичности уязвимостей:

- Значок  . **Критический**. К этому уровню критичности относятся очень опасные уязвимости, которые должны быть устранены немедленно. Злоумышленники активно используют уязвимости этого уровня для заражения операционной системы компьютера или для доступа к персональным данным пользователя. Специалисты "Лаборатории Касперского" рекомендуют своевременно выполнять все действия для устранения уязвимостей уровня "Критический".

- Значок  . **Важный**. К этому уровню критичности относятся важные уязвимости, которые должны быть устранены в ближайшее время. Злоумышленники могут начать активно использовать уязвимости этого уровня. В данный момент уязвимости уровня "Важный" не используются злоумышленниками активно. Специалисты "Лаборатории Касперского" рекомендуют своевременно выполнять все действия для устранения уязвимостей уровня "Важный".

- Значок  . **Предупреждение**. К этому уровню критичности относятся уязвимости, устранение которых можно отложить. Однако в будущем такие уязвимости могут поставить безопасность компьютера под угрозу.

- Идентификатор уязвимости.
- Название программы, в которой обнаружена уязвимость.
- Краткое описание уязвимости.
- Информация о производителе программного обеспечения согласно электронной цифровой подписи.
- Результат действий по устранению уязвимости.

Повторный запуск задачи поиска уязвимостей

Чтобы обновить информацию о ранее найденных уязвимостях, вы можете повторно запустить задачу поиска уязвимостей. Повторный запуск задачи может потребоваться, если поиск уязвимостей по какой-либо причине был прерван, или если нужно проверить компьютер на наличие уязвимостей после очередного обновления баз и модулей программы (см. раздел "Об обновлении баз и модулей программы" на стр. 397)

Чтобы повторно запустить задачу поиска уязвимостей, выполните следующие действия:

1. Откройте главное окно программы (на стр. 64).
2. По ссылке **Хранилище**, расположенной в верхней части главного окна программы, откройте окно **Хранилище**.
3. В окне **Хранилище** выберите закладку **Уязвимости**.

   Закладка **Уязвимости** содержит список уязвимостей, которые обнаружил Kaspersky Endpoint Security в результате выполнения задачи поиска уязвимостей.
4. В нижнем правом углу окна **Хранилище** нажмите на кнопку **Перепроверить**.

Kaspersky Endpoint Security обновит подробную информацию об уязвимостях в списке уязвимостей.

Статус уязвимости, которая была закрыта установкой предложенного патча, не изменяется после очередной проверки на уязвимости.

Исправление уязвимости

Вы можете исправить уязвимость, установив обновления для операционной системы, изменив конфигурацию программы или установив необходимый патч для программы.

Найденные уязвимости могут относиться не к установленным программам, а к их копиям. Патч устранит уязвимость только в том случае, если программа была установлена.

Чтобы исправить уязвимость, выполните следующие действия:

1. Откройте главное окно программы (на стр. 64).
2. По ссылке **Карантин**, расположенной в верхней части главного окна программы, откройте окно **Хранилища**.
3. В окне **Хранилища** выберите закладку **Уязвимости**.

Закладка **Уязвимости** содержит список уязвимостей, которые обнаружил Kaspersky Endpoint Security в результате выполнения задачи поиска уязвимостей.

4. В списке уязвимостей выберите запись о нужной вам уязвимости.

   В нижней части списка уязвимостей откроется блок со сведениями об этой уязвимости и рекомендациями по ее исправлению.

   Для каждой выбранной уязвимости доступна следующая информация:

   - Название программы, в которой обнаружена уязвимость.
   - Версия программы, в которой обнаружена уязвимость.
   - Уровень критичности уязвимости.
   - Идентификатор уязвимости.
   - Дата и время последнего обнаружения уязвимости.
   - Рекомендации по исправлению уязвимости (например, ссылка на веб-сайт с обновлениями для операционной системы или патч для программы).
   - Ссылка на веб-сайт с описанием уязвимости.

5. Если вы хотите получить подробное описание этой уязвимости, по ссылке **Дополнительная информация** откройте веб-страницу с описанием угрозы, связанной с выбранной уязвимостью. На веб-сайте www.secunia.com (http://www.secunia.com) вы можете загрузить нужное обновление для текущей версии программы и установить его.

6. Выберите один из следующих способов исправления уязвимости:

   - Если есть один или несколько патчей для программы, то для установки нужного патча выполните инструкции, указанные рядом с названием патча.
   - Если есть обновление для операционной системы, то для установки нужного обновления выполните инструкции, указанные рядом с названием обновления.

   После установки патча или обновления уязвимость устраняется. Kaspersky Endpoint Security присваивает уязвимости статус, который обозначает, что уязвимость

исправлена. Запись об исправленной уязвимости отображается в списке уязвимостей серым цветом.

7. Если в блоке в нижней части окна отсутствует информация об устранении уязвимости, то вы можете повторно запустить задачу поиска уязвимостей после обновления баз и модулей Kaspersky Endpoint Security. Поскольку Kaspersky Endpoint Security проверяет наличие уязвимостей по базе данных уязвимостей, то после обновления программы может появиться информация об исправлении этой уязвимости.

Скрытие записей в списке уязвимостей

Вы можете скрыть выбранную запись об уязвимости. Тем записям, которые вы выбрали в списке уязвимостей и отметили как скрытые, Kaspersky Endpoint Security присваивает статус *Скрытые*. После этого вы можете фильтровать список уязвимостей по статусу *Скрытые* (см. раздел "*Фильтрация списка уязвимостей по статусам Исправленные и Скрытые*" на стр. 450).

Чтобы скрыть запись в списке уязвимостей, выполните следующие действия:

1. Откройте главное окно программы (на стр. 64).

2. По ссылке **Карантин**, расположенной в верхней части главного окна программы, откройте окно **Хранилища**.

3. В окне **Хранилища** выберите закладку **Уязвимости**.

   Закладка **Уязвимости** содержит список уязвимостей, которые обнаружил Kaspersky Endpoint Security в результате выполнения задачи поиска уязвимостей.

4. В списке уязвимостей выберите запись об уязвимости, которую нужно скрыть.

   В нижней части списка уязвимостей откроется блок со сведениями о выбранной уязвимости и рекомендациями по ее исправлению.

5. Нажмите на кнопку **Скрыть**.

Kaspersky Endpoint Security присвоит выбранной уязвимости статус *Скрытая*. Записи об уязвимостях со статусом *Скрытая* перемещаются в конец списка уязвимостей и выделяются серым цветом.

6. Чтобы скрыть запись об уязвимостях в списке уязвимостей, установите флажок **Скрытые** в верхней части списка.

Фильтрация списка уязвимостей по уровню критичности

Чтобы отфильтровать список уязвимостей по уровню критичности, выполните следующие действия:

1. Откройте главное окно программы (на стр. 64).

2. По ссылке **Карантин**, расположенной в верхней части главного окна программы, откройте окно **Хранилища**.

3. В окне **Хранилища** выберите закладку **Уязвимости**.

   Закладка **Уязвимости** содержит список уязвимостей, которые обнаружил Kaspersky Endpoint Security в результате выполнения задачи поиска уязвимостей. В верхней части списка уязвимостей в строке **Показать критичность** отображаются три значка уровней критичности уязвимостей (Предупреждение, Важный, Критический). Нажимая на значки, вы можете фильтровать список уязвимостей по уровню критичности.

4. Нажмите на один, два или три значка уровней критичности. Уязвимости, соответствующие выбранным уровням критичности, отобразятся в списке. Чтобы выключить отображение уязвимостей определенного уровня в списке, нажмите на значок уровня критичности еще раз. Если не выбран ни один уровень критичности, список уязвимостей пуст.

Заданные вами условия фильтрации записей в списке уязвимостей сохраняются после того, как вы закрыли окно **Хранилища**.

Фильтрация списка уязвимостей по статусам Исправленные и Скрытые

Чтобы отфильтровать список уязвимостей по статусам уязвимостей Исправленные и Скрытые, выполните следующие действия:

1. Откройте главное окно программы (на стр. 64).

2. По ссылке **Карантин**, расположенной в верхней части главного окна программы, откройте окно **Хранилища**.

3. В окне **Хранилища** выберите закладку **Уязвимости**.

   Закладка **Уязвимости** содержит список уязвимостей, которые обнаружил Kaspersky Endpoint Security в результате выполнения задачи поиска уязвимостей.

4. Рядом с параметром **Показать уязвимости** находятся флажки, обозначающие статус уязвимостей. Чтобы отфильтровать список уязвимостей по статусу *Исправленные*, выполните одно из следующих действий:

   - Установите флажок **Исправленные**, если хотите, чтобы в списке уязвимостей отображались записи об исправленных уязвимостях. Записи об исправленных уязвимостях отображаются в списке уязвимостей серым цветом.

   - Снимите флажок **Исправленные**, если хотите, чтобы в списке уязвимостей не отображались записи об исправленных уязвимостях.

5. Чтобы отфильтровать список уязвимостей по статусу *Скрытые*, выполните одно из следующих действий:

   - Установите флажок **Скрытые**, если хотите, чтобы в списке уязвимостей отображались записи о скрытых уязвимостях. Записи о скрытых уязвимостях отображаются в списке уязвимостей серым цветом.

   - Снимите флажок **Скрытые**, если хотите, чтобы в списке уязвимостей не отображались записи о скрытых уязвимостях.

Заданные вами условия фильтрации записей в списке уязвимостей не сохраняются после того, как вы закрыли окно **Хранилища**.

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. 453) процесс ее выполнения отображается в поле напротив названия задачи в блоке **Управление задачами** на закладке **Центр управления** главного окна Kaspersky Endpoint Security.

Информация о результатах выполнения задачи проверки целостности фиксируется в отчетах (см. раздел "Работа с отчетами" на стр. 456).

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. 64).
2. Выберите закладку **Центр управления**.
3. Раскройте блок **Управление задачами**.
4. По правой клавише мыши откройте контекстное меню строки с названием задачи проверки целостности.
5. Выполните одно из следующих действий:

   - Выберите в контекстном меню пункт **Запустить проверку**, если вы хотите запустить задачу проверки целостности.

     Статус выполнения задачи, отображающийся справа от кнопки с названием задачи, изменится на *Выполняется*.

   - Выберите в контекстном меню пункт **Остановить проверку**, если вы хотите остановить задачу проверки целосности.

     Статус выполнения задачи, отображающийся справа от кнопки с названием задачи, изменится на *Остановлено*.

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. 66).

2. В левой части окна в разделе **Задачи по расписанию** 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 **OK**.

6. 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

Принципы работы с отчетами

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.

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 **Все компоненты защиты**. Содержит информацию о событиях, возникающих в ходе работы следующих компонентов Kaspersky Endpoint Security:
  - Файловый Антивирус.
  - Почтовый Антивирус.
  - Веб-Антивирус.
  - Мониторинг системы.
  - Сетевой экран.
  - Защита от сетевых атак.
  - Защита от атак BadUSB.
- 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. 463) 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.

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. 66).

2. В левой части окна в разделе **Дополнительные параметры** выберите подраздел **Отчеты и хранилища**.

3. В правой части окна в блоке **Параметры отчетов** 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. 66).

2. В левой части окна в разделе **Дополнительные параметры** выберите подраздел **Отчеты и хранилища**.

3. В правой части окна в блоке **Параметры отчетов** 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

Чтобы просмотреть отчеты, выполните следующие действия:

1. Откройте главное окно программы (на стр. 64).

2. По ссылке **Отчеты**, расположенной в верхней части главного окна программы, откройте окно **Отчеты**.

3. Если вы хотите сформировать отчет "Все компоненты защиты", в левой части окна **Отчеты** в списке компонентов и задач выберите пункт **Все компоненты защиты**.

   В правой части окна отобразится отчет "Все компоненты защиты", содержащий список событий о работе всех компонентов защиты Kaspersky Endpoint Security.

4. Если вы хотите сформировать отчет о работе компонента или задачи, 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.

По умолчанию события в отчете отсортированы по возрастанию значений 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. 64).

2. По ссылке **Отчеты**, расположенной в верхней части главного окна программы, откройте 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

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. 64).
2. По ссылке **Отчеты**, расположенной в верхней части главного окна программы, откройте окно **Отчеты**.
3. Выполните одно из следующих действий:
   - Если вы хотите сформировать отчет "Все компоненты защиты", в списке компонентов и задач выберите пункт **Все компоненты защиты**.

     В правой части окна отобразится отчет "Все компоненты защиты", содержащий список событий о работе всех компонентов защиты.
   - Если вы хотите сформировать отчет о работе определенного компонента или задачи, выберите этот компонент или задачу в списке компонентов и задач.

     В правой части окна отобразится отчет, содержащий список событий о работе выбранного компонента или задачи.
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. 66).

2. В левой части окна в разделе **Дополнительные параметры** выберите подраздел **Отчеты и хранилища**.

3. В правой части окна в блоке **Параметры отчетов** нажмите на кнопку **Удалить отчеты**.

   Откроется окно **Удаление информации из отчетов**.

4. Установите флажки для тех отчетов, из которых вы хотите удалить информацию:

   - **Все отчеты**.
   - **Общий отчет защиты**. Содержит информацию о работе следующих компонентов Kaspersky Endpoint Security:

- Файловый Антивирус.
- Почтовый Антивирус.
- Веб-Антивирус.
- Мониторинг системы.
- Сетевой экран.
- Защита от сетевых атак.
- Защита от атак BadUSB.

- **Отчет задач проверки**. Содержит информацию о выполненных задачах проверки:
  - Полная проверка.
  - Проверка важных областей.
  - Выборочная проверка.
  - Проверка целостности.
- **Отчет задач обновления**. Содержит информацию о выполненных задачах обновления.
- **Отчет компонента Сетевой экран**. Содержит информацию о работе Сетевого экрана.
- **Отчет компонентов контроля**. Содержит информацию о работе следующих компонентов Kaspersky Endpoint Security:
  - Контроль запуска программ.
  - Контроль активности программ.
  - Контроль устройств.
  - Веб-Контроль.
- **Отчет о шифровании данных**.

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 баз и модулей 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. 66).

2. В левой части окна в разделе **Дополнительные параметры** выберите подраздел **Отчеты и хранилища**.

   В правой части окна отобразятся параметры отчетов и хранилищ.

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, нажмите **Пуск** → **Панель уравления** → **Администрирование** → **Просмотр событий**.

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. 66).

2. В левой части окна в разделе **Дополнительные параметры** выберите подраздел **Отчеты и хранилища**.

   В правой части окна отобразятся параметры отчетов и хранилищ.

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.

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. Нажмите на кнопку **ОК**.

11. В окне **Настройка почтовых уведомлений** 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. 66).

2. В левой части окна в разделе **Дополнительные 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. 62) 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 при первом лечении или удалении этого файла. Резервные копии файлов хранятся в специальном формате и не представляют опасности.

Иногда при лечении файлов не удается сохранить их целостность. Если вылеченный файл содержал важную информацию, которая в результате лечения стала полностью или частично недоступна, пользователь может попытаться восстановить файл из его вылеченной копии в папку исходного размещения файла.

После очередного обновления баз и модулей программы возможна ситуация, когда Kaspersky Endpoint Security сможет однозначно определить угрозу и устранить ее. По этой причине рекомендуется проверять копии файлов, находящиеся в резервном хранилище, после каждого обновления баз и модулей программы.

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. 66).

2. В левой части окна в разделе **Дополнительные параметры** выберите подраздел **Отчеты и хранилища**.

3. Выполните одно из следующих действий:

   - В правой части окна в блоке **Параметры резервного хранилища** 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 **Параметры резервного хранилища** 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. 66).

2. В левой части окна в разделе **Дополнительные параметры** выберите подраздел **Отчеты и хранилища**.

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 **Параметры резервного хранилища** 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.

Работа с карантином

Kaspersky Endpoint Security удаляет файлы (см. раздел «Удаление файлов из карантина» на стр. 478) с любым статусом из из карантина автоматически по истечении времени, заданного в параметрах программы.

Работая с карантином, вы можете выполнять следующие действия с файлами:

- просматривать файлы, помещенные на карантин в ходе работы Kaspersky Endpoint Security;
- проверять возможно зараженные файлы, используя текущую версию баз и модулей Kaspersky Endpoint Security;
- восстанавливать файлы из карантина в папки их исходного размещения;
- удалять файлы из карантина;
- открывать папки исходного размещения файлов.

Набор файлов, помещенных на карантин, представлен в виде таблицы.

Кроме того, вы можете выполнять следующие действия, работая с табличными данными:

- фильтровать файлы, помещенные на карантин, по графам или по условиям сложного фильтра;
- использовать функцию поиска файлов на карантине;
- сортировать файлы на карантине;
- изменять порядок и набор граф, отображаемых в таблице файлов на карантине;

Вы можете скопировать выбранные события карантина в буфер обмена. Чтобы выбрать несколько файлов, помещенных на карантин, 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

Включение и выключение проверки файлов на карантине после обновления

Если при проверке файла Kaspersky Endpoint Security обнаруживает некоторые признаки заражения, но не может однозначно определить, какими вредоносными программами он заражен, то Kaspersky Endpoint Security помещает такой файл на карантин (см. раздел "О резервном хранилище" на стр. 471). Возможно, после очередного обновления баз и модулей программы Kaspersky Endpoint Security однозначно определит угрозу и устранит ее. Вы

можете включить автоматическую проверку файлов на карантине после каждого обновления баз и модулей программы.

Рекомендуется периодически проверять файлы на карантине. В результате проверки статус файлов может измениться. Ряд файлов может быть вылечен и восстановлен в прежнее местоположение, и вы сможете продолжить работу с ними.

Чтобы включить или выключить проверку файлов на карантине после обновления, выполните следующие действия:

1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 66).

2. В левой части окна в разделе **Дополнительные параметры** выберите подраздел **Отчеты и хранилища**.

   В правой части окна отобразятся параметры управления отчетами и хранилищами.

3. В блоке **Параметры карантина и резервного хранилища** выполните одно из следующих действий:

   - Установите флажок **Проверять файлы на карантине после обновления**, если вы хотите включить проверку файлов на карантине после каждого обновления Kaspersky Endpoint Security.

   - Снимите флажок **Проверять файлы на карантине после обновления**, если вы хотите выключить проверку файлов на карантине после каждого обновления Kaspersky Endpoint Security.

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

Запуск задачи выборочной проверки для файлов на карантине

После очередного обновления баз и модулей программы возможна ситуация, когда Kaspersky Endpoint Security сможет однозначно определить угрозу в файлах, хранящихся на карантине, и устранить ее. Если в параметрах программы не задана автоматическая проверка файлов на карантине после каждого обновления баз и модулей программы, то вы можете вручную запустить задачу выборочной проверки для файлов на карантине.

Чтобы запустить задачу выборочной проверки для файлов на карантине, выполните следующие действия:

1. Откройте главное окно программы (на стр. 64).

2. По ссылке **Карантин**, расположенной в верхней части главного окна программы, откройте окно **Хранилища**.

   Откроется закладка **Карантин** окна **Хранилища**.

3. На закладке **Карантин** выберите один или несколько возможно зараженных файлов, которые вы хотите проверить.

   Чтобы выбрать несколько файлов, помещенных на карантин, 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**.

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**.

После завершения проверки на экране отобразится уведомление о количестве проверенных файлов и количестве обнаруженных угроз.

Восстановление файлов из карантина

Чтобы восстановить файлы из карантина, выполните следующие действия:

1. Откройте главное окно программы (на стр. 64).

2. По ссылке **Карантин**, расположенной в верхней части главного окна программы, откройте окно **Хранилища**.

   Откроется закладка **Карантин** окна **Хранилища**.

3. Если вы хотите восстановить все файлы, помещенные на карантин, то в контекстном меню любого файла выберите пункт **Восстановить все**.

Kaspersky Endpoint Security переместит все файлы из карантина в папки их исходного размещения.

4. Если вы хотите восстановить один или несколько файлов из карантина, то выполните следующие действия:

   a. На закладке **Карантин** выберите один или несколько файлов, которые вы хотите восстановить из карантина.

   Чтобы выбрать несколько файлов, помещенных на карантин, 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 переместит выбранные файлы в папки их исходного размещения.

Удаление файлов из карантина

Чтобы удалить файлы из карантина, выполните следующие действия:

1. Откройте главное окно программы (на стр. 64).

2. По ссылке **Карантин**, расположенной в верхней части главного окна программы, откройте окно **Хранилища**.

   Откроется закладка **Карантин** окна **Хранилища**.

3. Если вы хотите удалить все файлы из карантина, то в контекстном меню любого файла выберите пункт **Удалить все**.

   Kaspersky Endpoint Security удалит все файлы из карантина.

4. Если вы хотите удалить один или несколько файлов из карантина, то выполните следующие действия:

    a. В таблице на закладке **Карантин** выберите один или несколько возможно зараженных файлов, которые вы хотите удалить из карантина.

    Чтобы выбрать несколько файлов, помещенных на карантин, 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 файлы из карантина.

Работа с резервным хранилищем

Если в файле обнаружен вредоносный код, Kaspersky Endpoint Security блокирует файл, 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 (см. раздел "Удаление резервных копий файлов из резервного хранилища" на стр. 482) 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;
- 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 выбранные события 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

Чтобы восстановить файлы из резервного хранилища, выполните следующие действия:

1. Откройте главное окно программы (на стр. 64).

2. По ссылке **Хранилище**, расположенной в верхней части главного окна программы, откройте окно **Хранилище**.

3. В окне **Хранилище** выберите закладку **Резервное хранилище**.

4. Если вы хотите восстановить все файлы из резервного хранилища, то в контекстном меню любого файла выберите пункт **Восстановить все**.

   Kaspersky Endpoint Security восстановит все файлы из их резервных копий в папки их исходного размещения.

5. Если вы хотите восстановить один или несколько файлов из резервного хранилища, то выполните следующие действия:

   a. В таблице на закладке **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. 64).

2. По ссылке **Хранилище**, расположенной в верхней части главного окна программы, откройте окно **Хранилище**.

3. В окне **Хранилище** выберите закладку **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 на закладке **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 дополнительных параметров Kaspersky Endpoint Security.

В этом разделе

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. 66).
2. В левой части окна выберите раздел **Дополнительные параметры**.

   В правой части окна отобразятся дополнительные параметры программы.
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. 66).
2. В левой части окна выберите раздел **Дополнительные параметры**.

   В правой части окна отобразятся дополнительные параметры программы.
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.

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:

- Файловый Антивирус.
- Почтовый Антивирус.
- Веб-Антивирус.
- Контроль активности программ.
- Задачи проверки.
- Мониторинг системы.

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. 494).

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. 66).

2. В левой части окна 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 оба критерия 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 **Название файла или папки**.

   c. Введите название файла или папки, маску названия 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".

   d. Нажмите на кнопку **ОК** в окне **Хеш объекта**.

   Ссылка на добавленное 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. 66).

2. В левой части выберите раздел **Антивирусная защита**.

   В правой части окна отобразятся параметры антивирусной защиты.

3. В блоке **Исключения из проверки и доверенные программы** 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. 66).

2. В левой части выберите раздел **Антивирусная защита**.

   В правой части окна отобразятся параметры антивирусной защиты.

3. В блоке **Исключения из проверки и доверенные программы** 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. 66).

2. В левой части выберите раздел **Антивирусная защита**.

   В правой части окна отобразятся параметры антивирусной защиты.

3. В блоке **Исключения из проверки и доверенные программы** 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. 66).

2. В левой части выберите раздел **Антивирусная защита**.

   В правой части окна отобразятся параметры антивирусной защиты.

3. В блоке **Исключения из проверки и доверенные программы** 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 **OK** 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. 497). 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 **ОК** 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. 66).

2. В левой части выберите раздел **Антивирусная защита**.

   В правой части окна отобразятся параметры антивирусной защиты.

3. В блоке **Исключения из проверки и доверенные программы** 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 **ОК**.

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. 66).

2. В левой части выберите раздел **Антивирусная защита**.

   В правой части окна отобразятся параметры антивирусной защиты.

3. В блоке **Исключения из проверки и доверенные программы** 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.

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. 66).

2. В левой части окна выберите раздел **Дополнительные параметры**.

   В правой части окна отобразятся дополнительные параметры программы.

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. 66).

2. В левой части окна выберите раздел **Дополнительные параметры**.

   В правой части окна отобразятся дополнительные параметры программы.

3. Выполните одно из следующих действий:

   - Установите флажок **Выключить внешнее управление системной службой**, если вы хотите включить механизм защиты от внешнего управления.

   - Снимите флажок **Выключить внешнее управление системной службой**, 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. 66).

2. В левой части выберите раздел **Антивирусная защита**.

   В правой части окна отобразятся параметры антивирусной защиты.

3. В блоке **Исключения из проверки и доверенные программы** 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. 506), 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 (см. раздел "Об обновлении баз и модулей программы" на стр. 397);
- задача полной проверки (см. раздел "О задачах проверки" на стр. 412);
- задача проверки важных областей (см. раздел "О задачах проверки" на стр. 412);
- задача выборочной проверки (см. раздел "О задачах проверки" на стр. 412);
- задача проверки целостности (см. раздел "О задаче проверки целостности" на стр. 452).

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. 507). *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. 508).

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. 66).

2. В левой части окна выберите раздел **Антивирусная защита**.

   В правой части окна отобразятся параметры антивирусной защиты.

3. В блоке **Объекты** 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** 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. 66).

2. В левой части окна выберите раздел **Антивирусная защита**.

   В правой части окна отобразятся параметры антивирусной защиты.

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 **Общие параметры защиты** 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 **Общие параметры защиты** 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. 66).

2. В левой части окна выберите раздел **Дополнительные параметры**.

   В правой части окна отобразятся дополнительные параметры программы.

3. В блоке **Режим работы** нажмите на кнопку **Настройка**.

   Откроется окно **Режим работы**.

4. В окне **Режим работы** 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.

5. 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. 66).

2. В левой части окна выберите раздел **Дополнительные параметры**.

   В правой части окна отобразятся дополнительные параметры программы.

3. В блоке **Режим работы** нажмите на кнопку **Настройка**.

   Откроется окно **Режим работы**.

4. В окне **Режим работы** 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.

5. 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 10 Service Pack 2 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. 552).

Чтобы включить защиту паролем, выполните следующие действия:

1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 66).
2. В левой части окна выберите раздел **Дополнительные параметры**.

   В правой части окна отобразятся параметры программы.
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**.

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. 66).

2. В левой части окна выберите раздел **Дополнительные параметры**.

   В правой части окна отобразятся параметры программы.

3. В блоке **Защита паролем** нажмите на кнопку **Настройка**.

   Откроется окно **Защита паролем**.

4. Снимите флажок **Включить защиту паролем**.

5. Нажмите на кнопку **ОК**.

После выключения защиты паролем ограничение доступа к программе будет отменено при следующем запуске Kaspersky Endpoint Security .

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. 66).

2. В левой части окна выберите раздел **Дополнительные параметры**.

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.

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 **Дополнительные параметры** выберите подраздел **Параметры программы**.
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 (см. раздел "Применение временного пароля в интерфейсе Kaspersky Endpoint Security" на стр. 517).

Применение временного пароля в интерфейсе Kaspersky Endpoint Security

Эта инструкция адресована пользователям клиентских компьютеров с установленной программой Kaspersky Endpoint Security.

Чтобы применить временный пароль, выполните следующие действия:

1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 66).

2. В левой части окна выберите раздел **Дополнительные параметры**.

   В правой части окна отобразятся параметры программы.

3. В блоке **Защита паролем** нажмите на кнопку **Временный пароль**.

   Откроется окно **Временный пароль**.

4. Установите флажок **Включить использование временного пароля**.

5. В поле ввода укажите пароль, полученный от администратора Kaspersky Security Center.

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

После применения временного пароля становятся доступны операции, указанные администратором Kaspersky Security Center. В окне **Временный пароль** отображается дата истечения срока действия временного пароля и разрешенные операции.

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.

Вы можете найти информацию об управлении программой через Kaspersky Security Center, не указанную в этой справке, в *Руководстве администратора 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 (на стр. 18).

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"**.

     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"**.

     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 **Дополнительные 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 **Дополнительные 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 баз и модулей 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.

- **Обновление**. Kaspersky Endpoint Security обновляет базы и модули программы в соответствии с установленными параметрами обновления.
- **Откат обновления**. Kaspersky Endpoint Security откатывает последнее обновление баз и модулей.
- **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 **Дополнительные параметры** выберите подраздел **Параметры программы**.
7. В блоке **Режим работы** 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: <Нзвание 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.
5. В окне мастера **Выбор устройств, которым будет назначена задача** нажмите на кнопку **Назначить задачу выборке устройств**.

6. В следующем окне мастера нажмите на кнопку **Выбрать**.

   Откроется окно **Выборка устройств**.

7. Выберите нужную выборку устройств.

8. Нажмите на кнопку **ОК** в окне **Выборка устройств**.

9. 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. 521) 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. 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.
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. 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 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. 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.

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 **OK**, 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.

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 параметр программы на клиентском компьютере определяется статусом «замка» у параметра в политике:

- Если параметр закрыт "замком" (), это означает, что вы не можете изменить значение параметра локально. Для всех клиентских компьютеров группы администрирования используется значение параметра, заданное политикой.

- Если параметр не закрыт "замком" (), это означает, что вы можете изменить значение параметра локально. Для всех клиентских компьютеров группы администрирования используются значения параметра, установленные локально. Значение параметра, установленное в политике, не применяется.

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:

- Антивирусная защита. Функциональная область включает Файловый Антивирус, Почтовый Антивирус, Веб-Антивирус, задачи проверки.

- Контроль запуска программ. Функциональная область включает компонент Контроль запуска программ.

- Контроль устройств. Функциональная область включает компонент Контроль устройств.
- Шифрование. Функциональная область включает компоненты шифрования жестких дисков, файлов и папок.
- Доверенная зона. Функциональная область включает Доверенную зону.
- Веб-Контроль. Функциональная область включает компонент Веб-Контроль.
- Предотвращение вторжений. Функциональная область включает Мониторинг активности программ, Сетевой экран, Защиту от сетевых атак, Контроль активности программ.
- Базовая функциональность. Функциональная область включает общие параметры программы, не указанные в других функциональных областях, в том числе: лицензирование, параметры KSN, задачи инвентаризации и обновления баз и модулей 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. 522). В разделах **Антивирусная защита** и **Контроль рабочего места** окна **Свойства: <Название политики>** представлены параметры компонентов защиты и контроля, в разделе **Шифрование данных** представлены параметры шифрования файлов и папок, жестких дисков и съемных дисков, а в разделе **Дополнительные параметры** представлены параметры программы.

   Чтобы включить отображение параметров шифрования данных и компонентов контроля в параметрах политики, требуется установить соответствующие флажки в окне Kaspersky Security Center **Настройка интерфейса**.

6. Измените параметры политики.

7. В окне **Свойства: <Название политики>** нажмите на кнопку **ОК**, чтобы сохранить внесенные изменения.

Выбор параметров для отображения в политике Kaspersky Security Center

Чтобы выбрать параметры для отображения в политике Kaspersky Security Center, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.

2. В контекстном меню узла **Сервер администрирования – <Имя компьютера>** дерева Консоли администрирования выберите пункт **Вид → Настройка интерфейса**.

   Откроется окно **Настройка интерфейса**.

3. В окне **Настройка интерфейса** установите флажки напротив тех параметров, которые должны отображаться в параметрах создания политики Kaspersky Security Center и в ее свойствах:

   - Установите флажок **Отображать параметры контроля рабочего места**, если вы хотите включить отображение параметров компонентов контроля в мастере создания политики Kaspersky Security Center и в ее свойствах.

   - Установите флажок **Отображать шифрование и защиту данных**, если вы хотите включить отображение параметров шифрования данных в мастере создания политики Kaspersky Security Center и в ее свойствах.

4. Нажмите на кнопку **OK**.

Отправка сообщений пользователей на сервер Kaspersky Security Center

У пользователя может возникнуть необходимость отправить сообщение администратору локальной сети организации в следующих случаях:

- Контроль устройств заблокировал доступ к устройству.

  Шаблон сообщения с запросом доступа к заблокированному устройству доступен в интерфейсе Kaspersky Endpoint Security в разделе Контроль устройств (см. стр. 256).

- Контроль запуска программ запретил запуск программы.

  Шаблон сообщения с запросом разрешения на запуск заблокированной программы доступен в интерфейсе Kaspersky Endpoint Security в разделе Контроль запуска программ (см. стр. 196).

- 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. 291).

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. 542). 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 запуска программ (см. раздел "Изменение шаблонов сообщений Контроля запуска программ" на стр. 196), Контроль устройств (см. раздел "Изменение шаблонов сообщений Контроля устройств" на стр. 256) и Веб-Контроль (см. раздел "Изменение шаблонов сообщений Веб-Контроля" на стр. 291) 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 программа Kaspersky Endpoint Security, установленная на компьютере пользователя, работает не под политикой или под политикой 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.

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

(инфраструктура расположена на сторонних серверах, например, внутри сети интернет-провайдера).

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

Во время использования 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.

Сбор, обработка и хранение персональных данных пользователя не производится. 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. 547).

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. 535).

Участие в Kaspersky Security Network является добровольным. Программа предлагает участвовать в 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. 66).
2. В левой части окна в разделе **Дополнительные параметры** выберите подраздел **Параметры KSN**.

   В правой части окна отобразятся параметры Kaspersky Security Network.
3. Выполните одно из следующих действий:

   - Установите флажок **Принимаю условия Положения и участвую в KSN**, если вы хотите включить использование Kaspersky Security Network.

- Снимите флажок **Принимаю условия Положения и участвую в KSN**, 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 кнопку **Kaspersky Security Network**.

   Откроется окно **Kaspersky Security Network**.

   В левой части окна **Kaspersky Security Network** отображается режим подключения к Kaspersky Security Network в виде круглой кнопки **KSN**:

   - Если Kaspersky Endpoint Security не подключен к Kaspersky Security Network, то кнопка **KSN** имеет серый цвет. Под кнопкой **KSN** отображается статус *Выключено*.

   - Если Kaspersky Endpoint Security подключен к Kaspersky Security Network и серверы KSN доступны, то кнопка **KSN** имеет зеленый цвет. Под кнопкой **KSN** отображается статус *Включено*, тип используемого KSN – **Локальный KSN** или **Глобальный KSN**, а также дата и время последней синхронизации с серверами KSN. В правой части окна отображается статистика о репутации файлов, веб-ресурсов и программного обеспечения.

   > Получение статистических данных по использованию KSN Kaspersky Endpoint Security производит при открытии окна **Kaspersky Security Network**. Обновление статистики в реальном времени не производится.

- Если Kaspersky Endpoint Security подключен к Kaspersky Security Network, но серверы KSN недоступны, то кнопка **KSN** имеет красный цвет. Под кнопкой **KSN** отображается статус *Включено*.

  > Если время, прошедшее после последней синхронизации с серверами KSN, превышает 15 минут или имеет статус *Неизвестно*, это означает, что серверы KSN недоступны. В такой ситуации рекомендуется обратиться в Службу технической поддержки или к поставщику услуг.

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

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

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. 546).

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».

Источники информации о программе

Этот раздел содержит описание источников информации о программе.

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

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 (см. раздел "Источники информации о программе" на стр. 551), рекомендуется обратиться в Службу технической поддержки. Сотрудники Службы технической поддержки ответят на ваши вопросы об установке и использовании программы.

Техническая поддержка предоставляется только пользователям, которые приобрели коммерческую лицензию на использование программы. Пользователям, которые получили пробную лицензию, техническая поддержка не предоставляется.

> Перед обращением в Службу технической поддержки ознакомьтесь с правилами предоставления технической поддержки (http://support.kaspersky.ru/support/rules).

Вы можете связаться со специалистами Службы технической поддержки одним из

следующих способов:

- позвонить 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 (http://support.kaspersky.ru/support/rules).

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 (http://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, дампы падения программы.

С помощью Kaspersky Endpoint Security вы можете получить необходимую информацию. Полученную информацию вы можете сохранить на жесткий диск и отправить позже в удобное для вас время.

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 и отправки 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.

Параметры, связанные с определением адреса дамп-сервера для отправки файлов дампов в "Лабораторию Касперского", хранятся на компьютере пользователя. В случае необходимости значения этих параметров могут быть изменены в ветке реестра операционной системы `"DumpServerConfigUrl"="https://dmpcfg.kaspersky-labs.com/dumpserver/config.xml"`.

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. 64).
2. В главном окне программы нажмите на кнопку  .

   Откроется окно **Поддержка**.
3. В окне **Поддержка** нажмите на кнопку **Трассировка системы**.

   Откроется окно **Информация для поддержки**.
4. Чтобы запустить процесс трассировки, установить флажок **Включить трассировку**.
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 снимите флажок **Включить трассировку**.

После создания файла трассировки вы можете перейти к загрузке результатов трассировки на сервер "Лаборатории Касперского" (см. раздел "Отправка файлов на сервер Службы технической поддержки" на стр. 561).

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 измененном и недоступном для чтения виде 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.enc1`.

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. Для консультации по просмотру данных требуется обратиться в Службу технической поддержки "Лаборатории Касперского".

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 Почтового Антивируса 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.

Включение и выключение отправки файлов дампов и файлов трассировки в "Лабораторию Касперского"

Чтобы включить или выключить отправку файлов дампов и файлов трассировки в "Лабораторию Касперского", выполните следующие действия:

1. Откройте окно настройки параметров программы (см. раздел "Закладка настройки параметров программы" на стр. 66).

2. В левой части окна выберите раздел **Дополнительные параметры**.

   В правой части окна отобразятся дополнительные параметры программы.

3. В блоке **Режим работы** нажмите на кнопку **Настройка**.

   Откроется окно **Режим работы**.

4. В окне **Режим работы** установите флажок **Включить запись дампов**, чтобы программа записывала дампы программы.

5. Выполните одно из следующих действий:

   - Установите флажок **Отсылать файлы дампов и файлы трассировки в "Лабораторию Касперского"**, если вы хотите, чтобы в случае сбоя в работе программы при последующем ее запуске с помощью окна **Загрузка информации для поддержки на сервер** программа предлагала отправить файлы дампов и трассировки на исследование причин сбоя в "Лабораторию Касперского".

   - Иначе снимите флажок **Отсылать файлы дампов и файлы трассировки в "Лабораторию Касперского"**.

6. Нажмите на кнопку **ОК** в окне **Режим работы**.

7. Нажмите на кнопку **Сохранить** в главном окне программы, чтобы сохранить внесенные изменения.

Отправка файлов на сервер Службы технической поддержки

Файлы с информацией об операционной системе, файлы трассировки и файлы дампов требуется отправить специалистам Службы технической поддержки "Лаборатории Касперского".

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

1. Перезапустите программу Kaspersky Endpoint Security после сбоя в ее работе.

   Откроется окно **Сбой при предыдущем запуске программы**.

   > Окно **Сбой при предыдущем запуске программы** будет открываться после каждого запуска Kaspersky Endpoint Security (в том числе и после перезагрузки компьютера), пока вы не отправите файлы дампов или файлы трассировки в Службу технической поддержки или не нажмете на кнопку **Не отправлять**.

2. В окне **Сбой при предыдущем запуске программы** откройте список сформированных файлов по ссылке **здесь**.

3. Установите флажки рядом с теми файлами, которые вы хотите отправить в Службу технической поддержки.

4. Нажмите на кнопку **Показать текст Положения**.

   Откроется окно **Положение о предоставлении данных**.

5. Прочтите текст Положения о предоставлении данных и нажмите на кнопку **Закрыть**.

6. В окне **Сбой при предыдущем запуске программы** установите флажок **Я ознакомился и согласен с Положением о предоставлении данных**.

7. Нажмите на кнопку **Отправить**.

   Откроется окно **Номер запроса**.

8. В окне **Номер запроса** укажите номер, присвоенный вашему запросу при обращении в Службу технической поддержки через Kaspersky CompanyAccount.

9. Нажмите на кнопку **ОК**.

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

Включение и выключение защиты файлов дампов и трассировок

Файлы дампов и файлы трассировки содержат информацию об операционной системе, а также конфиденциальные данные пользователя (см. раздел "О составе и хранении файлов трассировки" на стр. 557). 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. 66).

2. В левой части выберите раздел **Дополнительные параметры**.

   В правой части окна отобразятся параметры программы.

3. В блоке **Режим работы** нажмите на кнопку **Настройка**.

   Откроется окно **Режим работы**.

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 **Режим работы**.
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

O

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.

A

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 пройти процедуру аутентификации для доступа к зашифрованным жестким дискам и для загрузки операционной системы после шифрования системного жесткого диска.

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".

В

Возможно зараженный файл

Файл, внутри которого содержится либо модифицированный код известного вируса, либо код, напоминающий вирус, но пока не известный "Лаборатории Касперского". Возможно зараженные файлы обнаруживаются с помощью эвристического анализатора.

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

Карантин

Папка, в которую программа "Лаборатории Касперского" помещает обнаруженные возможно зараженные файлы. Файлы на карантине хранятся в зашифрованном виде.

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.

M

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.

H

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 HTTP-логина, пароля и порта соединения, понижение верхнего регистра символов адреса веб-ресурса до нижнего регистра).

В контексте антивирусной 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 антивирусной 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.

Помещение файлов на карантин

Способ обработки возможно зараженного файла, при котором доступ к файлу блокируется и файл перемещается из исходного местоположения в папку карантина, где сохраняется в закодированном виде, что исключает угрозу заражения.

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.

Р

Резервное хранилище

Специальное хранилище, предназначенное для сохранения резервных копий объектов, создаваемых перед их лечением или удалением.

С

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":	http://www.kaspersky.ru
Вирусная энциклопедия:	https://securelist.ru/
Вирусная лаборатория:	https://virusdesk.kaspersky.ru/ (для проверки подозрительных файлов и сайтов)
Веб-форум "Лаборатории Касперского":	http://forum.kaspersky.com

Информация о стороннем коде

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

Предметный указатель

А

Б

В

Г

Д

З

И

К

Л

М

Н

О

П

P

C

У

Ф

Ш

Э