Kaspersky Endpoint Security 10 для Windows

Руководство администратора

ВЕРСИЯ ПРОГРАММЫ: 10.0

Уважаемый пользователь!

Спасибо за то, что выбрали наш продукт. Мы надеемся, что этот документ поможет вам в работе и ответит на большинство возникающих вопросов.

Дата редакции документа: 10.12.2012

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

СОДЕРЖАНИЕ

ОБ ЭТОМ РУКОВОДСТВЕ

Этот документ представляет собой руководство администратора Kaspersky Endpoint Security 10 для Windows® (далее также «Kaspersky Endpoint Security»).

Руководство адресовано администраторам локальных сетей организаций, а также сотрудникам, отвечающим за антивирусную защиту компьютеров в организациях. Руководство также может помочь в решении некоторых задач обычным пользователям, на рабочих компьютерах которых установлена программа Kaspersky Endpoint Security.

Руководство предназначено для следующих целей:

- Помочь установить программу на компьютер, активировать ее и оптимально настроить программу с учетом задач пользователя.
- Обеспечить быстрый поиск информации для решения вопросов, связанных с работой программы.
- Рассказать о дополнительных источниках информации о программе и способах получения технической поддержки.

В ЭТОМ РАЗДЕЛЕ

В ЭТОМ РУКОВОДСТВЕ

Этот документ содержит следующие разделы.

Источники информации о программе (см. стр. 15)

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

Kaspersky Endpoint Security 10 для Windows (см. стр. 17)

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

Установка и удаление программы (см. стр. 22)

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.

Лицензирование программы (см. стр. 50)

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

Интерфейс программы (см. стр. 45)

Этот раздел содержит информацию об основных элементах графического интерфейса программы: значке программы и контекстном меню значка программы, главном окне программы и окне настройки параметров программы.

Запуск и остановка программы (см. стр. 58)

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.

Типовые задачи (см. стр. 60)

Группа разделов, описывающих типовые задачи и компоненты программы. Разделы содержат подробную информацию о том, как настроить параметры задач и компонентов программы.

Управление программой через Kaspersky Security Center (см. стр. 281)

Этот раздел содержит информацию об управлении программой Kaspersky Endpoint Security через Kaspersky Security Center.

Участие в Kaspersky Security Network (см. стр. 293)

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

Обращение в Службу технической поддержки (см. стр. 296)

Этот раздел содержит информацию о способах получения технической поддержки и о том, какие условия требуются для получения помощи от Службы технической поддержки.

Глоссарий (см. стр. 301)

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

ЗАО «Лаборатория Касперского» (см. стр. 305)

Этот раздел содержит информацию о ЗАО «Лаборатория Касперского».

Информация о стороннем коде (см. стр. 306)

Этот раздел содержит информацию о стороннем коде.

Уведомления о товарных знаках (см. стр. 307)

Этот раздел содержит информацию о товарных знаках, упомянутых в документе.

Предметный указатель

Этот раздел позволяет быстро найти необходимые сведения в документе.

Условные обозначения

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

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

Таблица 1. Условные обозначения

Пример текста	Описание условного обозначения
Обратите внимание на то, что...	Предупреждения выделены красным цветом и заключены в рамку. В предупреждениях содержится информация о возможных нежелательных действиях, которые могут привести к потере информации, сбоям в работе оборудования или операционной системы.
Рекомендуется использовать...	Примечания заключены в рамку. Примечания могут содержать полезные советы, рекомендации, особые значения параметров или важные частные случаи в работе программы.
Пример: ...	Примеры приведены в блоках на желтом фоне под заголовком «Пример».
Обновление – это... Возникает событие *Базы устарели*.	Курсивом выделены следующие смысловые элементы текста: • новые термины; • названия статусов и событий программы.
Нажмите на клавишу **ENTER**. Нажмите комбинацию клавиш **ALT**+**F4**.	Названия клавиш клавиатуры выделены полужирным шрифтом и прописными буквами. Названия клавиш, соединенные знаком + (плюс), означают комбинацию клавиш. Такие клавиши нужно нажимать одновременно.
Нажмите на кнопку **Включить**.	Названия элементов интерфейса программы, например, полей ввода, пунктов меню, кнопок, выделены полужирным шрифтом.
➧ *Чтобы настроить расписание задачи, выполните следующие действия:*	Вводные фразы инструкций выделены курсивом и значком «стрелка».
В командной строке введите текст `help` Появится следующее сообщение: `Укажите дату в формате ДД:ММ:ГГ.`	Специальным стилем выделены следующие типы текста: • текст командной строки; • текст сообщений, выводимых программой на экран; • данные, которые требуется ввести пользователю.
<Имя пользователя>	Переменные заключены в угловые скобки. Вместо переменной требуется подставить соответствующее ей значение, опустив угловые скобки.

ИСТОЧНИКИ ИНФОРМАЦИИ О ПРОГРАММЕ

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

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

В ЭТОМ РАЗДЕЛЕ

Источники информации для самостоятельного поиска

Для самостоятельного поиска информации о программе вы можете использовать электронную справку.

В состав электронной справки программы входят файлы справки.

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

Полная справка содержит подробную информацию о том, как управлять защитой компьютера с помощью программы.

Если вы не нашли решения возникшей проблемы самостоятельно, вам рекомендуется обратиться в Службу технической поддержки «Лаборатории Касперского» (см. раздел «Техническая поддержка по телефону» на стр. 299).

Обсуждение программ «Лаборатории Касперского» на форуме

Если ваш вопрос не требует срочного ответа, вы можете обсудить его со специалистами «Лаборатории Касперского» и другими пользователями на нашем форуме (http://forum.kaspersky.com/index.php?showforum=9).

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

Обращение в Отдел локализации и разработки технической документации

Для обращения в Группу разработки документации требуется отправить письмо по адресу docfeedback@kaspersky.com. В качестве темы письма нужно указать «Kaspersky Help Feedback: Kaspersky Endpoint Security 10 для Windows».

KASPERSKY ENDPOINT SECURITY 10 ДЛЯ WINDOWS

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

В ЭТОМ РАЗДЕЛЕ

Что нового

В Kaspersky Endpoint Security 10 для Windows появились следующие новые возможности:

- Добавлена функциональность шифрования жестких дисков и съемных устройств, позволяющая шифровать устройства вместе с их файловой системой.
- Введено разграничение режимов работы программы в зависимости от типа лицензии. В зависимости от типа действующей лицензии программа может работать в следующих режимах:
  - Базовая защита (Core).
  - Стандартная защита (Select).
  - Расширенная защита (Advanced).

Улучшено:

- Внесены улучшения в функциональность компонентов Контроль запуска программ, Контроль устройств и Веб-Контроль.

Комплект поставки

В комплект поставки входят следующие файлы:

- Файлы, необходимые для установки программы всеми доступными способами.
- Файл ksn.txt, с помощью которого вы можете ознакомиться с условиями участия в Kaspersky Security Network (см. раздел «Участие в Kaspersky Security Network» на стр. 293).
- Файл license.txt, с помощью которого вы можете ознакомиться с Лицензионным соглашением. В Лицензионном соглашении указано, на каких условиях вы можете пользоваться программой.

Организация защиты компьютера

Kaspersky Endpoint Security обеспечивает комплексную защиту компьютера от известных и новых 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.

- **Контроль активности программ**. 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.

- **Мониторинг уязвимостей**. Мониторинг уязвимостей в режиме реального времени проверяет программы, запущенные на компьютере пользователя, а также проверяет программы в момент их запуска.

- **Контроль устройств**. Компонент позволяет установить гибкие ограничения доступа к устройствам, являющимся источниками информации (например, жесткие диски, съемные носители информации, 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:

- Контроль запуска программ использует правила контроля запуска программ (см. раздел «О правилах контроля запуска программ» на стр. 123).

- Контроль активности программ использует правила контроля программ (см. раздел «О Контроле активности программ» на стр. 135).

- 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. 150).

- Веб-Контроль использует правила доступа к веб-ресурсам (см. раздел «О правилах доступа к веб-ресурсам» на стр. 161).

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 собирает данные о действиях программ на компьютере и предоставляет эту информацию другим компонентам для более эффективной защиты компьютера.

- **Почтовый Антивирус**. Компонент проверяет входящие и исходящие почтовые сообщения 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.

- **IM-Антивирус**. Компонент проверяет трафик, поступающий на компьютер по протоколам программ для быстрого обмена сообщениями. Компонент обеспечивает безопасную работу со многими программами, предназначенными для быстрого обмена сообщениями.

- **Сетевой экран**. Компонент обеспечивает защиту личных данных, хранящихся на компьютере пользователя, блокируя все возможные для операционной системы угрозы 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. 96).

- **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 тщательную 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 новых вирусов и других программ, представляющих угрозу.

- **Поиск уязвимостей**. Kaspersky Endpoint Security проверяет операционную систему и установленное программное обеспечение на наличие уязвимостей. Это позволяет диагностировать и своевременно решать возможные проблемы, которые могут быть использованы злоумышленниками.

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

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.

Сервисные функции программы

Kaspersky Endpoint Security включает ряд сервисных функций. Сервисные 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 или возможно зараженные файлы, она блокирует эти файлы. Возможно зараженные файлы Kaspersky Endpoint Security переносит в *карантин*, специальное хранилище. 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, самостоятельно помещать файлы на карантин, а также очищать хранилище данных.

- **Сервис уведомлений**. Сервис 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 сбора 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.

Аппаратные и программные требования

Для функционирования Kaspersky Endpoint Security компьютер должен удовлетворять следующим требованиям.

Общие требования:

- 1 ГБ свободного места на жестком диске.
- Microsoft® Internet Explorer® 7.0 и выше.
- Microsoft Windows Installer 3.0 и выше.
- Подключение к интернету для активации программы, обновления баз и модулей программы.

Аппаратные требования к компьютерам, на которых установлены операционные системы для рабочих станций:

- Microsoft Windows XP Professional x86 Edition SP3 и выше:
  - процессор Intel® Pentium® 1 ГГц и выше (или совместимый аналог);
  - 256 МБ свободной оперативной памяти.
- Microsoft Windows Vista® x86 Edition SP2 и выше, Microsoft Windows Vista x64 Edition SP2 и выше, Microsoft Windows 7 Professional / Enterprise / Ultimate x86 Edition, Microsoft Windows 7

Professional / Enterprise / Ultimate x64 Edition, Microsoft Windows 7 Professional / Enterprise / Ultimate x86 Edition SP1 и выше, Microsoft Windows 7 Professional / Enterprise / Ultimate x64 Edition SP1 и выше, Microsoft Windows 8 Professional / Enterprise x86 Edition, Microsoft Windows 8 Professional / Enterprise x64 Edition:

- (x86) процессор Intel Pentium 1 ГГц и выше (или совместимый аналог);
- (x64) процессор Intel Pentium 2 ГГц и выше (или совместимый аналог);
- 512 МБ свободной оперативной памяти.

Аппаратные требования к компьютерам, на которых установлены операционные системы для файловых серверов:

Microsoft Windows Server® 2003 Standard x86 Edition SP2, Microsoft Windows Server 2003 Standard x64 Edition SP2, Microsoft Windows Server 2003 R2 Standard / Enterprise x86 Edition SP2 и выше, Microsoft Windows Server 2003 R2 Standard x64 Edition SP2 и выше, Microsoft Windows Server 2008 R2 Standard / Enterprise x64 Edition, Microsoft Windows Server 2008 R2 Standard / Enterprise x64 Edition SP1 и выше, Microsoft Windows Server 2008 Standard / Enterprise x86 Edition SP2 и выше, Microsoft Windows Server 2008 Standard / Enterprise x64 Edition SP2 и выше, Microsoft Windows Small Business Server 2011 Essentials / Standard x64 Edition, Microsoft Windows Server 2012 Standard / Foundation / Essentials x64 Edition:

- (x86) процессор Intel Pentium 1 ГГц и выше (или совместимый аналог);
- (x64) процессор Intel Pentium 2 ГГц и выше (или совместимый аналог);
- 512 МБ свободной оперативной памяти.

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 10 для Windows может быть установлен на компьютер несколькими способами:

- *Локальная установка* – установка программы на отдельном компьютере. Для запуска и проведения локальной установки требуется непосредственный доступ к этому компьютеру. Локальная установка может быть проведена в одном из двух режимов:

  - *Интерактивном*, с помощью мастера установки программы (см. раздел «Установка программы с помощью мастера установки программы» на стр. 23). Этот режим требует вашего участия в процессе установки.

  - *Тихом*, запуск установки программы в этом режиме выполняется из командной строки, ваше участие в процессе установки (см. раздел «Установка программы из командной строки» на стр. 27) не требуется.

- *Удаленная установка* – установка программы на компьютеры сети, выполняемая удаленно с рабочего места администратора с использованием:

  - программного комплекса Kaspersky Security Center (см. *Руководство по внедрению Kaspersky Security Center*);

  - редактора управления групповыми доменными политиками Microsoft Windows Server (см. раздел «Установка программы через редактор управления групповыми доменными политиками Microsoft Windows Server» на стр. 29).

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

Установка программы с помощью мастера установки программы

Интерфейс мастера установки программы состоит из последовательности окон (шагов). 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, следует 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. 17).

   Запустится мастер установки программы.

2. Следуйте указаниям мастера установки программы.

В этом разделе

Шаг 1. Проверка соответствия системы необходимым условиям установки

Перед установкой Kaspersky Endpoint Security 10 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. 20).
- Выполнение аппаратных и программных требований (см. раздел «Аппаратные и программные требования» на стр. 20).
- 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 привести к возникновению конфликтов. Если такие программы найдены, вам предлагается удалить их вручную.

Если в числе обнаруженных программ есть Антивирус Касперского 6.0 для Windows Workstations® MP4, Антивирус Касперского 6.0 для Windows Servers MP4 или Kaspersky Endpoint Security 8 для Windows, все данные, которые могут быть мигрированы (например, информация об активации, параметры программы), сохраняются и используются при установке Kaspersky Endpoint Security 10 для Windows, а Антивирус Касперского 6.0 для Windows Workstations MP4, Антивирус Касперского 6.0 для Windows Servers MP4 или Kaspersky Endpoint Security 8 для Windows автоматически удаляется.

Шаг 2. Стартовое окно процедуры установки

Если условия для установки программы полностью соответствует 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**. Чтобы прекратить работу мастера установки программы, нажмите на кнопку **Отмена**.

Шаг 3. Просмотр Лицензионного соглашения

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

Внимательно прочтите 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. Соглашение об участии в Kaspersky Security Network

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

Ознакомьтесь с положением о Kaspersky Security Network:

- Если вы согласны со всеми его пунктами, в окне мастера установки программы выберите вариант **Я согласен участвовать в Kaspersky Security Network**.
- Если вы не согласны с условиями участия в Kaspersky Security Network, в окне мастера установки программы выберите вариант **Я не согласен участвовать в Kaspersky Security Network**.

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 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 только компоненты защиты 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».

- *Полная установка*. Если вы выбираете этот тип установки, на компьютер пользователя устанавливаются все компоненты программы с параметрами, рекомендуемыми специалистами «Лаборатории Касперского», включая функциональность шифрования данных. Функциональность шифрования данных недоступна до тех пор, пока отдельно не установлен модуль шифрования (см. раздел «Установка модуля шифрования» на стр. 36).

- *Выборочная установка*. Если вы выбираете этот тип установки, вам предлагается выбрать компоненты для установки (см. раздел «Шаг 6. Выбор компонентов программы для установки» на стр. 25) и указать папку, в которую будет установлена программа (см. раздел «Шаг 7. Выбор папки для установки программы» на стр. 25).

По умолчанию выбрана базовая 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 6. Выбор компонентов программы для установки

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

На этом шаге вы можете выбрать компоненты Kaspersky Endpoint Security 10 для Windows, которые вы хотите установить. По умолчанию для установки выбраны все компоненты программы.

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

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

Чтобы отказаться от установки компонента, в контекстном меню выберите пункт **Компонент будет недоступен**.

Чтобы вернуться к списку устанавливаемых по умолчанию компонентов, 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 7. 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 8. 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 9. Подготовка к установке программы

Поскольку на компьютере могут присутствовать вредоносные программы, способные помешать установке Kaspersky Endpoint Security 10 для Windows, процесс установки рекомендуется защищать.

По умолчанию защита процесса установки включена.

Выключать защиту процесса установки рекомендуется в том случае, когда невозможно выполнить установку программы (например, такая ситуация может возникнуть при удаленной установке через Windows Remote Desktop). Причиной этому может быть включенная защита установки программы. В этом случае прервите установку и запустите мастер установки программы с начала. На шаге «Подготовка к установке программы» снимите флажок **Защитить процесс установки**.

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 название 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**.

При установке программы на компьютер возможен разрыв текущих сетевых соединений. Большинство разорванных соединений восстанавливается через некоторое время.

Шаг 10. 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 10 для Windows запускается мастер первоначальной настройки программы (на стр. 33).

Установка программы из командной строки

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

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

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

  введите в командной строке `setup.exe /pEULA=1 /pKSN=1|0 /pINSTALLEVEL=<значение> /pALLOWREBOOT=1|0 /s` или

  `msiexec /i <название установочного пакета> EULA=1 KSN=1|0 INSTALLEVEL=<значение> ALLOWREBOOT=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. 17). Согласие с положениями Лицензионного соглашения является необходимым условием для установки программы или обновления предыдущей версии программы.

  - `KSN=1|0` означает согласие или отказ от участия 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. 17).

  - `INSTALLLEVEL=<значение>` указывает на тип установки Kaspersky Endpoint Security (см. раздел «Шаг 5. Выбор типа установки» на стр. 25). Параметр необязательный. Если в команде не указано значение параметра `INSTALLLEVEL`, по умолчанию выполняется базовая установка программы.

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

    - `100`. Указывает на базовую установку программы.
    - `200`. Указывает на стандартную установку программы.
    - `300`. Указывает на полную установку программы.

  - `ALLOWREBOOT=1|0` означает согласие или запрет на автоматическую перезагрузку компьютера, если она потребуется после установки программы или обновления предыдущей версии программы. Параметр необязательный. Если в команде не указано значение параметра `ALLOWREBOOT`, по умолчанию считается, что вы запрещаете перезагрузку компьютера после установки программы или обновления предыдущей версии программы.

    Перезагрузка компьютера может понадобиться после обновления предыдущей 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).

- *Чтобы установить программу или обновить предыдущую версию программы с установкой пароля, подтверждающего право на изменение параметров программы и операции с программой,*

  введите в командной строке:

  - `setup.exe /pKLPASSWD=***** /pKLPASSWDAREA=<область действия пароля>` или

    `msiexec /i <название установочного пакета>KLPASSWD=***** KLPASSWDAREA=<область действия пароля>` для установки программы или обновления предыдущей версии программы в интерактивном режиме.

  - `setup.exe /pEULA=1 /pKSN=1|0 /pINSTALLEVEL=<значение> /pKLPASSWD=***** /pKLPASSWDAREA=<область действия пароля> /s` или

    `msiexec /i <название установочного пакета> EULA=1 KSN=1|0 INSTALLEVEL=<значение> KLPASSWD=***** KLPASSWDAREA=<область действия пароля> ALLOWREBOOT=1|0/qn` для установки программы или обновления предыдущей версии программы в тихом режиме.

    Где вместо `<область действия пароля>` вы можете указать один или несколько следующих значений параметра KLPASSWDAREA через «;»:

    - `SET`. Установка пароля на изменение параметров программы.
    - `EXIT`. Установка пароля на завершение работы программы.
    - `DISPROTECT`. Установка пароля на выключение компонентов защиты и остановку задач проверки.
    - `DISPOLICY`. Установка пароля на выключение политики Kaspersky Security Center.
    - `UNINST`. Установка пароля на удаление программы с компьютера.
    - `DISCTRL`. Установка пароля на выключение компонентов контроля (Контроль запуска программ, Контроль активности программ, Мониторинг уязвимостей, Контроль устройств, Веб-Контроль).
    - `REMOVELIC`. Установка пароля на удаление ключа.

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

- setup.ini (см. раздел «Описание параметров файла setup.ini» на стр. 30), содержащего общие параметры установки программы;
- конфигурационного файла install.cfg;
- setup.reg.

Файлы setup.ini, install.cfg и setup.reg должны быть расположены в одной папке с установочным пакетом Kaspersky Endpoint Security 10 для Windows.

Установка программы через редактор управления групповыми доменными политиками Microsoft Windows Server

С помощью редактора управления групповыми доменными политиками Microsoft Windows Server вы можете устанавливать Kaspersky Endpoint Security на рабочих станциях организации, входящих в состав домена, без использования Kaspersky Security Center.

Чтобы установить Kaspersky Endpoint Security через редактор управления групповыми доменными политиками Microsoft Windows Server, выполните следующие действия:

1. Создайте сетевую папку общего доступа на компьютере, являющемся контроллером домена.

2. Поместите дистрибутив Kaspersky Endpoint Security в формате MSI в сетевую папку общего доступа, созданную на предыдущем шаге инструкции.

   Дополнительно в эту сетевую папку общего доступа можно поместить файл setup.ini (см. раздел «Описание параметров файла setup.ini» на стр. 30), содержащий перечень параметров установки Kaspersky Endpoint Security, конфигурационный файл install.cfg, а также файл ключа.

3. Откройте редактор управления групповыми доменными политиками Microsoft Windows Server через консоль управления (MMC) (подробную информацию о работе с редакторе управления групповыми доменными политиками Microsoft Windows Server читайте в *Справочной системе к Microsoft Windows Server*). Для этого выполните следующие действия:

   a. В меню **Пуск** выберите **Администрирование** → **Управление групповыми политиками**.

      Откроется окно Microsoft Windows **Управление групповыми политиками**.

   b. В дереве окна **Управление групповыми политиками** выберите нужный объект групповой политики.

   c. По правой клавише мыши вызовите контекстное меню объекта групповой политики и выберите пункт **Изменить**.

      Откроется редактор управления групповыми доменными политиками Microsoft Windows Server.

4. Создайте новый установочный пакет редактора управления групповыми доменными политиками Microsoft Windows Server. Для этого выполните следующие действия:

   a. В дереве консоли выберите **Объект групповой политики \ Конфигурация компьютера \ Политики \ Конфигурация программ \ Установка программного обеспечения**.

   b. По правой клавише мыши откройте контекстное меню узла **Установка программного обеспечения**.

   c. В контекстном меню выберите пункт **Создать** → **Пакет**.

      Откроется стандартное окно Microsoft Windows Server **Открыть**.

   d. В стандартном окне Microsoft Windows Server **Открыть** укажите путь к дистрибутиву Kaspersky Endpoint Security в формате MSI.

   e. В диалоговом окне **Развертывание программы** выберите параметр **Назначенный**.

   f. Нажмите на кнопку **ОК**.

Групповая политика Microsoft Windows Server будет применена на каждой рабочей станции при следующей регистрации компьютеров в домене. В результате Kaspersky Endpoint Security будет установлен на все компьютеры в домене.

Описание параметров файла setup.INI

Файл setup.ini используется при установке программы через командную строку или редактор управления групповыми доменными политиками Microsoft Windows Server. Файл setup.ini располагается в папке установочного пакета Kaspersky Endpoint Security.

Файл setup.ini содержит следующие параметры:

[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`. Установка этого значения означает согласие с положениями Лицензионного соглашения.
  - `0`. Установка этого значения означает несогласие с положениями Лицензионного соглашения.
- `KSN` – согласие или несогласие участвовать в Kaspersky Security Network. Возможные значения параметра `KSN`:
  - `1`. Установка этого значения означает согласие участвовать в Kaspersky Security Network.
  - `0`. Установка этого значения означает несогласие участвовать в Kaspersky Security Network.
- `Password` – установить пароль для доступа к управлению функциями и параметрами Kaspersky Endpoint Security.
- `PasswordArea` – задать область действия пароля для доступа к управлению функциями и параметрами Kaspersky Endpoint Security. Возможные значения параметра `PasswordArea`:
  - `SET`. Установка пароля на изменение параметров программы.
  - `EXIT`. Установка пароля на завершение работы программы.
  - `DISPROTECT`. Установка пароля на выключение компонентов защиты и остановку задач проверки.
  - `DISPOLICY`. Установка пароля на выключение политики Kaspersky Security Center.
  - `UNINST`. Установка пароля на удаление программы с компьютера.
  - `DISCTRL`. Установка пароля на выключение компонентов контроля (Контроль запуска программ, Контроль активности программ, Мониторинг уязвимостей, Контроль устройств, Веб-Контроль).
  - `REMOVELIC`. Установка пароля на удаление ключа.
- `SelfProtection` – следует ли включать механизм самозащиты Kaspersky Endpoint Security при установке программы. Возможные значения параметра `SelfProtection`:
  - `1`. Установка этого значения означает, что механизм самозащиты включен.
  - `0`. Установка этого значения означает, что механизм самозащиты выключен.

- Reboot – следует ли, при необходимости, выполнять перезагрузку компьютера по завершении установки программы. Возможные значения параметра Reboot:

  - 1. Установка этого значения означает, что при необходимости выполняется перезагрузка компьютера по завершении установки программы.

  - 0. Установка этого значения означает, что, в случае необходимости, перезагрузка компьютера по завершении установки программы не выполняется.

- MSExclusions – добавить программы, рекомендованные 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. 20). Возможные значения параметра MSExclusions:

  - 1. Установка этого значения означает, что программы, рекомендованные компанией Microsoft, добавляются в исключения из проверки.

  - 0. Установка этого значения означает, что программы, рекомендованные компанией Microsoft, не добавляются в исключения из проверки.

- KLExclusions – добавить программы, рекомендованные компанией «Лаборатория Касперского», в исключения из проверки. Возможные значения параметра KLExclusions:

  - 1. Установка этого значения означает, что программы, рекомендованные компанией «Лаборатория Касперского», добавляются в исключения из проверки.

  - 0. Установка этого значения означает, что программы, рекомендованные компанией «Лаборатория Касперского», не добавляются в исключения из проверки.

- NoKLIM5 – следует ли отменить установку сетевых драйверов Kaspersky Endpoint Security при установке программы. По умолчанию сетевые драйверы устанавливаются. Сетевые драйверы Kaspersky Endpoint Security, относящиеся к группе драйверов NDIS и отвечающие за перехват сетевого трафика для таких компонентов программы, как Контроль устройств, Веб-Контроль, Почтовый Антивирус, Веб-Антивирус, Сетевой экран и Защита от сетевых атак, могут привести к конфликтам с другими программами или оборудованием, установленным на компьютере пользователя. На компьютерах под управлением Microsoft Windows XP Professional x86 и Microsoft Windows Server 2003 x86 для решения возможных конфликтов можно отказаться от установки сетевых драйверов. Возможные значения компонента NoKLIM5:

  - 1. Указание этого значения означает, что установка сетевых драйверов Kaspersky Endpoint Security при установке программы отменяется.

  - 0. Указание этого значения означает, что установка сетевых драйверов Kaspersky Endpoint Security при установке программы не отменяется.

- AddEnviroment – добавить в системную переменную %PATH% путь к исполняемым файлам, расположенным в папке установки Kaspersky Endpoint Security. Возможные значения параметра AddEnviroment:

  - 1. Установка этого значения означает, что в системную переменную %PATH% добавляется путь к исполняемым файлам, расположенным в папке установки Kaspersky Endpoint Security.

  - 0. Установка этого значения означает, что в системную переменную %PATH% не добавляется путь к исполняемым файлам, расположенным в папке установки Kaspersky Endpoint Security.

[Components] – выбор компонентов программы для установки. Если не указан ни один из компонентов, то устанавливаются все доступные для операционной системы компоненты.

- ALL – установка всех компонентов.

- MailAntiVirus – установка компонента Почтовый Антивирус.

- `FileAntiVirus` – установка компонента Файловый Антивирус.
- `IMAntiVirus` – установка компонента IM-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 сети.
- `WebControl` – установка компонента Веб-Контроль.
- `DeviceControl` – установка компонента Контроль устройств.
- `ApplicationStartupControl` – установка компонента Контроль запуска программ.
- `DataEncryption` – установка функциональности шифрования данных.
- `VulnerabilityAssessment` – установка функциональности для поиска уязвимостей.
- `AdminKitConnector` – установка коннектора к Агенту администрирования для удаленного управления программой через Kaspersky Security Center.

  Возможные значения параметров:

- 1. Установка этого значения означает, что компонент устанавливается.
- `0`. Установка этого значения означает, что компонент не устанавливается.

[Tasks] – выбор задач для включения в список задач Kaspersky Endpoint Security. Если не указана ни одна задача, все задачи включаются в список задач Kaspersky Endpoint Security.

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

  Возможные значения параметров:

- `1`. Установка этого значения означает, что задача обновления включается в список задач Kaspersky Endpoint Security.
- `0`. Установка этого значения означает, что задача обновления не включается 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 производит сбор 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.

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

Завершение обновления до Kaspersky Endpoint Security 10 для Windows

Этот шаг доступен, если вы выполняете обновление одной из предыдущих версий программы (см. раздел «О способах обновления предыдущей версии программы» на стр. 39) до Kaspersky Endpoint Security 10 для Windows.

На этом шаге вам предлагается перезагрузить компьютер. Чтобы завершить обновление предыдущей версии программы и перейти к первоначальной настройке Kaspersky Endpoint Security 10 для Windows, нажмите на кнопку **Завершить**.

Активация программы

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. 51), 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 онлайн

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 файла 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 лицензированием, 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 вариант защиты компьютера (см. раздел «Организация защиты компьютера» на стр. 18), которая будет доступна после активации программы:

- **Базовая защита**. Если выбран этот вариант, то после активации программы будут доступны только компоненты защиты.
- **Стандартная защита**. Если выбран этот вариант, то после активации программы будут доступны компоненты защиты и контроля.
- **Расширенная защита**. Если выбран этот вариант, то после активации программы будут доступны все компоненты программы, включая функциональность шифрования данных.

Вариант защиты можно выбирать независимо от лицензии. Набор компонентов, соответствующий выбранному варианту защиты, будет установлен. Если приобретенная лицензия допускает меньший набор компонентов, то после активации программы недоступные по лицензии компоненты не будут работать.

По умолчанию выбрана базовая защита.

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..... 18

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 распространяется лицензия;
- 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 сбор 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 работы мастера 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 10 для Windows** и нажмите на кнопку **Завершить**.

Установка модуля шифрования

В состав установочного пакета Kaspersky Endpoint Security входит модуль шифрования. Модуль шифрования требуется устанавливать отдельно. Без установленного модуля шифрования функциональность шифрования данных программы недоступна.

Этот раздел содержит информацию о том, как установить модуль шифрования на компьютер.

В этом разделе

О способах установки модуля шифрования

Вы можете установить модуль шифрования как до, так и после установки Kaspersky Endpoint Security 10 для Windows.

Для установки модуля шифрования доступны те же способы, что и для установки Kaspersky Endpoint Security:

- *Локальная установка* – установка на отдельном компьютере. Для запуска и проведения локальной установки требуется непосредственный доступ к этому компьютеру. Локальная установка может быть проведена в одном из двух режимов:
  - *Интерактивном*, с помощью мастера установки модуля шифрования (см. раздел «Установка модуля шифрования с помощью мастера установки модуля шифрования» на стр. 37). Этот режим требует вашего участия в процессе установки.

- *Тихом*, запуск установки модуля шифрования в этом режиме выполняется из командной строки, ваше участие в процессе установки (см. раздел «Установка модуля шифрования из командной строки» на стр. 37) не требуется.

- *Удаленная установка* – установка модуля шифрования на компьютеры сети, выполняемая удаленно с рабочего места администратора с использованием:

  - программного комплекса Kaspersky Security Center (см. *Руководство по внедрению Kaspersky Security Center*);

  - редактора управления групповыми доменными политиками Microsoft Windows Server (см. раздел «Установка модуля шифрования через редактор управления групповыми доменными политиками Microsoft Windows Server» на стр. 37).

Установка модуля шифрования с помощью мастера установки модуля шифрования

Интерфейс мастера установки модуля шифрования состоит из последовательности окон (шагов). Чтобы переключаться между окнами мастера установки модуля шифрования, требуется использовать кнопки **Назад** и **Далее**. Работа мастера установки модуля шифрования завершается нажатием на кнопку **Завершить**. Чтобы прекратить работу мастера установки модуля шифрования на любом этапе, следует нажать на кнопку **Отмена**.

Чтобы установить модуль шифрования с помощью мастера установки модуля шифрования, выполните следующие действия:

1. Запустите файл xxx_encryption_module.msi. В качестве xxx может быть название алгоритма шифрования, на котором основана функциональность шифрования Kaspersky Endpoint Security.

   Запустится мастер установки модуля шифрования.

   Вы можете скачать исполняемый файл модуля шифрования на сайте «Лаборатории Касперского» или обратиться для его получения к партнерам, с помощью которых вы приобретали лицензию на использование программы.

2. Следуйте указаниям мастера установки модуля шифрования.

Установка модуля шифрования из командной строки

Чтобы запустить мастер установки модуля шифрования из командной строки,

введите в командной строке `msiexec /i <название установочного пакета>`.

Чтобы установить модуль шифрования в тихом режиме (без запуска мастера установки модуля шифрования),

введите в командной строке `msiexec /i <название установочного пакета> EULA=1 /qn`,

где `EULA=1` означает, что вы принимаете положения Лицензионного соглашения. Текст Лицензионного соглашения поставляется вместе с установочным пакетом модуля шифрования. Согласие с положениями Лицензионного соглашения является необходимым условием для установки модуля шифрования.

Установка модуля шифрования через редактор управления групповыми доменными политиками Microsoft Windows Server

С помощью редактора управления групповыми доменными политиками Microsoft Windows Server вы можете устанавливать модуль шифрования на рабочих станциях организации, входящих в состав домена, без использования Kaspersky Security Center.

Чтобы установить модуль шифрования через редактор управления групповыми доменными политиками Microsoft Windows Server, выполните следующие действия:

1. Создайте сетевую папку общего доступа на компьютере, являющемся контроллером домена.

2. Поместите дистрибутив модуля шифрования в формате MSI в сетевую папку общего доступа, созданную на предыдущем шаге инструкции.

3. Откройте редактор управления групповыми доменными политиками Microsoft Windows Server через консоль управления (MMC) (подробную информацию о работе с редактором управления групповыми доменными политиками Microsoft Windows Server читайте в *Справочной системе к Microsoft Windows Server*). Для этого выполните следующие действия:

   a. В меню **Пуск** выберите **Администрирование** → **Управление групповыми политиками**.

      Откроется окно Microsoft Windows **Управление групповыми политиками**.

   b. В дереве окна **Управление групповыми политиками** выберите нужный объект групповой политики Microsoft Windows Server.

   c. По правой клавише мыши вызовите контекстное меню объекта групповой политики Microsoft Windows Server и выберите пункт **Изменить**.

      Откроется редактор управления групповыми доменными политиками Microsoft Windows Server.

4. Создайте новый установочный пакет редактора управления групповыми доменными политиками Microsoft Windows Server. Для этого выполните следующие действия:

   a. В дереве консоли выберите **Объект групповой политики \ Конфигурация компьютера \ Политики \ Конфигурация программ \ Установка программного обеспечения**.

   b. По правой клавише мыши откройте контекстное меню узла **Установка программного обеспечения**.

   c. В контекстном меню выберите пункт **Создать** → **Пакет**.

      Откроется стандартное окно Microsoft Windows Server **Открыть**.

   d. В стандартном окне Microsoft Windows Server **Открыть** укажите путь к дистрибутиву модуля шифрования в формате MSI.

   e. В диалоговом окне **Развертывание программы** выберите параметр **Назначенный**.

   f. Нажмите на кнопку **ОК**.

Групповая доменная политика Microsoft Windows Server будет применена на каждой рабочей станции при следующей регистрации компьютеров в домене. В результате модуль шифрования будет установлен на все компьютеры в домене.

Обновление предыдущей версии программы

Этот раздел содержит информацию о том, как обновить предыдущую версию программы.

В этом разделе

О способах обновления предыдущей версии программы

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

- Антивирус Касперского 6.0 для Windows Workstations MP4.
- Антивирус Касперского 6.0 для Windows Servers MP4.
- Kaspersky Endpoint Security 8 для Windows.

Вы можете обновить предыдущую версию программы следующими способами:

- локально в интерактивном режиме с помощью мастера установки программы (см. раздел «Установка программы с помощью мастера установки программы» на стр. 23);
- локально в тихом режиме из командной строки (см. раздел «Установка программы из командной строки» на стр. 27);
- удаленно с помощью программного комплекса Kaspersky Security Center (информация приведена в *Руководстве по внедрению Kaspersky Security Center*);
- удаленно через редактор управления групповыми доменными политиками Microsoft Windows Server (см. раздел «Обновление предыдущей версии программы через редактор управления групповыми доменными политиками Microsoft Windows Server» на стр. 39).

Для обновления предыдущей версии программы до Kaspersky Endpoint Security 10 для Windows не нужно удалять предыдущую версию программы. Перед началом обновления предыдущей версии программы рекомендуется закрыть все работающие программы.

При обновлении любой из перечисленных выше программ до Kaspersky Endpoint Security 10 для Windows содержимое карантина и резервного хранилища не переносится.

Обновление предыдущей версии программы через редактор управления групповыми доменными политиками Microsoft Windows Server

С помощью редактора управления групповыми доменными политиками Microsoft Windows Server вы можете обновлять предыдущую версию Kaspersky Endpoint Security на рабочих станциях организации, входящих в состав домена, без использования Kaspersky Security Center.

➧ *Чтобы обновить предыдущую версию Kaspersky Endpoint Security через редактор управления групповыми доменными политиками Microsoft Windows Server, выполните следующие действия:*

1. Создайте сетевую папку общего доступа на компьютере, являющемся контроллером домена.
2. Поместите дистрибутив новой версии Kaspersky Endpoint Security в формате MSI в сетевую папку общего доступа, созданную на предыдущем шаге инструкции.

   Дополнительно в эту сетевую папку общего доступа можно поместить файл setup.ini (см. раздел «Описание параметров файла setup.ini» на стр. 30), содержащий перечень параметров установки Kaspersky Endpoint Security, конфигурационный файл install.cfg, а также файл ключа.

3. Откройте редактор управления групповыми доменными политиками Microsoft Windows Server через консоль управления (MMC) (подробную информацию о работе с редактором управления групповыми политиками читайте в *Справочной системе к Microsoft Windows Server*). Для этого выполните следующие действия:

   a. В меню **Пуск** выберите **Администрирование** → **Управление групповыми политиками**.

      Откроется окно Microsoft Windows **Управление групповыми политиками**.

   b. В дереве окна **Управление групповыми политиками** выберите нужный объект групповой политики.

   c. По правой клавише мыши вызовите контекстное меню объекта групповой политики и выберите пункт **Изменить**.

      Откроется редактор управления групповыми доменными политиками Microsoft Windows Server.

4. Создайте новый установочный пакет редактора управления групповыми доменными политиками Microsoft Windows Server. Для этого выполните следующие действия:

   a. В дереве консоли выберите **Объект групповой политики \ Конфигурация компьютера \ Политики \ Конфигурация программ \ Установка программного обеспечения**.

   b. По правой клавише мыши откройте контекстное меню узла **Установка программного обеспечения**.

   c. В контекстном меню выберите пункт **Создать** → **Пакет**.

      Откроется стандартное окно Microsoft Windows Server **Открыть**.

   d. В стандартном окне Microsoft Windows Server **Открыть** укажите путь к дистрибутиву новой версии Kaspersky Endpoint Security в формате MSI.

   e. В диалоговом окне **Развертывание программы** выберите параметр **Назначенный**.

   f. Нажмите на кнопку **ОК**.

5. В списке установочных пакетов редактора управления групповыми политиками доменными политиками Microsoft Windows Server выберите установочный пакет редактора управления групповыми доменными политиками Microsoft Windows Server, созданный на предыдущем шаге инструкции.

6. По правой клавише мыши откройте контекстное меню.

7. В контекстном меню выберите пункт **Свойства**.

   Откроется окно свойств установочного пакета редактора управления групповыми доменными политиками Microsoft Windows Server.

8. В окне свойств установочного пакета редактора управления групповыми доменными политиками Microsoft Windows Server выберите закладку **Обновления**.

9. На закладке **Обновления** добавьте установочный пакет редактора управления групповыми доменными политиками Microsoft Windows Server, который содержит дистрибутив предыдущей версии Kaspersky Endpoint Security.

10. Выберите вариант установки поверх существующего установочного пакета редактора управления групповыми доменными политиками Microsoft Windows Server, чтобы установить обновленную версию Kaspersky Endpoint Security с сохранением параметров предыдущей версии.

Групповая политика Microsoft Windows Server будет применена на каждой рабочей станции при следующей регистрации компьютеров в домене. В результате версия программы будет обновлена на всех компьютерах в домене.

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 10 для Windows компьютер и данные пользователя окажутся незащищенными.

Kaspersky Endpoint Security 10 для Windows может быть удален с компьютера несколькими способами:

- локально в интерактивном режиме с помощью мастера установки программы (см. раздел «Удаление программы с помощью мастера установки программы» на стр. 41);
- локально в тихом режиме из командной строки (см. раздел «Удаление программы из командной строки» на стр. 43);
- удаленно с помощью программного комплекса Kaspersky Security Center (информация приведена в *Руководстве по внедрению Kaspersky Security Center*);
- удаленно через редактор управления групповыми доменными политиками Microsoft Windows Server (см. раздел «Удаление программы через редактор управления групповыми доменными политиками Microsoft Windows Server» на стр. 43).

Удаление программы с помощью мастера установки программы

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

1. В меню **Пуск** выберите пункт **Программы → Kaspersky Endpoint Security для Windows → Изменение, восстановление или удаление**.

   Запустится мастер установки программы.

2. В окне мастера установки программы **Изменение, восстановление или удаление программы** нажмите на кнопку **Удаление**.

3. Следуйте указаниям мастера установки программы.

В этом разделе

Шаг 1. Сохранение данных программы для повторного использования

На этом шаге вам предлагается удалить программу полностью или сохранить объекты программы. Вы можете указать, какие используемые программой данные вы хотите сохранить для дальнейшего использования при повторной установке программы (например, ее более новой версии).

По умолчанию выбран вариант **Удалить программу полностью**. Параметры работы программы, информация об активации программы, объекты резервного хранилища и карантина в случае выбора этого варианта удаления программы будут удалены и недоступны пользователю.

Чтобы сохранить данные программы для повторного использования, выполните следующие действия:

1. Выберите вариант **Сохранить объекты программы**.
2. 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.
   - **Объекты резервного хранилища и карантина** – файлы, проверенные программой и помещенные в резервное хранилище и карантин.

     Доступ к объектам резервного хранилища и карантина, сохраненным после удаления программы, возможен только из той же версии программы, в которой они были сохранены.

     Если вы планируете использовать объекты резервного хранилища и карантина после удаления программы, вам нужно восстановить их из хранилищ до удаления программы. Однако, эксперты «Лаборатории Касперского» не рекомендуют восстанавливать объекты из резервного хранилища и карантина, 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.

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

Чтобы удалить программу из командной строки, выполните одно из следующих действий:

- Введите в командной строке `setup.exe /x` или

  `msiexec.exe /x {04CF7FBD-E56C-446D-8FC9-DD444BDBEE8E}` для удаления программы в интерактивном режиме.

  Запустится мастер установки программы. Следуйте указаниям мастера установки программы (см. раздел «Удаление программы с помощью мастера установки программы» на стр. 41).

- Введите в командной строке `setup.exe /s /x` или

  `msiexec.exe /x {04CF7FBD-E56C-446D-8FC9-DD444BDBEE8E} /qn` для удаления программы в тихом режиме (без запуска мастера установки программы).

Удаление программы через редактор управления групповыми доменными политиками Microsoft Windows Server

Чтобы удалить Kaspersky Endpoint Security через редактор управления групповыми доменными политиками Microsoft Windows Server, выполните следующие действия:

1. Откройте редактор управления групповыми доменными политиками Microsoft Windows Server через консоль управления (MMC) (подробную информацию о работе с редактором управления групповыми доменными политиками Microsoft Windows Server читайте в *Справочной системе к Microsoft Windows Server*). Для этого выполните следующие действия:

   a. В меню **Пуск** выберите **Администрирование** → **Управление групповыми политиками**.

      Откроется окно Microsoft Windows **Управление групповыми политиками**.

   b. В дереве окна **Управление групповыми политиками** выберите нужный объект групповой политики.

   c. По правой клавише мыши вызовите контекстное меню объекта групповой политики и выберите пункт **Изменить**.

      Откроется редактор управления групповыми доменными политиками Microsoft Windows Server.

2. В дереве консоли выберите **Объект групповой политики \ Конфигурация компьютера \ Политики \ Конфигурация программ \ Установка программного обеспечения**.

3. В списке установочных пакетов выберите установочный пакет Kaspersky Endpoint Security 10 для Windows.

4. По правой клавише мыши откройте контекстное меню установочного пакета и выберите пункт **Все задачи** → **Удалить**.

   Откроется окно **Удаление программ**.

5. В окне **Удаление программ** выберите параметр **Немедленное удаление этой программы с компьютеров всех пользователей**.

Групповая политика Microsoft Windows Server будет применена на каждой рабочей станции при следующей регистрации компьютеров в домене. В результате программы будет удалена на всех компьютерах в домене.

Удаление модуля шифрования

Чтобы удалить модуль шифрования, выполните следующие действия:

1. Откройте панель управления Windows.
2. Выберите пункт **Установка и удаление программ**.

   Откроется окно **Установка и удаление программ**.

3. В списке установленных программ выберите модуль шифрования.
4. Нажмите на кнопку **Удалить**.

ИНТЕРФЕЙС ПРОГРАММЫ

Этот раздел содержит информацию об основных элементах графического интерфейса программы: значке программы и контекстном меню значка программы, главном окне программы и окне настройки параметров 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. Он отражает состояние защиты компьютера, а также показывает действия, которые программа выполняет в текущий момент:

- Значок  означает, что работа всех компонентов защиты программы включена.
- Значок  означает, что Kaspersky Endpoint Security проверяет почтовое сообщение.
- Значок  означает, что Kaspersky Endpoint Security проверяет входящий или исходящий сетевой трафик.
- Значок  означает, что Kaspersky Endpoint Security обновляет базы и модули программы.
- 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(ов), повреждение баз программы.

По умолчанию включена анимация значка программы: например, если Kaspersky Endpoint Security проверяет почтовое сообщение, на фоне значка программы пульсирует миниатюрный значок письма, если Kaspersky Endpoint Security обновляет базы и модули программы, на фоне значка программы вращается значок глобуса.

Контекстное меню значка программы

Контекстное меню значка программы содержит следующие пункты:

- **Kaspersky Endpoint Security 10 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.

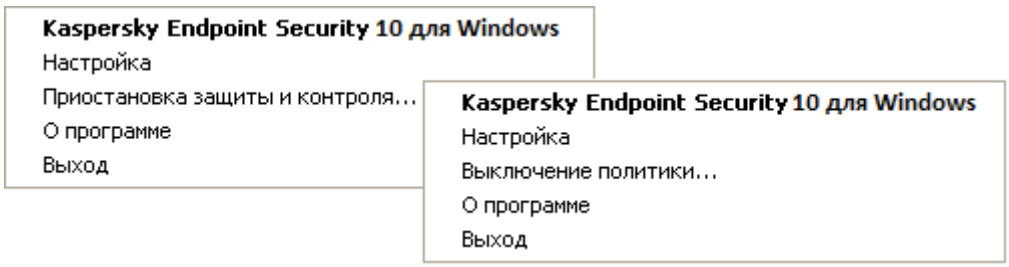

Рисунок 1. Контекстное меню значка программы

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 три части (см. рис. ниже):

- В верхней части окна расположены элементы интерфейса, с помощью которых вы можете просмотреть следующую информацию:
  - сведения о программе;
  - статистику репутационного сервиса KSN;
  - список необработанных файлов;
  - список найденных уязвимостей;
  - список файлов, помещенных на карантин;

- хранилище резервных 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 и задач программы. 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.

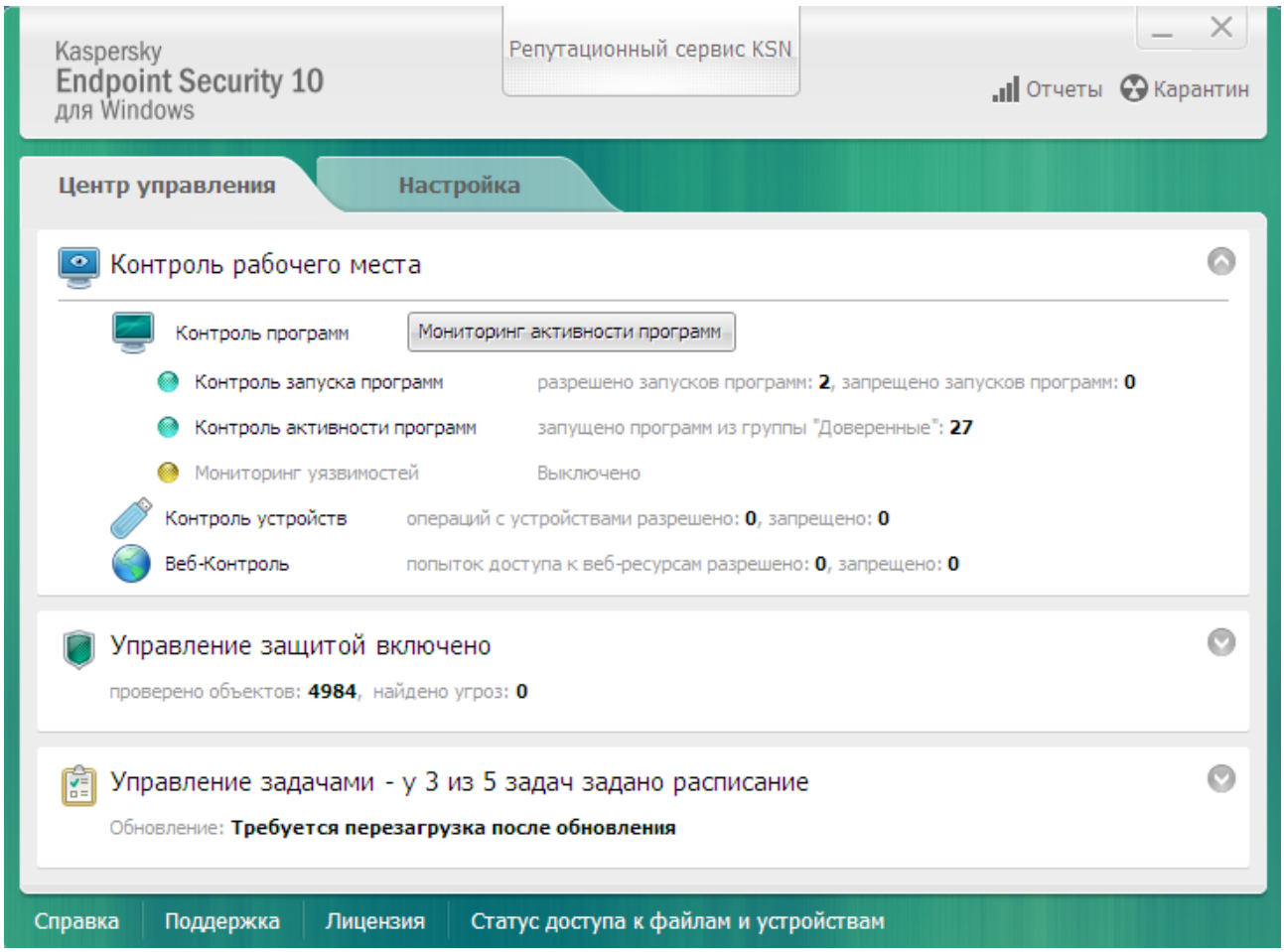

Рисунок 2. Главное окно программы

Вы можете воспользоваться следующими ссылками:

- **Справка**. По ссылке осуществляется переход к справочной системе Kaspersky Endpoint Security.
- **Поддержка**. По ссылке открывается окно **Поддержка** с информацией об операционной системе, текущей версии Kaspersky Endpoint Security и ссылками на информационные ресурсы «Лаборатории Касперского».
- **Лицензия**. По ссылке открывается окно **Лицензирование** с информацией о действующей лицензии.
- **Статус доступа к файлам и устройствам**. По ссылке открывается окно **Статус доступа к файлам и устройствам** с информацией об активных запросах доступа к файлам.

Открыть главное окно Kaspersky Endpoint Security можно одним из следующих способов:

- Наведением курсора на значок программы в области уведомлений панели задач Microsoft Windows и нажатием на левую клавишу мыши.
- Выбором пункта **Kaspersky Endpoint Security 10 для Windows** в контекстном меню значка программы (см. раздел «Контекстное меню значка программы» на стр. 46).

Окно настройки параметров программы

Окно настройки параметров Kaspersky Endpoint Security предназначено для настройки параметров работы программы в целом, отдельных ее компонентов, отчетов и хранилищ, задач проверки, задачи обновления и задачи поиска уязвимостей, а также для настройки обратной связи с Kaspersky Security Network.

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

- В левой части окна содержатся компоненты программы, задачи и другие составляющие, предназначенные для настройки.
- В правой части окна содержатся элементы управления, с помощью которых вы можете настроить работу составляющей, выбранной в левой части окна.

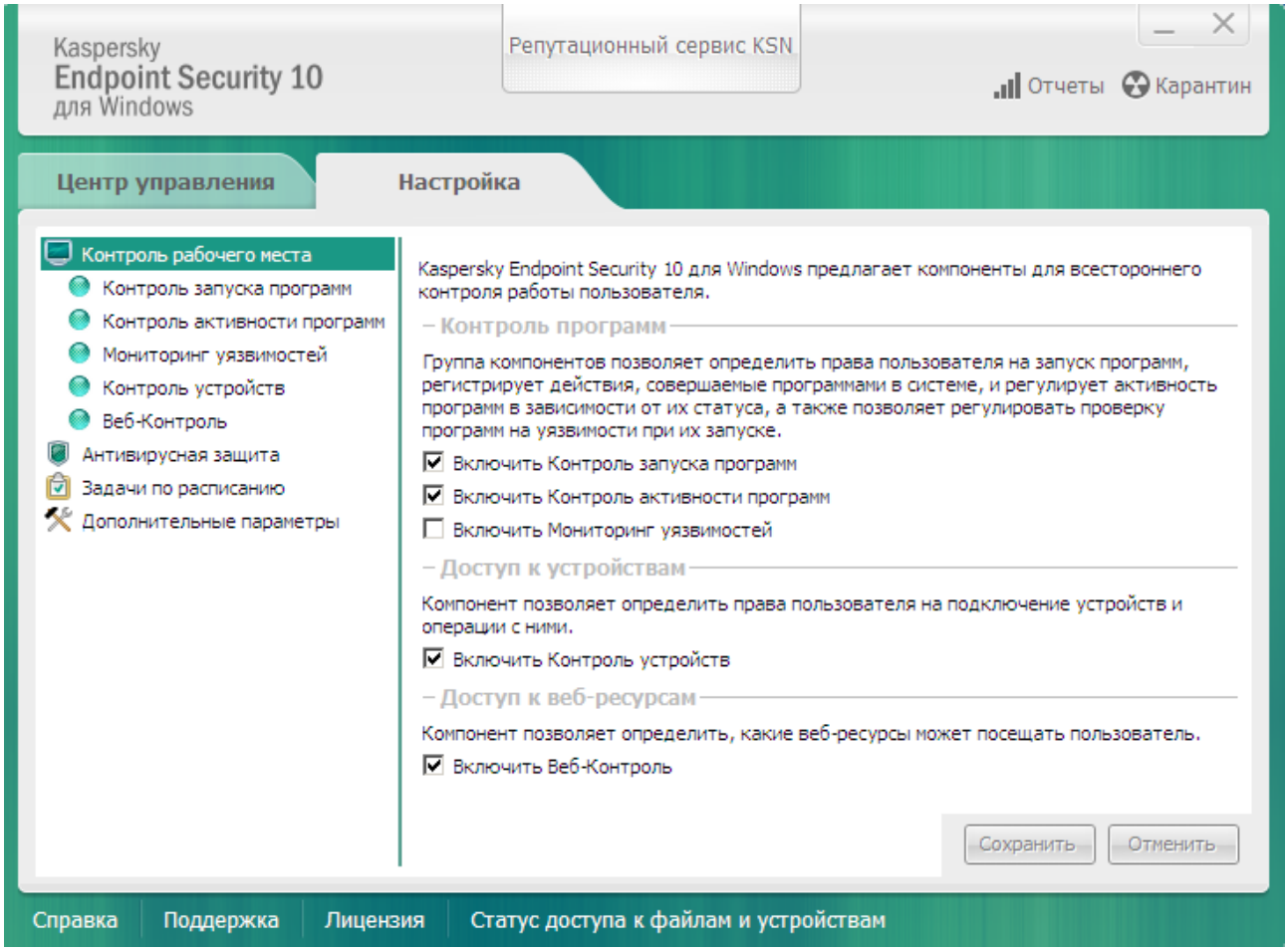

Рисунок 3. Окно настройки параметров программы

Как и в главном окне программы, вы можете воспользоваться следующими ссылками:

- **Справка**. По ссылке осуществляется переход к справочной системе Kaspersky Endpoint Security.

- **Поддержка**. По ссылке открывается окно **Поддержка** с информацией об операционной системе, текущей версии Kaspersky Endpoint Security и ссылками на информационные ресурсы «Лаборатории Касперского».

- **Лицензия**. По ссылке открывается окно **Лицензирование** с информацией о действующей лицензии.

- **Статус доступа к файлам и устройствам**. По ссылке открывается окно **Статус доступа к файлам и устройствам** с информацией об активных запросах доступа к файлам.

Открыть окно настройки параметров программы можно одним из следующих способов:

- Выбором закладки **Настройка** в главном окне программы (см. раздел «Главное окно программы» на стр. 46).

- Выбором пункта **Настройка** в контекстном меню значка программы (см. раздел «Контекстное меню значка программы» на стр. 46).

ЛИЦЕНЗИРОВАНИЕ ПРОГРАММЫ

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

В ЭТОМ РАЗДЕЛЕ

О Лицензионном соглашении

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

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

Вы можете ознакомиться с условиями Лицензионного соглашения следующими способами:

- Во время установки программы «Лаборатории Касперского» в интерактивном режиме (см. раздел «О способах установки программы» на стр. 22).
- Прочитав документ license.txt. Документ включен в комплект поставки программы (см. раздел «Комплект поставки» на стр. 17).

Считается, что 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. С лицензией связан уникальный код активации вашего экземпляра Kaspersky Endpoint Security.

Лицензия включает в себя право на получение следующих видов услуг:

- Использование программы на одном или нескольких компьютерах, в том числе обновление баз и предоставление новых версий программы.

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

- Обращение в Службу технической поддержки «Лаборатории Касперского» по вопросам, связанным с установкой, настройкой и использованием программы.

- Оповещение о выходе новых программ «Лаборатории Касперского», а также информацию о появлении новых вирусов и вирусных эпидемиях. Для использования этой услуги требуется подписаться на рассылку новостей ЗАО «Лаборатория Касперского» на веб-сайте Службы технической поддержки.

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

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. Для продолжения использования программы требуется приобрести коммерческую лицензию.

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

  По истечении срока действия коммерческой лицензии программа продолжает работу, но с ограниченной функциональностью. Вы можете использовать компоненты защиты и контроля и выполнять проверку на вирусы и другие программы, представляющие угрозу, на основе баз, установленных до даты окончания срока действия лицензии. Кроме того, программа шифрует изменяющиеся и зашифрованные до истечения срока действия лицензии файлы, но не шифрует новые файлы. Сервис Kaspersky Security Network недоступен.

  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 всех угроз компьютерной безопасности.

О коде активации

Код активации – это код, который вы получаете, приобретая коммерческую лицензию на Kaspersky Endpoint Security. Этот код требуется для активации программы.

Код активации представляет собой последовательность из двадцати цифр и латинских букв в формате xxxxx-xxxxx-xxxxx-xxxxx.

Если код активации был потерян или случайно удален после активации, то для его восстановления требуется отправить запрос в Службу технической поддержки «Лаборатории Касперского» (см. раздел «Обращение в Службу технической поддержки» на стр. 296).

О ФАЙЛЕ КЛЮЧА

Файл ключа – это файл вида xxxxxxxx.key. «Лаборатория Касперского» может предоставлять файл ключа при покупке Kaspersky Endpoint Security.

Если файл ключа был случайно удален, то для его восстановления вы можете выполнить следующие действия:

- отправить запрос в Службу технической поддержки (см. раздел «Обращение в Службу технической поддержки» на стр. 296);
- получить файл ключа на основе имеющегося кода активации на веб-сайте (https://activation.kaspersky.com/ru/).

Файл ключа содержит следующую информацию:

- Ключ – уникальная буквенно-цифровая последовательность. Ключ используется, например, для получения технической поддержки «Лаборатории Касперского».
- Ограничение на количество компьютеров – максимальное количество компьютеров, на которых вы можете активировать программу с помощью этого файла ключа.
- Дата создания файла ключа – дата создания файла ключа на сервере активации.
- Срок действия лицензии – срок использования программы, предусмотренный в Лицензионном соглашении и отсчитываемый с даты первой активации программы с помощью этого файла ключа. Например, 1 год.

  Срок действия лицензии истекает не позднее даты окончания срока годности файла ключа, с помощью которого по этой лицензии была активирована программа.

- Дата окончания срока годности файла ключа – активировать программу с помощью данного файла ключа можно только до даты окончания срока его годности.

О ПРЕДОСТАВЛЕНИИ ДАННЫХ

Принимая условия Лицензионного соглашения, вы соглашаетесь передавать в автоматическом режиме информацию о контрольных суммах обрабатываемых файлов (MD5) и информацию для определения репутации веб-адресов. Полученная информация не содержит персональных данных и иной конфиденциальной информации. «Лаборатория Касперского» защищает полученную информацию в соответствии с установленными законом требованиями. Вы можете получить более подробную информацию на веб-сайте http://support.kaspersky.ru.

О СПОСОБАХ АКТИВАЦИИ ПРОГРАММЫ

Активация – это процедура введения в действие лицензии на использование полнофункциональной версии программы.

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. 33).
- Локально из интерфейса программы с помощью мастера активации программы (см. раздел «Мастер активации программы» на стр. 54).

- Удаленно с помощью программного комплекса Kaspersky Security Center путем создания (см. раздел «Управление задачами» на стр. 283) и последующего запуска (см. раздел «Запуск, остановка, приостановка и возобновление выполнения задачи» на стр. 286) задачи добавления ключа.
- 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*).

Лицензирование

Этот раздел содержит информацию о действиях, которые вы можете выполнить в контексте лицензирования программы.

В этом разделе

Активация программы с помощью мастера активации программы

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

1. Запустите мастер активации программы (на стр. 54). Для этого выполните одно из следующих действий:
   - В окне уведомления Kaspersky Endpoint Security, появляющегося в области уведомлений панели задач, по ссылке **Подробнее** откройте окно **Лицензирование**. В окне **Лицензирование** нажмите на кнопку **Активировать программу по новой лицензии**.
   - По ссылке **Лицензия**, расположенной в нижней части главного окна программы, откройте окно **Лицензирование**. В окне **Лицензирование** нажмите на кнопку **Активировать программу по новой лицензии**.
2. Следуйте указаниям мастера активации программы (см. раздел «Мастер активации программы» на стр. 54).

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. 52).

Чтобы приобрести лицензию, выполните следующие действия:

1. Откройте главное окно программы (на стр. 46).
2. По ссылке **Лицензия**, расположенной в нижней части главного окна программы, откройте 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. 53) новый код активации программы или файл ключа.

2. Активируйте программу (см. раздел «О способах активации программы» на стр. 52) с помощью полученного кода активации или файла ключа.

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

Просмотр информации о лицензии

Чтобы просмотреть информацию о лицензии, выполните следующие действия:

1. Откройте главное окно программы (на стр. 46).

2. По ссылке **Лицензия**, расположенной в нижней части главного окна программы, откройте окно **Лицензирование**.

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

Мастер активации программы

Интерфейс мастера активации программы состоит из последовательности окон (шагов). Чтобы переключаться между окнами мастера активации программы, требуется использовать кнопки **Назад** и **Далее**. Чтобы завершить работу мастера активации программы, следует нажать на кнопку **Завершить**. Чтобы прекратить работу мастера активации программы на любом этапе, следует нажать на кнопку **Отмена**.

В этом разделе

Активация программы

На этом шаге предлагается выбрать 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. 51), 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.

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

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

Активация онлайн

Этот шаг доступен только при активации программы с помощью кода активации. Если вы выполняете 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 активации программы автоматически переходит к следующему шагу.
- Если код активации не проходит проверку, на экране появляется соответствующее уведомление. В этом случае вам следует обратиться за информацией в компанию, где вы получили код активации для Kaspersky Endpoint Security.
- Если допустимое число активаций с помощью кода активации превышено, на экране появляется соответствующее уведомление. Работа мастера активации программы прерывается, и программа предлагает вам обратиться в Службу технической поддержки «Лаборатории Касперского».

Чтобы вернуться к предыдущему шагу мастера активации программы, нажмите на кнопку **Назад**. Чтобы прекратить работу мастера активации 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 файла 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 лицензированием, при их наличии. Например, *Поврежден черный список ключей*.

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

Выбор активируемой функциональности

Этот шаг доступен только при активации пробной версии программы.

На этом шаге предлагается выбрать вариант защиты компьютера (см. раздел «Организация защиты компьютера» на стр. 18), которая будет доступна после активации программы:

- **Базовая защита**. Если выбран этот вариант, то после активации программы будут доступны только компоненты защиты.
- **Стандартная защита**. Если выбран этот вариант, то после активации программы будут доступны компоненты защиты и контроля.
- **Расширенная защита**. Если выбран этот вариант, то после активации программы будут доступны все компоненты программы, включая функциональность шифрования данных.

Вариант защиты можно выбирать независимо от лицензии. Набор компонентов, соответствующий выбранному варианту защиты, будет установлен. Если приобретенная лицензия допускает меньший набор компонентов, то после активации программы недоступные по лицензии компоненты не будут работать.

По умолчанию выбрана базовая защита.

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

Завершение активации программы

На этом шаге мастер активации 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 распространяется лицензия;
- дата окончания срока действия лицензии;
- функциональность программы, которая доступна по лицензии.

Чтобы завершить работу мастера активации программы, нажмите на кнопку **Завершить**.

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 Kaspersky Endpoint Security запускается автоматически после своей установки. В дальнейшем программа запускается автоматически после старта операционной системы.

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

1. Откройте окно настройки параметров программы (на стр. 48).
2. В левой части выберите блок **Антивирусная защита**.

   В правой части окна отобразятся параметры антивирусной защиты.
3. Выполните одно из следующих действий:
   - Установите флажок **Запускать Kaspersky Endpoint Security 10 для Windows при включении компьютера**, если вы хотите включить автоматический запуск программы.
   - Снимите флажок **Запускать Kaspersky Endpoint Security 10 для Windows при включении компьютера**, если вы хотите выключить автоматический запуск программы.

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 личных данных окажется под угрозой. Если требуется, вы можете приостановить защиту компьютера (см. раздел «Приостановка и возобновление защиты и контроля компьютера» на стр. 59) 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. 58).

Чтобы запустить программу вручную,

в меню **Пуск** выберите пункт **Программы** → **Kaspersky Endpoint Security 10 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 компонентов контроля Kaspersky Endpoint Security.

Индикатором работы программы служит значок программы в области уведомлений панели задач (см. раздел «Значок программы в области уведомлений» на стр. 45):

- Значок  свидетельствует о приостановке защиты и контроля компьютера.
- Значок  свидетельствует о возобновлении защиты и контроля компьютера.

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 или возобновить защиту и контроль компьютера, выполните следующие действия:

1. Если вы хотите приостановить защиту и контроль компьютера, выполните следующие действия:
   a. По правой клавише мыши откройте контекстное меню значка программы, который расположен в области уведомлений панели задач.
   b. В контекстном меню выберите пункт **Приостановка защиты и контроля**.

      Откроется окно **Приостановка защиты и контроля**.
   c. Выберите один из следующих вариантов:
      - **Приостановить на указанное время** – защита и контроль компьютера включатся через интервал времени, указанный в раскрывающемся списке ниже. Вы можете выбрать нужный интервал в раскрывающемся списке.
      - **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 ее.
2. Если вы хотите возобновить защиту и контроль компьютера, то вы можете это сделать в любой момент, независимо от того, какой был выбран вариант приостановки защиты и контроля компьютера. Чтобы возобновить защиту и контроль компьютера, выполните следующие действия:
   a. По правой клавише мыши откройте контекстное меню значка программы, который расположен в области уведомлений панели задач.
   b. В контекстном меню выберите пункт **Возобновление защиты и контроля**.

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 вашем компьютере и на всех присоединенных дисках на наличие в них вирусов и других программ, представляющих угрозу.

Файловый Антивирус использует методы сигнатурного и эвристического анализа, а также технологии iChecker и iSwift.

Когда пользователь или программа обращается к файлу, который находится в области защиты, Файловый Антивирус проверяет наличие информации об этом файле в базах iChecker и iSwift и на основании полученных сведений принимает решение о необходимости проверки файла.

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

1. Определяет тип обнаруженного в файле объекта (например, *вирус*, *троянская программа*).

2. Присваивает файлу статус *возможно зараженный*, если в результате проверки невозможно однозначно определить, заражен файл или нет. Возможно, в файле присутствует последовательность кода, свойственная вирусам и другим программам, представляющим угрозу, или модифицированный код известного вируса.

3. Выводит на экран уведомление (см. стр. 251) об обнаруженном в файле объекте (если это указано в параметрах уведомлений) и выполняет над файлом заданное в параметрах Файлового Антивируса действие (см. раздел «Изменение действия Файлового Антивируса над зараженными файлами» на стр. 64).

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. 46);
- из окна настройки параметров программы (см. раздел «Окно настройки параметров программы» на стр. 48).

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 блоке **Антивирусная защита** выберите раздел **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 компонента 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» (http://support.kaspersky.ru/helpdesk.html). 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 (на стр. 48).
2. В левой части окна в блоке **Антивирусная защита** выберите раздел **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. Далее нажмите на кнопку **ОК**.

   - 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. Далее нажмите на кнопку **ОК**.
7. В окне **Файловый Антивирус** нажмите на кнопку **ОК**.
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 файлов.

  Вы можете выбрать один из предустановленных уровней безопасности файлов или настроить параметры уровня безопасности файлов самостоятельно. После того как вы изменили параметры уровня безопасности файлов, вы всегда можете вернуться к рекомендуемым параметрам уровня безопасности файлов.

- 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 сигнатурный анализ. В процессе сигнатурного анализа Файловый Антивирус сравнивает найденный объект с записями в базах. В соответствии с рекомендациями специалистов «Лаборатории Касперского» 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 новые вредоносные объекты, записей о которых еще нет в базах.

- Выбрать технологии проверки.

  Вы 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.

- 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, что изменились с момента их предыдущего анализа. Такой режим проверки распространяется как на простые, так и на составные файлы.

- Настроить проверку составных файлов.

- Изменить режим проверки файлов.

В этом разделе

Изменение уровня безопасности файлов

Для защиты файловой системы компьютера Файловый Антивирус применяет разные наборы параметров. Такие наборы параметров называют *уровнями безопасности файлов*. Предустановленно три уровня безопасности файлов: **Высокий**, **Рекомендуемый**, **Низкий**. Параметры уровня безопасности файлов **Рекомендуемый** считаются оптимальными, они рекомендованы специалистами «Лаборатории Касперского».

Чтобы изменить уровень безопасности файлов, выполните следующие действия:

1. Откройте окно настройки параметров программы (на стр. 48).
2. В левой части окна в блоке **Антивирусная защита** выберите раздел **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 файлов (**Высокий**, **Рекомендуемый**, **Низкий**), выберите его при помощи ползунка.
   - Если вы хотите настроить уровень безопасности файлов самостоятельно, нажмите на кнопку **Настройка** и задайте параметры в открывшемся окне **Файловый Антивирус**.

     После того как вы самостоятельно настроили уровень безопасности файлов, название уровня безопасности файлов в блоке **Уровень безопасности** изменится на **Другой**.
   - Если вы хотите изменить уровень безопасности файлов 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 (на стр. 48).
2. В левой части окна в блоке **Антивирусная защита** выберите раздел **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 (на стр. 48).
2. В левой части окна в блоке **Антивирусная защита** выберите раздел **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** на закладке **Общие** 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.

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

   - Нажмите на кнопку **Добавить**, если вы хотите добавить новый объект в список проверяемых объектов.
   - Если вы хотите изменить местоположение объекта, выберите объект в списке проверяемых объектов и нажмите на кнопку **Изменить**.

   Откроется окно **Выбор объекта для 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.

6. Выполните одно из следующих действий:

   - Если вы хотите добавить новый объект или изменить местоположение объекта из списка проверяемых объектов, в окне **Выбор объекта для проверки** выберите объект и нажмите на кнопку **Добавить**.

     Все объекты, выбранные в окне **Выбор объекта для проверки**, отобразятся в списке **Область защиты** в окне **Файловый Антивирус**.

     Далее нажмите на кнопку **OK**.

   - Если вы хотите удалить объект, нажмите на кнопку **Да** в окне подтверждения удаления.

7. При необходимости повторите пункты 5-6 для добавления, изменения местоположения или удаления объектов из списка проверяемых объектов.

8. 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.

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

10. 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 (на стр. 48).

2. В левой части окна в блоке **Антивирусная защита** выберите раздел **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 детализации 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 (на стр. 48).

2. В левой части окна в блоке **Антивирусная защита** выберите раздел **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 (на стр. 48).

2. В левой части окна в блоке **Антивирусная защита** выберите раздел **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 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 круг проверяемых составных файлов, таким образом увеличив скорость проверки.

Чтобы настроить проверку составных файлов, выполните следующие действия:

1. Откройте окно настройки параметров программы (на стр. 48).

2. В левой части окна в блоке **Антивирусная защита** выберите раздел **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 вложенные OLE-объекты.

6. Если в блоке **Оптимизация проверки** снят флажок **Проверять только новые и измененные файлы**, для каждого типа составного файла вы можете выбрать, следует ли проверять все файлы этого типа или только новые. Для выбора нажмите на ссылку **все / новые**, расположенную рядом с названием типа составного файла. Ссылка меняет свое значение после нажатия на нее левой клавишей мыши.

   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 **Фоновая проверка** выполните одно из следующих действий:

   - Если вы не хотите, чтобы Файловый Антивирус распаковывал составные файлы в фоновом режиме, снимите флажок **Распаковывать составные файлы в фоновом режиме**.

   - Если вы хотите, чтобы Файловый Антивирус распаковывал составные файлы большого размера 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:

   - Если вы не хотите, чтобы Файловый Антивирус распаковывал составные файлы большого размера, установите флажок **Не распаковывать составные файлы большого размера** и в поле **Максимальный размер файла** укажите нужное значение.

   - Если вы хотите, чтобы Файловый Антивирус распаковывал 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 (на стр. 48).
2. В левой части окна в блоке **Антивирусная защита** выберите раздел **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.

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. 20).

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

В ЭТОМ РАЗДЕЛЕ

О Мониторинге системы

Мониторинг системы собирает 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 помещает исполняемый файл этой программы на карантин (см. раздел «Работа с карантином и резервным хранилищем» на стр. 254).

Откат действий, произведенных вредоносными программами

На основе информации, собранной 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 проактивной защитой, Файловым Антивирусом (см. стр. 60), а также во время проверки на вирусы (см. раздел «Проверка компьютера» на стр. 220).

Откат действий вредоносной программы затрагивает строго ограниченный набор данных. Это 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 рекомендованном специалистами «Лаборатории Касперского» режиме. Вы можете выключить Мониторинг системы при необходимости.

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

Включить и выключить компонент можно двумя способами:

- на закладке **Центр управления** главного окна программы (см. раздел «Главное окно программы» на стр. 46);
- из окна настройки параметров программы (см. раздел «Окно настройки параметров программы» на стр. 48).

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 (на стр. 48).
2. В левой части окна в блоке **Антивирусная защита** выберите раздел **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.

Использование шаблонов опасного поведения программ

Чтобы использовать шаблоны опасного поведения программ, выполните следующие действия:

1. Откройте окно настройки параметров программы (на стр. 48).
2. В левой части окна в блоке **Антивирусная защита** выберите раздел **Мониторинг системы**.

   В правой части окна отобразятся параметры компонента **Мониторинг системы**.
3. В блоке **Проактивная защита** установите флажок **Использовать обновляемые шаблоны опасного поведения (BSS)**.
4. В раскрывающемся списке **При обнаружении вредоносной активности программы** выберите нужное действие:

   - **Выбирать действие автоматически**. Если выбран этот элемент, то, обнаружив вредоносную активность программы, Kaspersky Endpoint Security выполняет действие, установленное специалистами «Лаборатории Касперского» по умолчанию. По умолчанию Kaspersky Endpoint Security помещает исполняемый файл вредоносной программы на карантин.
   - **Помещать файл на карантин**. Если выбран этот элемент, то, обнаружив вредоносную активность программы, Kaspersky Endpoint Security помещает исполняемый файл этой программы на карантин.
   - **Завершать работу вредоносной программы**. Если выбран этот элемент, то, обнаружив вредоносную активность программы, Kaspersky Endpoint Security завершает работу программы.
   - **Пропускать**. Если выбран этот элемент, то, обнаружив вредоносную активность программы, Kaspersky Endpoint Security не выполняет действий над исполняемым файлом этой программы.
5. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Откат действий вредоносных программ при лечении

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

1. Откройте окно настройки параметров программы (на стр. 48).
2. В левой части окна в блоке **Антивирусная защита** выберите раздел **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.

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. 20).

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 почтовые сообщения 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 почтовые сообщения, получаемые или отправляемые по протоколам POP3, SMTP, IMAP, MAPI и NNTP.

Почтовый Антивирус перехватывает и проверяет каждое почтовое сообщение, принимаемое или отправляемое пользователем. Если угрозы в почтовом сообщении не обнаружены, оно становится доступным для пользователя.

При обнаружении угрозы в почтовом сообщении Почтовый Антивирус выполняет следующие действия:

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

2. Присваивает почтовому сообщению статус *возможно зараженный*, если в результате проверки невозможно однозначно определить, заражено почтовое сообщение или нет. Возможно, в почтовом сообщении присутствует последовательность кода, свойственная вирусам и другим программам, представляющим угрозу, или модифицированный код известного вируса.

После этого программа блокирует почтовое сообщение, выводит на экран уведомление (см. стр. 251) (если это указано в параметрах уведомлений) об обнаруженном объекте и выполняет заданное в параметрах Почтового Антивируса действие (см. раздел «Изменение действия над зараженными почтовыми сообщениями» на стр. 76).

Компонент взаимодействует с почтовыми программами, установленными на компьютере. Для почтовых программ Microsoft Office Outlook® и The Bat! предусмотрены встраиваемые модули расширения (далее также «плагины»), позволяющие производить более тонкую настройку параметров проверки почтовых сообщений. Плагин Почтового Антивируса встраивается в почтовые программы Microsoft Office Outlook и The Bat! во время установки Kaspersky Endpoint Security.

Индикатором работы Почтового Антивируса служит значок 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. 46);
- из окна настройки параметров программы (см. раздел «Окно настройки параметров программы» на стр. 48).

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 блоке Антивирусная защита выберите раздел **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 почтовыми сообщениями.

- Сформировать область защиты Почтового Антивируса.

- Настроить проверку вложенных в почтовые сообщения составных файлов.

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

- Настроить фильтрацию по типу вложений в почтовых сообщениях.

  Фильтрация по типу вложений в почтовых 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 почтовых сообщениях новые угрозы, записей о которых еще нет в базах Kaspersky Endpoint Security.

- Настроить параметры проверки почты в программе Microsoft Office Outlook.

  Для почтовой программы Microsoft Office Outlook предусмотрен встраиваемый плагин, позволяющий удобно настраивать параметры проверки почты.

- Настроить параметры проверки почты в программе The Bat!.

  Для почтовой программы The Bat! предусмотрен встраиваемый плагин, позволяющий удобно настраивать параметры проверки почты.

  Работая с остальными почтовыми программами (в том числе с Microsoft Outlook Express®, Windows Mail и Mozilla™ Thunderbird™), Почтовый Антивирус проверяет почту на трафике по протоколам SMTP, POP3, IMAP и NNTP.

  Работая с почтовой программой Mozilla Thunderbird, Почтовый Антивирус не проверяет на вирусы и другие программы, представляющие угрозу, почтовые сообщения, передаваемые по протоколу IMAP в случае, если используются фильтры, перемещающие почтовые 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*. Предустановленно 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 (на стр. 48).
2. В левой части окна в блоке **Антивирусная защита** выберите раздел **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 почтовыми сообщениями

Чтобы изменить действие над зараженными почтовыми сообщениями, выполните следующие действия:

1. Откройте окно настройки параметров программы (на стр. 48).

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

Под областью защиты подразумеваются 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 программы, тип почтовых сообщений и почтовые протоколы, трафик которых проверяет Почтовый Антивирус. По умолчанию Kaspersky Endpoint Security проверяет как входящие, так и исходящие почтовые сообщения, трафик почтовых протоколов POP3, SMTP, NNTP и IMAP, а также интегрируется в почтовые программы Microsoft Office Outlook и The Bat!.

Чтобы сформировать область защиты Почтового Антивируса, выполните следующие действия:

1. Откройте окно настройки параметров программы (на стр. 48).

2. В левой части окна в блоке **Антивирусная защита** выберите раздел **Почтовый Антивирус**.

   В правой части окна отобразятся параметры компонента Почтовый Антивирус.

3. Нажмите на кнопку **Настройка**.

   Откроется закладка **Общие** окна **Почтовый Антивирус**.

4. 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 почтовые сообщения на вашем компьютере.
   - Выберите вариант **Только входящие сообщения**, если вы хотите, чтобы Почтовый Антивирус проверял только входящие почтовые сообщения на вашем компьютере.

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

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

   - Установите флажок **Трафик POP3 / SMTP / NNTP / IMAP**, если вы хотите, чтобы Почтовый Антивирус проверял почтовые 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 почтовые сообщения, передающиеся по протоколам POP3, SMTP, NNTP и IMAP, до их получения на компьютере пользователя. В этом случае почтовые сообщения проверяют плагины Почтового Антивируса, встроенные в почтовые программы Microsoft Office Outlook и The Bat!, после их получения на компьютере пользователя.

Если вы используете почтовую программу, отличную от Microsoft Office Outlook и The Bat!, то при снятом флажке **Трафик POP3 / SMTP / NNTP / IMAP** почтовые сообщения, передающиеся по почтовым протоколам POP3, SMTP, NNTP и IMAP, Почтовый Антивирус не проверяет.

Если флажки **Дополнительно: плагин в Microsoft Office Outlook** и **Дополнительно: плагин в The Bat!** сняты, то Почтовый Антивирус также не проверяет почтовые сообщения, передающиеся по почтовым протоколам POP3, SMTP, NNTP и IMAP.

- Установите флажок **Дополнительно: плагин в Microsoft Office Outlook**, если вы хотите открыть доступ к настройке параметров Почтового Антивируса из программы Microsoft Office Outlook и включить проверку почтовых сообщений, передающихся по протоколам POP3, SMTP, NNTP, IMAP и MAPI, после их получения на компьютере пользователя на стороне плагина, интегрированного в программу Microsoft Office Outlook.

  Снимите флажок **Дополнительно: плагин в Microsoft Office Outlook**, если вы хотите закрыть доступ к настройке параметров Почтового Антивируса из программы Microsoft Office Outlook и выключить проверку почтовых сообщений, передающихся по протоколам POP3, SMTP, NNTP, IMAP и MAPI, после их получения на компьютере пользователя на стороне плагина, интегрированного в программу Microsoft Office Outlook.

- Установите флажок **Дополнительно: плагин в The Bat!**, если вы хотите включить проверку почтовых сообщений, передающихся по протоколам POP3, SMTP, NNTP, IMAP и MAPI, после их получения на компьютере пользователя на стороне плагина, интегрированного в программу The Bat!.

  Снимите флажок **Дополнительно: плагин в The Bat!**, если вы хотите выключить проверку почтовых сообщений, передающихся по протоколам POP3, SMTP, NNTP, IMAP и MAPI, после их получения на компьютере пользователя на стороне плагина, интегрированного в программу The Bat!.

Плагин Почтового Антивируса встраивается в почтовые программы Microsoft Office Outlook и The Bat! во время установки Kaspersky Endpoint Security.

6. Нажмите на кнопку **OK**.

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

Проверка вложенных в почтовые сообщения составных файлов

Чтобы настроить проверку вложенных в почтовые сообщения составных файлов, выполните следующие действия:

1. Откройте окно настройки параметров программы (на стр. 48).

2. В левой части окна в блоке **Антивирусная защита** выберите раздел **Почтовый Антивирус**.

   В правой части окна отобразятся параметры компонента Почтовый Антивирус.

3. Нажмите на кнопку **Настройка**.

   Откроется окно **Почтовый Антивирус**.

4. На закладке **Общие** в блоке **Проверка составных файлов** выполните следующие действия:

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

   - Установите флажок **Не проверять архивы размером более N МБ**, если вы хотите, чтобы Почтовый Антивирус не проверял вложенные в почтовые 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 вложенные архивы более N с**, если вы хотите, чтобы Почтовый Антивирус проверял вложенные в почтовые сообщения архивы, если на их проверку затрачивается более N секунд.

5. Нажмите на кнопку **ОК**.

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

Фильтрация вложений в почтовых сообщениях

Вредоносные программы могут распространяться через почту в виде вложений в почтовых сообщениях. Вы можете настроить фильтрацию по типу вложений в почтовых сообщениях, которая позволяет автоматически переименовывать или удалять файлы указанных типов.

Чтобы настроить фильтрацию вложений, выполните следующие действия:

1. Откройте окно настройки параметров программы (на стр. 48).

2. В левой части окна в блоке **Антивирусная защита** выберите раздел **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 параметр **Не применять фильтр**, если вы хотите, чтобы Почтовый Антивирус не фильтровал вложения в почтовые сообщения.

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

   - Выберите параметр **Удалять вложения указанных типов**, если вы хотите, чтобы Почтовый Антивирус удалял вложенные в почтовые сообщения файлы указанных типов.

6. Выполните одно из следующих действий:

   - Если в пункте 5 инструкции вы выбрали параметр **Не применять фильтр**, перейдите к пункту 7 инструкции.

   - Если в пункте 5 инструкции вы выбрали параметр **Переименовать вложения указанных типов** или параметр **Удалять вложения указанных типов**, становится активным список типов файлов. 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.

Использование эвристического анализа

Чтобы использовать эвристический анализ, выполните следующие действия:

1. Откройте окно настройки параметров программы (на стр. 48).
2. В левой части окна в блоке **Антивирусная защита** выберите раздел **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 **Дополнительно**.
5. На закладке **Дополнительно** в блоке **Методы проверки** установите флажок **Эвристический анализ**.
6. При помощи ползунка задайте уровень детализации проверки во время использования эвристического анализа: **поверхностный**, **средний** или **глубокий**.
7. Нажмите на кнопку **OK**.
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 встраивается специальный плагин. Он позволяет быстро перейти к настройке параметров Почтового Антивируса из программы Microsoft Office Outlook, а также указать, в какой момент проверять почтовые сообщения на присутствие вирусов и других программ, представляющих угрозу. Почтовый плагин программы Microsoft Office Outlook может проверять входящие и исходящие почтовые сообщения, переданные по протоколам POP3, SMTP, NNTP, IMAP и MAPI.

Настройка параметров Почтового Антивируса из программы Microsoft Office Outlook доступна в том случае, если в интерфейсе программы Kaspersky Endpoint Security установлен флажок **Дополнительно: плагин в Microsoft Office Outlook**.

В программе Microsoft Office Outlook входящие почтовые сообщения сначала проверяет Почтовый Антивирус (если установлен флажок **Трафик POP3 / SMTP / NNTP / IMAP**), затем почтовый плагин программы Microsoft Office Outlook. Если Почтовый Антивирус обнаруживает в почтовом сообщении вредоносный объект, он уведомляет вас об этом.

От выбора действия в окне уведомления зависит, кто устраняет угрозу в почтовом сообщении: Почтовый Антивирус или почтовый плагин программы Microsoft Office Outlook:

- Если в окне уведомления Почтового Антивируса пользователь выбирает действие **Лечить** или **Удалить**, то действие по устранению угрозы выполняет Почтовый Антивирус.
- Если в окне уведомления Почтового Антивируса пользователь выбирает действие **Пропустить**, то действие по устранению угрозы выполняет почтовый плагин программы Microsoft Office Outlook.

Исходящие почтовые сообщения сначала проверяет почтовый плагин программы Microsoft Office Outlook, а затем Почтовый Антивирус.

Чтобы перейти к настройке параметров проверки почты в программе Microsoft Office Outlook, выполните следующие действия:

1. Откройте главное окно Microsoft Office Outlook.

2. В меню программы выберите пункт **Сервис** → **Параметры**.

   Откроется окно **Параметры**.

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

См. также

Формирование области защиты Почтового Антивируса 77

Проверка почты в The Bat!

Во время установки Kaspersky Endpoint Security в программу The Bat! встраивается специальный плагин. Он позволяет быстро перейти к настройке параметров Почтового Антивируса из программы The Bat!, а также указать, в какой момент проверять почтовые сообщения на присутствие вирусов и других программ, представляющих угрозу. Почтовый плагин программы The Bat! может проверять входящие и исходящие почтовые сообщения, переданные по протоколам POP3, SMTP, NNTP, IMAP и MAPI.

Настройка параметров Почтового Антивируса из программы The Bat! доступна в том случае, если в интерфейсе программы Kaspersky Endpoint Security установлен флажок **Дополнительно: плагин в The Bat!**.

В программе The Bat! входящие почтовые сообщения сначала проверяет Почтовый Антивирус (если в интерфейсе программы Kaspersky Endpoint Security установлен флажок **Трафик POP3 / SMTP / NNTP / IMAP**), затем входящие почтовые сообщения проверяет почтовый плагин программы The Bat!. Если Почтовый Антивирус обнаруживает в почтовом сообщении вредоносный объект, он уведомляет вас об этом.

От выбора действия в окне уведомления зависит, кто устраняет угрозу в почтовом сообщении: Почтовый Антивирус или почтовый плагин программы The Bat!:

- 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 почтовый плагин программы The Bat!.

Исходящие почтовые сообщения сначала проверяет почтовый плагин программы The Bat!, а затем проверяет Почтовый Антивирус.

В программе The Bat! действия над зараженными почтовыми сообщениями определяются средствами программы The Bat!. Вы можете задать следующие параметры:

- выбрать поток почтовых сообщений (входящий, исходящий), который следует проверять;

- определить момент, когда нужно проверять почтовые сообщения (перед открытием почтового сообщения, перед сохранением почтового сообщения на диск);

- выбрать действие, которое выполняет программа The Bat!, обнаружив зараженные почтовые сообщения:

  - **Попробовать излечить зараженные части**. Если вы выбрали этот вариант, программа The Bat! пытается вылечить зараженные почтовые сообщения. Если их вылечить не удается, программа The Bat! оставляет почтовые сообщения в неизменном виде.

  - **Удалить зараженные части**. Если вы выбрали этот вариант, программа The Bat! удаляет зараженные или возможно зараженные почтовые сообщения.

  По умолчанию программа The Bat! помещает все зараженные почтовые сообщения на карантин без лечения.

Программа The Bat! не отмечает специальным заголовком зараженные почтовые сообщения.

Чтобы перейти к настройке параметров проверки почты в программе The Bat!, выполните следующие действия:

1. Откройте главное окно программы The Bat!.
2. В меню **Свойства** выберите пункт **Настройка**.
3. В дереве настройки выберите объект **Защита от вирусов**.

См. также

Формирование области защиты Почтового Антивируса 77

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. 20).

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 (см. раздел «Изменение действия над вредоносными объектами веб-трафика» на стр. 86).

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. 46);
- из окна настройки параметров программы (см. раздел «Окно настройки параметров программы» на стр. 48).

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 блоке **Антивирусная защита** выберите раздел **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 новые 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*. Предустановленно 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 (на стр. 48).

2. В левой части окна в блоке **Антивирусная защита** выберите раздел **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 (на стр. 48).

2. В левой части окна в блоке **Антивирусная защита** выберите раздел **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 *фишинг-атак*. Частным примером фишинг-атаки 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 (на стр. 48).
2. В левой части окна в блоке **Антивирусная защита** выберите раздел **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. 293).
6. Нажмите на кнопку **ОК**.
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 (на стр. 48).
2. В левой части окна в блоке **Антивирусная защита** выберите раздел **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. В окне **Веб-Антивирус** выберите закладку **Общие**.
5. Выполните следующие действия:

   - 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 детализации эвристического анализа: **поверхностный**, **средний** или **глубокий**.
   - 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** и при помощи ползунка задайте уровень детализации эвристического анализа: **поверхностный**, **средний** или **глубокий**.

6. Нажмите на кнопку **OK**.

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

Настройка продолжительности кеширования веб-трафика

Чтобы повысить эффективность обнаружения вредоносного кода, Веб-Антивирус применяет кеширование фрагментов объектов, поступающих из интернета. Используя кеширование, Веб-Антивирус проверяет объекты только после того, как они полностью получены на компьютер.

Кеширование увеличивает продолжительность обработки объектов и передачи их пользователю для работы. Кроме того, кеширование может вызывать проблемы при загрузке и обработке больших объектов, связанные с истечением тайм-аута на соединение HTTP-клиента.

Для решения этой проблемы предусмотрена возможность ограничивать продолжительность кеширования фрагментов объектов, поступающих из интернета. По истечении определенного времени каждая полученная часть объекта передается пользователю непроверенной, а по завершении копирования объект проверяется целиком. Это позволяет уменьшить продолжительность передачи объектов пользователю и решить проблему разрыва соединения. Уровень безопасности работы в интернете при этом не снижается.

Снятие ограничения на продолжительность кеширования веб-трафика приводит к повышению эффективности антивирусной проверки, но одновременно предполагает замедление доступа к объектам.

Чтобы настроить продолжительность кеширования веб-трафика, выполните следующие действия:

1. Откройте окно настройки параметров программы (на стр. 48).

2. В левой части окна в блоке **Антивирусная защита** выберите раздел **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. В блоке **Действия** выполните одно из следующих действий:

   - Установите флажок **Ограничивать продолжительность кеширования веб-трафика**, если вы хотите ограничить продолжительность кеширования веб-трафика и ускорить его проверку.

   - Снимите флажок **Ограничивать продолжительность кеширования веб-трафика**, если вы хотите отменить ограничение на продолжительность кеширования веб-трафика.

6. Нажмите на кнопку **OK**.

7. 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 (на стр. 48).

2. В левой части окна в блоке **Антивирусная защита** выберите раздел **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 этого выполните следующие действия:

   a. Нажмите на кнопку **Добавить**.

      Откроется окно **Адрес / Маска 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.

   d. Повторите пункты a-c инструкции, если это требуется.

7. Нажмите на кнопку **OK**.

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

ЗАЩИТА ТРАФИКА ИНТЕРНЕТ-ПЕЙДЖЕРОВ. 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. 20).

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 *интернет-пейджерами*).

Сообщения, переданные через интернет-пейджеры, 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 фишинг-атак.

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

Через интернет-пейджеры можно передавать файлы. Во время попытки сохранения этих файлов их проверяет компонент Файловый Антивирус (см. раздел «О Файловом Антивирусе» на стр. 60).

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

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

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 «Окно настройки параметров программы» на стр. 48).

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 (на стр. 48).
2. В левой части окна в блоке **Антивирусная защита** выберите раздел **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:

- Сформировать область защиты.

  Вы можете расширить или сузить область защиты, изменив тип проверяемых сообщений, поступающих через интернет-пейджеры.

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

- Настроить использование эвристического анализа на наличие исходного кода вирусов в сообщениях интернет-пейджеров.

  Чтобы повысить эффективность защиты, вы можете использовать эвристический анализ. Эвристический анализ позволяет обнаруживать в сообщениях интернет-пейджеров исходный код вирусов.

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 интернет-пейджеры. 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 (на стр. 48).
2. В левой части окна в блоке **Антивирусная защита** выберите раздел **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 интернет-пейджеров.

   - Выберите вариант **Только входящие сообщения**, если вы хотите, чтобы IM-Антивирус проверял только входящие сообщения интернет-пейджеров.
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 (на стр. 48).
2. В левой части окна в блоке **Антивирусная защита** выберите раздел **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 интернет-пейджеров на их принадлежность к базе вредоносных веб-адресов.
   - Установите флажок **Проверять ссылки по базе фишинговых веб-адресов**, если вы хотите проверять ссылки в сообщениях интернет-пейджеров на их принадлежность к базе фишинговых веб-адресов.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Использование эвристического анализа в работе IM-Антивируса

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

1. Откройте окно настройки параметров программы (на стр. 48).
2. В левой части окна в блоке **Антивирусная защита** выберите раздел **IM-Антивирус**.

   В правой части окна отобразятся параметры компонента IM-Антивирус.
3. В блоке **Методы проверки** выполните следующие действия:

   a. Установите флажок **Эвристический анализ**.

   b. При помощи ползунка задайте уровень детализации эвристического анализа: **поверхностный**, **средний** или **глубокий**.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

ЗАЩИТА СЕТИ

Этот раздел содержит информацию о принципах работы и настройке компонентов Сетевой экран и Защита сети, а также о контроле сетевого трафика.

В ЭТОМ РАЗДЕЛЕ

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 личных данных, хранящихся на компьютере пользователя, блокируя все возможные для операционной системы угрозы в то время, когда компьютер подсоединен к сети Интернет 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. 96). 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. 46);
- из окна настройки параметров программы (см. раздел «Окно настройки параметров программы» на стр. 48).

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 (на стр. 48).
2. В левой части окна в блоке **Антивирусная защита** выберите раздел **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 (на стр. 48).
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 **Доступные сети**.

   Откроется окно **Сетевой экран** на закладке **Сети**.
4. На закладке **Сети** выберите сетевое соединение, статус которого вы хотите изменить.
5. По правой клавише мыши откройте контекстное меню сетевого соединения.
6. В контекстном меню выберите статус сетевого соединения (см. раздел «О статусах сетевого соединения» на стр. 96):
   - **Публичная сеть**.
   - **Локальная сеть**.
   - **Доверенная сеть**.
7. Нажмите на кнопку **ОК** в окне **Сетевой экран**.
8. 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 (на стр. 48).
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 пакетные правила**.

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

   На этой закладке представлен список сетевых пакетных правил, установленных Сетевым экраном по умолчанию.
4. 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**.
5. 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 имя сетевого сервиса одним из следующих способов:

   - Нажмите на значок , расположенный справа от поля **Название**, и в раскрывающемся списке выберите имя сетевого сервиса.

     В состав Kaspersky Endpoint Security включены сетевые сервисы, описывающие наиболее часто используемые сетевые соединения.

   - В поле **Название** введите имя сетевого сервиса вручную.

   Сетевой сервис – это набор параметров, характеризующих сетевую активность, для которой вы создаете сетевое правило.

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.

      По умолчанию флажок **Протокол** снят.

      Если сетевой сервис выбран из раскрывающегося списка **Название**, то флажок **Протокол** устанавливается автоматически и раскрывающийся список рядом с флажком заполняется типом протокола, который соответствует выбранному сетевому сервису.

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

   Сетевой экран контролирует сетевые соединения со следующими направлениями:

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

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 задать порты компьютера пользователя и удаленного компьютера, соединение между которыми контролируется:

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

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

12. Если требуется, в поле **Адрес** укажите сетевой адрес.

    В качестве сетевого адреса вы можете использовать IP-адрес или указать статус сетевого соединения. В последнем случае сетевые адреса берутся из всех активных сетевых соединений, имеющих выбранный статус.

Вы можете выбрать одну из следующих категорий сетевых адресов:

- **Любой адрес**.
- **Адреса подсети**.
- **Адреса из списка**.

13. Установите флажок **Записать в отчет**, если вы хотите, чтобы действие сетевого правила было отражено в отчете (см. раздел «Работа с отчетами» на стр. 245).
14. 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.
15. Нажмите на кнопку **ОК** в окне **Сетевой экран**.
16. 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 (на стр. 48).
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 пакетные правила**.

   Откроется окно **Сетевой экран** на закладке **Сетевые пакетные правила**.
4. В списке сетевых пакетных правил выберите нужное вам 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**.

   Окно **Сетевой экран** закроется.
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 (на стр. 48).

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 пакетные правила**.

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

4. В списке сетевых пакетных правил выберите 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**.

   Окно **Сетевой экран** закроется.

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 (на стр. 48).

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 пакетные правила**.

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

4. В списке сетевых пакетных правил выберите 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. Окно **Сетевой экран** закроется.

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

Работа с сетевыми правилами группы 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 уровня опасности, 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,
  - индекс опасности программ меньше 50,
  - 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,
  - индекс опасности программ находится в диапазоне 51-71,
  - 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,
  - индекс опасности программ находится в диапазоне 71-100,
  - пользователь поместил программы в группу «Недоверенные».

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

Как и компонент Контроль активности программ (на стр. 135), 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 можете выполнить следующие действия в процессе работы с сетевыми правилами группы программ:

- Создать новое сетевое правило группы программ.

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

- Включить и выключить сетевое правило группы программ.

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

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

- Изменить параметры сетевого правила группы программ.

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

- Изменить действие Сетевого экрана для сетевого правила группы программ.

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

- Изменить приоритет сетевого правила группы программ.

  Вы можете повысить или понизить приоритет созданного вручную сетевого правила группы программ.

- Удалить сетевое правило группы программ.

  Вы можете удалить созданное вручную сетевое правило группы программ, если вы не хотите, чтобы Сетевой экран применял это сетевое правило к выбранной группе программ при обнаружении сетевой активности и чтобы оно отображалось в списке сетевых правил группы программ.

В этом разделе

Создание и изменение сетевого правила группы программ

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

1. Откройте окно настройки параметров программы (на стр. 48).
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 программ выберите группу программ, для которой хотите создать или изменить сетевое правило.
5. По правой клавише мыши откройте контекстное меню и выберите пункт **Правила группы**.

   Откроется окно **Правила контроля группы программ**.
6. В открывшемся окне **Правила контроля группы программ** выберите закладку **Сетевые правила**.
7. Выполните одно из следующих действий:
   - Если хотите создать новое сетевое правило группы программ, нажмите на кнопку **Добавить**.
   - Если хотите изменить сетевое правило группы программ, выберите его в списке сетевых правил и нажмите на кнопку **Изменить**.
8. Откроется окно **Сетевое правило**.
9. В раскрывающемся списке **Действие** выберите действие, которое должен выполнять Сетевой экран, обнаружив этот вид сетевой активности:
   - **Разрешать**.
   - **Запрещать**.
10. В поле **Название** укажите имя сетевого сервиса одним из следующих способов:
    - Нажмите на значок  , расположенный справа от поля **Название**, и в раскрывающемся списке выберите имя сетевого сервиса.

      В состав Kaspersky Endpoint Security включены сетевые сервисы, описывающие наиболее часто используемые сетевые соединения.
    - В поле **Название** введите имя сетевого сервиса вручную.

    Сетевой сервис – это набор параметров, характеризующих сетевую активность, для которой вы создаете сетевое правило.
11. 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.

По умолчанию флажок **Протокол** снят.

Если сетевой сервис выбран из раскрывающегося списка **Название**, то флажок **Протокол** устанавливается автоматически и раскрывающийся список рядом с флажком заполняется типом протокола, который соответствует выбранному сетевому сервису.

12. 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**.

13. 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.

14. Если в качестве протокола выбран протокол TCP или UDP, вы можете задать порты 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.

15. Если требуется, в поле **Адрес** укажите сетевой адрес.

    В качестве сетевого адреса вы можете использовать IP-адрес или указать статус сетевого соединения. В последнем случае сетевые адреса берутся из всех активных сетевых соединений, имеющих выбранный статус.

    Вы можете выбрать одну из следующих категорий сетевых адресов:

    - **Любой адрес**.
    - **Адреса подсети**.
    - **Адреса из списка**.

16. Установите флажок **Записать в отчет**, если вы хотите, чтобы действие сетевого правила было отражено в отчете (см. раздел «Работа с отчетами» на стр. 245).

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

    Если вы создали новое сетевое правило группы программ, оно отобразится на закладке **Сетевые правила** окна **Правила контроля группы программ**.

18. Нажмите на кнопку **ОК** в окне **Правила контроля группы программ**.

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

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

Включение и выключение сетевого правила группы программ

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

1. Откройте окно настройки параметров программы (на стр. 48).
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 программ выберите нужную группу программ.
5. По правой клавише мыши откройте контекстное меню и выберите пункт **Правила группы**.

   Откроется окно **Правила контроля группы программ**.
6. Выберите закладку **Сетевые правила**.
7. В списке сетевых правил группы программ выберите нужное вам сетевое правило группы программ.
8. Выполните одно из следующих действий:
   - Установите флажок рядом с названием сетевого правила группы программ, если вы хотите включить правило.
   - Снимите флажок рядом с названием сетевого правила группы программ, 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**.
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 группы программ

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

Чтобы изменить действие Сетевого экрана для сетевых правил всей группы программ, выполните следующие действия:

1. Откройте окно настройки параметров программы (на стр. 48).
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 программ выберите группу программ, если вы хотите изменить действие Сетевого экрана для всех ее сетевых правил, созданных по умолчанию. Сетевые правила группы программ, 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 группы программ, выполните следующие действия:

1. Откройте окно настройки параметров программы (на стр. 48).

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 программ выберите нужную группу программ.

5. По правой клавише мыши откройте контекстное меню и выберите пункт **Правила группы**.

   Откроется окно **Правила контроля группы программ**.

6. В открывшемся окне **Правила контроля группы программ** выберите закладку **Сетевые правила**.

7. В списке сетевых правил группы программ выберите сетевое правило группы программ, 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**.

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

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

Изменение приоритета сетевого правила группы программ

Приоритет выполнения сетевого правила группы программ 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 группы программ имеют более высокий приоритет, чем сетевые правила группы программ, созданные по умолчанию.

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

Чтобы изменить приоритет сетевого правила группы программ, выполните следующие действия:

1. Откройте окно настройки параметров программы (на стр. 48).
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 программ выберите нужную группу программ.
5. По правой клавише мыши откройте контекстное меню и выберите пункт **Правила группы**.

   Откроется окно **Правила контроля группы программ**.
6. В открывшемся окне **Правила контроля группы программ** выберите закладку **Сетевые правила**.
7. В списке сетевых правил группы программ выберите сетевое правило группы программ, приоритет которого вы хотите изменить.
8. С помощью кнопок **Вверх** и **Вниз** переместите сетевое правило группы программ на нужную позицию в списке сетевых правил группы программ.
9. Нажмите на кнопку **ОК** в окне **Правила контроля группы программ**.
10. Нажмите на кнопку **ОК** в окне **Сетевой экран**.
11. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Работа с сетевыми правилами программы

В соответствии с сетевыми правилами программы Сетевой экран регулирует доступ этой программы к различным сетевым соединениям.

Сетевой экран по умолчанию создает набор сетевых правил для каждой группы программ, которые Kaspersky Endpoint Security обнаружил на компьютере. Программы, входящие в эту группу программ, наследуют эти сетевые правила. Вы можете изменить действия Сетевого экрана для унаследованных сетевых правил программы. Вы не можете изменить, удалить или выключить сетевые правила программ, унаследованные от родительской группы программ, а также изменить их приоритет.

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

- Создать новое сетевое правило программы.

  Вы можете создать новое сетевое правило программы, в соответствии с которым Сетевой экран должен регулировать сетевую активность этой программы.

- Включить и выключить сетевое правило программы.

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

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

- Изменить параметры сетевого правила программы.

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

- Изменить действие Сетевого экрана для сетевого правила программы.

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

- Изменить приоритет сетевого правила программы.

  Вы можете повысить или понизить приоритет созданного вручную сетевого правила программы.

- Удалить сетевое правило программы.

  Вы можете удалить созданное вручную сетевое правило программы, если вы не хотите, чтобы Сетевой экран применял это сетевое правило к выбранной программе при обнаружении сетевой активности, и чтобы оно отображалось в списке сетевых правил программы.

В этом разделе

Создание и изменение сетевого правила программы

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

1. Откройте окно настройки параметров программы (на стр. 48).
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 программ выберите программу, для которой хотите создать или изменить сетевое правило.
5. По правой клавише мыши откройте контекстное меню и выберите пункт **Правила программы**.

   Откроется окно **Правила контроля программы**.
6. В открывшемся окне **Правила контроля программы** выберите закладку **Сетевые правила**.
7. Выполните одно из следующих действий:

   - Если хотите создать новое сетевое правило программы, нажмите на кнопку **Добавить**.
   - Если хотите изменить сетевое правило программы, выберите его в списке сетевых правил программы и нажмите на кнопку **Изменить**.
8. Откроется окно **Сетевое правило**.
9. В раскрывающемся списке **Действие** выберите действие, которое должен выполнять Сетевой экран, обнаружив этот вид сетевой активности:

   - **Разрешать**.
   - **Запрещать**.
10. В поле **Название** укажите имя сетевого сервиса одним из следующих способов:

    - Нажмите на значок  , расположенный справа от поля **Название**, и в раскрывающемся списке выберите имя сетевого сервиса.

      В состав Kaspersky Endpoint Security включены сетевые сервисы, описывающие наиболее часто используемые сетевые соединения.
    - В поле **Название** введите имя сетевого сервиса вручную.

    Сетевой сервис – это набор параметров, характеризующих сетевую активность, для которой вы создаете сетевое правило.
11. 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.

       По умолчанию флажок **Протокол** снят.

       Если сетевой сервис выбран из раскрывающегося списка **Название**, то флажок **Протокол** устанавливается автоматически и раскрывающийся список рядом с флажком заполняется типом протокола, который соответствует выбранному сетевому сервису.
12. 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**.

13. 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.
14. Если в качестве протокола выбран протокол TCP или UDP, вы можете задать порты компьютера пользователя и удаленного компьютера, соединение между которыми будет контролироваться:
    a. В поле **Удаленные порты** введите порты удаленного компьютера.
    b. В поле **Локальные порты** введите порты компьютера пользователя.
15. Если требуется, в поле **Адрес** укажите сетевой адрес.

    В качестве сетевого адреса вы можете использовать IP-адрес или указать статус сетевого соединения. В последнем случае сетевые адреса берутся из всех активных сетевых соединений, имеющих выбранный статус.

    Вы можете выбрать одну из следующих категорий сетевых адресов:

    - **Любой адрес**.
    - **Адреса подсети**.
    - **Адреса из списка**.
16. Установите флажок **Записать в отчет**, если вы хотите, чтобы действие сетевого правила было отражено в отчете (см. раздел «Работа с отчетами» на стр. 245).
17. Нажмите на кнопку **ОК** в окне **Сетевое правило**.

    Если вы создали новое сетевое правило программы, оно отобразится на закладке **Сетевые правила** окна **Правила программы**.
18. Нажмите на кнопку **ОК** в окне **Правила контроля программы**.
19. Нажмите на кнопку **ОК** в окне **Сетевой экран**.
20. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Включение и выключение сетевого правила программы

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

1. Откройте окно настройки параметров программы (на стр. 48).
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 программ выберите нужную программу.

5. По правой клавише мыши откройте контекстное меню и выберите пункт **Правила программы**.

   Откроется окно **Правила контроля программы**.

6. Выберите закладку **Сетевые правила**.

7. В списке сетевых правил программы выберите нужное вам сетевое правило программы.

8. Выполните одно из следующих действий:

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

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

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

9. Нажмите на кнопку **ОК** в окне **Правила контроля 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 программы

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

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

1. Откройте окно настройки параметров программы (на стр. 48).

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 программ выберите программу, если хотите изменить действие Сетевого экрана для всех ее сетевых правил, созданных по умолчанию.

   Сетевые правила программы, 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** в окне **Сетевой экран**.

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

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

1. Откройте окно настройки параметров программы (на стр. 48).

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 программ выберите нужную программу.

5. По правой клавише мыши откройте контекстное меню и выберите пункт **Правила программы**.

   Откроется окно **Правила контроля программы**.

6. В открывшемся окне **Правила контроля программы** выберите закладку **Сетевые правила**.

7. В списке сетевых правил программы выберите сетевое правило программы, 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**.

10. В окне **Сетевой экран** нажмите на кнопку **ОК**.

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

Изменение приоритета сетевого правила программы

Приоритет выполнения сетевого правила программы 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 программы имеют более высокий приоритет, чем сетевые правила, унаследованные от родительской группы программ.

Вы не можете изменить приоритет унаследованных сетевых правил программы.

Сетевые правила программы (как унаследованные, так и созданные вручную) имеют приоритет над сетевыми правилами группы программ. То есть в группе все программы автоматически наследуют сетевые правила этой группы, но если для отдельной программы изменить какое-либо правило или создать новое, то оно обрабатывается прежде, чем все унаследованные.

Чтобы изменить приоритет сетевого правила программы, выполните следующие действия:

1. Откройте окно настройки параметров программы (на стр. 48).
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 программ выберите нужную программу.
5. По правой клавише мыши откройте контекстное меню и выберите пункт **Правила программы**.

   Откроется окно **Правила контроля программы**.
6. В открывшемся окне **Правила контроля программы** выберите закладку **Сетевые правила**.
7. В списке сетевых правил программы выберите сетевое правило программы, приоритет которого вы хотите изменить.
8. С помощью кнопок **Вверх** и **Вниз** переместите сетевое правило программы на нужную позицию в списке сетевых правил программы.
9. Нажмите на кнопку **ОК** в окне **Правила контроля программы**.
10. Нажмите на кнопку **ОК** в окне **Сетевой экран**.
11. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Настройка дополнительных параметров работы Сетевого экрана

Вы можете настроить дополнительные параметры работы Сетевого экрана.

Чтобы настроить дополнительные параметры работы Сетевого экрана, выполните следующие действия:

1. Откройте окно настройки параметров программы (на стр. 48).
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 пакетные правила**.

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

   Откроется окно **Дополнительно**.
5. В открывшемся окне **Дополнительно** выполните одно из следующих действий:

   - Установите флажок рядом с названием дополнительного параметра, если вы хотите включить параметр.
   - Снимите флажок рядом с названием дополнительного параметра, если вы хотите выключить параметр.

К дополнительным параметрам работы Сетевого экрана относятся следующие:

- **Разрешать активный режим FTP**.
- **Блокировать соединения, если нет возможности запроса действия (не загружен интерфейс программы)**.
- **Не отключать Сетевой экран до полной остановки системы**.

По умолчанию дополнительные параметры работы Сетевого экрана включены.

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

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 (см. раздел «Изменение параметров блокирования атакующего компьютера» на стр. 116).

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. 211).

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. 46);
- из окна настройки параметров программы (см. раздел «Окно настройки параметров программы» на стр. 48).

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 Защита 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 Защита 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 (на стр. 48).
2. В левой части окна в блоке **Антивирусная защита** выберите раздел **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.

Изменение параметров блокирования атакующего компьютера

Чтобы изменить параметры блокирования атакующего компьютера, выполните следующие действия:

1. Откройте окно настройки параметров программы (на стр. 48).
2. В левой части окна выберите раздел **Защита от сетевых атак**.

   В правой части окна отобразятся параметры компонента Защита от сетевых атак.
3. В блоке **Защита от сетевых атак** 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 не установлен, 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.

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. 73), Веб-Антивирус (см. раздел «Защита компьютера в интернете. Веб-Антивирус» на стр. 83) и IM-Антивирус (см. раздел «Защита трафика интернет-пейджеров. IM-Антивирус» на стр. 90) 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, Веб-Антивирус и IM-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 (на стр. 48).
2. В левой части окна выберите блок **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 (на стр. 48).
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 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.

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 (на стр. 48).

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**.

   По умолчанию флажок установлен.

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.

   c. После выбора программы откроется окно **Программа**.

d. В поле **Название** введите название для выбранной программы.

e. Нажмите 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** для сохранения внесенных изменений.

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. 46).

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.

КОНТРОЛЬ ЗАПУСКА ПРОГРАММ

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. 20).

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. 123).

Запуск программ, параметры которых не удовлетворяют ни одному из правил контроля запуска программ, регулируются созданным по умолчанию правилом «Разрешить все». Правило «Разрешить все» разрешает любым пользователям запускать любые программы.

Все попытки запуска программ пользователями фиксируются в отчетах (см. раздел «Работа с отчетами» на стр. 245).

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. 46);
- из окна настройки параметров программы (см. раздел «Окно настройки параметров программы» на стр. 48).

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 (на стр. 48).
2. В левой части окна в блоке **Контроль рабочего места** выберите раздел 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.

О правилах контроля запуска программ

Правило контроля запуска программ представляет собой набор параметров, которые определяют следующие функции компонента Контроль запуска программ:

- Классификация всех установленных на компьютере программ с помощью *условий срабатывания правила* (далее также «условий»). Условие срабатывания правила представляет собой соответствие: критерий условия – значение условия – тип условия (см. рис. ниже).

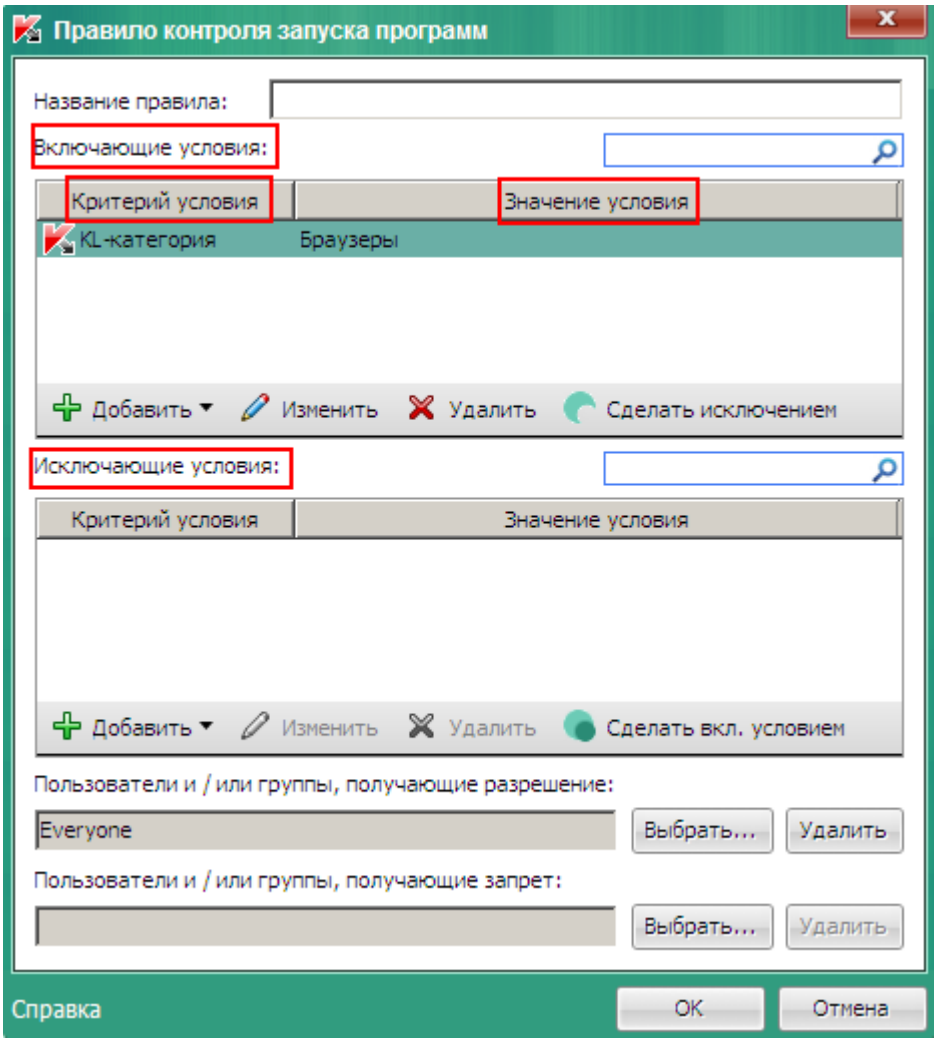

Рисунок 4. Правило контроля запуска программ. Параметры условия срабатывания правила

Критерием условия срабатывания правила может быть:

- 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.
- MD5-хеш исполняемого файла программы.
- Принадлежность программы к KL-категории. KL-категория – сформированный специалистами «Лаборатории Касперского» список программ, обладающих общими тематическими признаками.

  Например, KL-категория «Офисные программы» включает в себя программы из пакета Microsoft Office, Adobe® Acrobat® и другие.

- Расположение исполняемого файла программы на съемном носителе.

Тип условия срабатывания правила определяет порядок отнесения программы к правилу:

- *Включающие условия*. Программа удовлетворяет правилу, если ее параметры удовлетворяют хотя бы одному включающему условию срабатывания правила.

- *Исключающие условия*. Программа не удовлетворяет правилу, если ее параметры удовлетворяют хотя бы одному исключающему условию срабатывания правила или не удовлетворяют ни одному включающему условию срабатывания правила. Правило не контролирует запуск таких программ.

- Разрешение выбранным пользователям и / или группам пользователей запускать программы.

  Вы можете выбрать пользователя и / или группу пользователей, которым разрешен запуск программ, удовлетворяющих правилу.

  Правило, в котором не указан ни один пользователь, которому разрешен запуск программ, удовлетворяющих правилу, называется *запрещающим*.

- Запрещение выбранным пользователям и / или группам пользователей запускать программы.

  Вы можете выбрать пользователя и / или группу пользователей, которым запрещен запуск программ, удовлетворяющих правилу контроля запуска программ.

  Правило, в котором не указан ни один пользователь, которому запрещен запуск программ, удовлетворяющих правилу, называется *разрешающим*.

Приоритет запрещающего правила выше приоритета разрешающего правила. Например, если для группы пользователей определено разрешающее правило контроля запуска программы, и для одного из пользователей этой группы определено запрещающее правило контроля запуска программы, то этому пользователю будет запрещен запуск программы.

Статус работы правила контроля запуска программ

Правила контроля запуска программ могут иметь три статуса работы:

- *Вкл.* Статус работы правила означает, что правило включено.

- *Выкл*. Статус работы правила означает, что правило выключено.

- *Тест*. Статус работы правила означает, что Kaspersky Endpoint Security не ограничивает запуск программ в соответствии с параметрами правила, а лишь фиксирует в отчетах (см. раздел «Работа с отчетами» на стр. 245) информацию о запуске программ.

  Статус работы правила *Тест* удобно использовать для проверки работы сформированного правила контроля запуска программ. Пользователь не ограничен в запуске программ, удовлетворяющих правилу со статусом работы *Тест*.Разрешение или запрет на запуск программы формируются отдельно для тестовых и не тестовых правил.

Правила контроля запуска программ по умолчанию

По умолчанию созданы следующие правила контроля запуска программ:

- **Разрешить все**. Правило разрешает запуск всех программ всем пользователям. На этом правиле основана работа Контроля запуска программ в режиме «Черный список» (см. раздел «О режимах работы Контроля запуска программ» на стр. 130). По умолчанию правило включено.

- **Доверенные программы обновления**. Правило разрешает запуск программ, которые установлены или обновлены программами из KL-категории «Доверенные программы обновления», и для которых не определены запрещающие правила. В KL-категорию «Доверенные программы обновления» включены программы обновления наиболее известных производителей программного обеспечения. Правило создано по умолчанию только на стороне Плагина управления Kaspersky Endpoint Security. По умолчанию правило выключено.

- **Операционная система и ее компоненты**. Правило разрешает всем пользователям запускать программы, принадлежащие KL-категории «Золотая категория». В KL-категорию «Золотая категория» включены программы, необходимые для запуска и нормальной работы операционной системы. Разрешение запускать программы из этой KL-категории требуется для работы Контроля запуска программ в режиме «Белый список» (см. раздел «О режимах работы Контроля запуска программ» на стр. 130). Правило создано по умолчанию только на стороне Плагина управления Kaspersky Endpoint Security. По умолчанию правило выключено.

Действия с правилами контроля запуска программ

Вы можете выполнить следующие действия с правилами контроля запуска программ:

- Добавить новое правило.
- Изменить правило.
- Сформировать условия срабатывания правила контроля запуска программ.
- Изменить статус работы правила.

  Правило контроля запуска программ может быть включено (статус работы *Вкл*), выключено (статус работы *Выкл*) или работать в тестовом режиме (статус работы *Тест*). По умолчанию после создания правило контроля запуска программ включено (имеет статус работы *Вкл)*. Вы можете выключить правило контроля запуска программ или включить работу правила в тестовом режиме.

- 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 (на стр. 48).
2. В левой части окна в блоке **Контроль рабочего места** выберите раздел **Контроль запуска программ**.

   В правой части окна отобразятся параметры компонента Контроль запуска программ.

3. Выполните одно из следующих действий:

   - Если вы хотите добавить правило, нажмите на кнопку **Добавить**.
   - Если вы хотите изменить правило, нажмите на кнопку **Изменить**.

   Откроется окно **Правило контроля запуска программ**.

4. Задайте или измените параметры правила. Для этого выполните следующие действия:

   a. В поле **Название** введите или измените название правила.

   b. В таблице **Включающие условия** сформируйте (см. раздел «Добавление условия срабатывания правила контроля запуска программ» на стр. 126) или измените список включающих условий срабатывания правила контроля запуска программ. Для этого воспользуйтесь кнопками **Добавить**, **Изменить**, **Удалить**, **Сделать исключением**.

   c. В таблице **Исключающие условия** сформируйте или измените список исключающих условий срабатывания правила контроля запуска программ. Для этого воспользуйтесь кнопками **Добавить**, **Изменить**, **Удалить**, **Сделать вкл. условием**.

   d. Вы можете изменить тип условия срабатывания правила. Для этого выполните следующие действия:

      - Чтобы изменить тип условия с включающего на исключающее, выберите условие в таблице **Включающие условия** и нажмите на кнопку **Сделать исключением**.

      - Чтобы изменить 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 запускать программы, удовлетворяющие включающим условиям срабатывания правила. Для этого в поле **Пользователи и / или группы, получающие разрешение** введите имена пользователей и / или группы пользователей вручную или нажмите на кнопку **Выбрать**. Откроется стандартное окно Microsoft Windows **Выбор пользователей или групп**. В этом окне вы можете выбрать пользователей и / или группы пользователей.

   f. Задайте или измените список пользователей и / или групп пользователей, которым запрещено запускать программы, удовлетворяющие включающим условиям срабатывания правила. Для этого в поле **Пользователи и / или группы, получающие запрет** введите имена пользователей и / или группы пользователей вручную или нажмите на кнопку **Выбрать**. Откроется стандартное окно Microsoft Windows **Выбор пользователей или групп**. В этом окне вы можете выбрать пользователей и / или группы пользователей.

5. Нажмите на кнопку **OK**.

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

Добавление условия срабатывания правила контроля запуска программ

Чтобы добавить условие срабатывания правила контроля запуска программ, выполните следующие действия:

1. Откройте окно настройки параметров программы (на стр. 48).

2. В левой части окна в блоке **Контроль рабочего места** выберите раздел **Контроль запуска программ**.

   В правой части окна отобразятся параметры компонента Контроль запуска программ.

3. Выполните одно из следующих действий:

   - Нажмите на кнопку **Добавить**, если вы хотите добавить условие срабатывания нового правила контроля запуска программ.

   - Выберите из списка **Правила контроля запуска программ** нужное правило и нажмите на кнопку **Добавить**, если вы хотите добавить условие срабатывания уже существующего правила контроля запуска программ.

Откроется окно **Правило контроля запуска программ**.

4. В таблице **Включающие условия** или **Исключающие условия** срабатывания правила контроля запуска программ нажмите на кнопку **Добавить**.

   Откроется контекстное меню кнопки **Добавить**.

5. Выполните следующие действия:

   - Выберите пункт **Условие из свойств файла**, если вы хотите сформировать условие срабатывания правила контроля запуска программ на основе свойств исполняемого файла программы. Для этого выполните следующие действия:

     a. В стандартном окне Microsoft Windows **Открыть файл** выберите исполняемый файл программы, на основе свойств которого вы хотите сформировать условие срабатывания правила контроля запуска программ.

     b. Нажмите на кнопку **Открыть**.

        Откроется окно **Условие из свойств файла**. Параметры окна **Условие из свойств файла** имеют значения, извлеченные из свойств выбранного исполняемого файла программы.

     c. В окне **Условие из свойств файла** выберите критерий, на основе которого вы хотите создать одно или несколько условий срабатывания правила: **Метаданные**, **Путь к файлу или папке** или **Хеш файла (MD5)**. Для этого выберите соответствующий параметр.

     d. При необходимости измените значения параметров выбранного критерия условия.

     e. Нажмите на кнопку **OK**.

   - Выберите пункт **Условие(я) из свойств файлов указанной папки**, если вы хотите сформировать одно или несколько условий срабатывания правила контроля запуска программ из свойств файлов указанной папки. Для этого выполните следующие действия:

     a. В окне **Выбор папки** выберите папку с исполняемыми файлами программ, на основе свойств которых вы хотите сформировать одно или несколько условий срабатывания правила контроля запуска программ.

     b. Нажмите на кнопку **OK**.

        Откроется окно **Добавление условий**.

     c. В поле **Папка** измените при необходимости путь к папке с исполняемыми файлами программ. Для этого нажмите на кнопку **Выбрать**. Откроется окно **Выбор папки**. В этом окне вы можете выбрать нужную папку.

     d. В раскрывающемся списке **Добавить по критерию** выберите критерий, на основе которого вы хотите создать одно или несколько условий срабатывания правила: **Метаданные**, **Путь к папке**, **Хеш файла (MD5)** или **KL-категория**, к которой принадлежит исполняемый файл программы.

        Если в раскрывающемся списке **Добавить по критерию** 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**.

     e. Установите флажки напротив названий исполняемых файлов программ, свойства которых вы хотите включить в условие(я) срабатывания правила.

     f. Нажмите на кнопку **Далее**.

        Отобразится список сформированных условий срабатывания правила.

     g. В списке сформированных условий срабатывания правила установите флажки около тех условий срабатывания правила, которые вы хотите добавить в правило контроля запуска программ.

     h. Нажмите на кнопку **Завершить**.

- Выберите пункт **Условие(я) из свойств запущенных программ**, если вы хотите сформировать одно или несколько условий срабатывания правила контроля запуска программ из свойств запущенных на компьютере программ. Для этого выполните следующие действия:

  a. В окне **Добавление условий** в раскрывающемся списке **Добавить по критерию** выберите критерий, на основе которого вы хотите создать одно или несколько условий срабатывания правила: **Метаданные**, **Путь к папке**, **Хеш файла (MD5)** или **KL-категория**, к которой принадлежит исполняемый файл программы.

     Если в раскрывающемся списке **Добавить по критерию** вы выбрали элемент **Метаданные**, установите флажки напротив тех свойств исполняемых файлов программы, которые вы хотите использовать в условии срабатывании правила: **Название файла**, **Название программы**, **Версия программы**, **Производитель**.

  b. Установите флажки напротив названий исполняемых файлов программ, свойства которых вы хотите включить в условие(я) срабатывания правила.

  c. Нажмите на кнопку **Далее**.

     Отобразится список сформированных условий срабатывания правила.

  d. В списке сформированных условий срабатывания правила установите флажки около тех условий срабатывания правила, которые вы хотите добавить в правило контроля запуска программ.

  e. Нажмите на кнопку **Завершить**.

- Выберите пункт **Условие(я) «KL-категория»**, если вы хотите сформировать одно или несколько условий срабатывания правила контроля запуска программ по критерию «KL-категория». Для этого выполните следующие действия:

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

  b. Нажмите на кнопку **OK**.

- Выберите пункт **Условие вручную**, если вы хотите сформировать условие срабатывания правила контроля запуска программ вручную. Для этого выполните следующие действия:

  a. В окне **Пользовательское условие** введите путь к исполняемому файлу программы. Для этого нажмите на кнопку **Выбрать**. Откроется окно Microsoft Windows **Открыть файл**. В этом окне вы можете выбрать исполняемый файл программы.

  b. Выберите критерий, на основе которого вы хотите создать одно или несколько условий срабатывания правила: **Метаданные**, **Путь к файлу или папке** или **Хеш файла (MD5)**. Для этого выберите соответствующий параметр.

  c. При необходимости измените значения параметров выбранного критерия условия.

  d. Нажмите на кнопку **OK**.

- Выберите пункт **Условие по носителю файла**, если вы хотите сформировать условие срабатывания правила контроля запуска, основанное на информации о носителе исполняемого файла программы. Для этого выполните следующие действия:

  a. В окне **Условие по носителю файла** в раскрывающемся списке **Носитель** выберите тип носителя, запуск программ с которого контролирует правило контроля запуска программ.

  b. Нажмите на кнопку **OK**.

Изменение статуса правила контроля запуска программ

Чтобы изменить статус работы правила контроля запуска программ, выполните следующие действия:

1. Откройте окно настройки параметров программы (на стр. 48).
2. В левой части окна в блоке **Контроль рабочего места** выберите раздел **Контроль запуска программ**.

   В правой части окна отобразятся параметры компонента Контроль запуска программ.
3. Выберите правило, статус работы которого вы хотите изменить.
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*.
   - Если вы хотите, чтобы правило работало в тестовом режиме, выберите значение *Тест*.
5. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

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 жалобу администратору локальной сети организации.

Для сообщения о блокировке запуска программы и письма-жалобы предусмотрены шаблоны. Вы можете изменять шаблоны сообщений.

Чтобы изменить шаблон сообщения, выполните следующие действия:

1. Откройте окно настройки параметров программы (на стр. 48).
2. В левой части окна в блоке **Контроль рабочего места** выберите раздел **Контроль запуска программ**.

   В правой части окна отобразятся параметры компонента Контроль запуска программ.
3. В правой части окна нажмите на кнопку **Шаблоны**.

   Откроется окно **Шаблоны**.
4. Выполните одно из следующих действий:
   - Если вы хотите изменить шаблон сообщения о блокировке запуска программы, выберите закладку **Блокировка**.
   - Если вы хотите изменить шаблон письма-жалобы администратору локальной сети организации, выберите закладку **Жалоба**.
5. Измените шаблон сообщения о блокировке или письма-жалобы. Для этого используйте кнопки **По умолчанию** и **Переменные**.
6. Нажмите на кнопку **ОК**.
7. 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. 123).

  Этот режим работы Контроля запуска программ настроен по умолчанию. Разрешение на запуск всех программ основано на правиле контроля запуска программ «Разрешено все», созданном 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. Таким образом, если разрешающие правила контроля запуска программ сформированы максимально полно, Контроль запуска программ запрещает запуск всех новых, не проверенных администратором локальной сети организации программ, но обеспечивает работоспособность операционной системы и проверенных программ, которые нужны пользователям для выполнения должностных обязанностей.

Настройка Контроля запуска программ для работы в этих режимах возможна как в локальном интерфейсе Kaspersky Endpoint Security, так и на стороне Kaspersky Security Center.

Однако Kaspersky Security Center предоставляет инструменты, недоступные в локальном интерфейсе Kaspersky Endpoint Security и необходимые для:

- Создания категорий программ (см. раздел «Этап 2. Создание категорий программ» на стр. 131). Правила контроля запуска программ на стороне Kaspersky Security Center основываются на созданных вами категориях программ, а не на включающих и исключающих условиях, как в локальном интерфейсе Kaspersky Endpoint Security.

- Сбора информации о программах, которые установлены на компьютерах локальной сети организации (см. раздел «Этап 1. Сбор информации о программах, которые установлены на компьютерах пользователей» на стр. 131).

- Анализа работы Контроля запуска программ после изменения режима (см. раздел «Этап 4. Тестирование разрешающих правил контроля запуска программ» на стр. 133).

Поэтому настройку режима работы компонента Контроль запуска программ рекомендуется выполнять на стороне Kaspersky Security Center.

Переход из режима «Черный список» к режиму «Белый список»

Этот раздел содержит информацию о переходе из режима работы Контроля запуска программ «Черный список» в режим «Белый список» на стороне Kaspersky Security Center и рекомендации по оптимальному использованию функциональности Контроля запуска программ.

В этом разделе

Этап 1. Сбор информации о программах, которые установлены на компьютерах пользователей

На этом этапе требуется получить представление о программах, используемых на компьютерах локальной сети организации. Для этого рекомендуется собрать информацию о:

- Производителях, версиях и локализациях программ, которые используются в локальной сети организации.
- Регулярности обновлений программ.
- Политиках использования программ, принятых в организации. Это могут быть политики безопасности или административные политики.
- Расположении хранилища дистрибутивов программ.

Чтобы собрать информацию о программах, которые используются на компьютерах локальной сети организации, вы можете использовать данные, представленные в папках **Реестр программ** и **Исполняемые файлы программ**. Папки **Реестр программ** и **Исполняемые файлы программ** входят в состав папки **Программы и уязвимости** дерева консоли 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 Kaspersky Endpoint Security (см. раздел «О задачах для Kaspersky Endpoint Security» на стр. 283).

Открыв окно свойств выбранной программы в папке **Реестр программ** или **Исполняемые файлы программ**, вы можете получить общую информацию о программе и информацию об исполняемых файлах программы, а также просмотреть список компьютеров, на которых установлена эта программа.

Этап 2. Создание категорий программ

На этом этапе требуется создать категории программ, на основе которых можно создать правила 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. Откройте папку **Программы и уязвимости – Категории программ** дерева консоли.
3. В панели результатов по правой клавише мыши откройте контекстное меню.
4. В контекстном меню выберите пункт **Создать** → **Категорию**.

   Запустится мастер создания категории программ.
5. Следуйте указаниям мастера создания категории программ.

Этап 3. Создание разрешающих правил контроля запуска программ

На этом этапе требуется создать правила контроля запуска программ, которые разрешают пользователям локальной сети организации запускать программы, принадлежащие категориям, созданным на предыдущем этапе.

Чтобы создать разрешающее правило контроля запуска программ выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые компьютеры** дерева консоли откройте папку с названием группы администрирования, в состав которой входят нужные клиентские компьютеры.
3. В панели результатов выберите закладку **Политики**.
4. По правой кнопке мыши откройте контекстное меню политики
5. В контекстном меню политики выберите пункт **Свойства**.

   Откроется окно свойство политики.
6. В окне свойств политики выберите раздел **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 на предыдущем шаге категорию программ, на основе которой вы хотите создать разрешающее правило.
9. Задайте список пользователей и / или групп пользователей, которым разрешено запускать программы, принадлежащие к выбранной категории. Для этого в поле **Пользователи и / или группы, получающие разрешение** введите имена пользователей и / или группы пользователей вручную или нажмите на кнопку **Выбрать**. Откроется стандартное окно Microsoft Windows **Выбор пользователей или групп**. В этом окне вы можете выбрать пользователей и / или группы пользователей.
10. Список пользователей, которым запрещено запускать программы, принадлежащие к выбранной категории, оставьте пустым.
11. Установите флажок **Доверенные программы обновления**, если вы хотите, чтобы программы из категории, указанной в правиле, Kaspersky Endpoint Security считал доверенными программами обновления и разрешал им запускать другие программы, для которых не определены правила контроля их запуска.

12. Нажмите на кнопку **OK**.

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

Этап 4. Тестирование разрешающих правил контроля запуска программ

На этом этапе требуется выполнить следующие действия:

1. Изменить статус работы созданных разрешающих правил контроля запуска программ (см. раздел «Изменение статуса правила контроля запуска программ на стороне Kaspersky Security Center» на стр. 134) на *Тест*.

2. Проанализировать работу тестовых разрешающих правил контроля запуска программ.

   Для анализа работы тестовых правил контроля запуска программ требуется изучить события о работе компонента Контроль запуска программ, приходящие на Kaspersky Security Center. Если разрешен запуск всех программ, которые вы имели в виду при формировании категорий программ, то созданы верные правила. В противном случае рекомендуется уточнить параметры созданных вами категорий программ и правил контроля запуска программ.

Чтобы в хранилище событий Kaspersky Security Center просмотреть события о работе компонента Контроль запуска программ, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.

2. Откройте папку **Выборки событий** \ **События** \ **Информационные события** \ **Критические события** дерева консоли для просмотра событий о разрешенных / запрещенных запусках программ.

   В рабочей области Kaspersky Security Center, расположенной справка от дерева консоли, отображается список всех событий выбранного уровня важности, переданных на Kaspersky Security Center за период, указанный в свойствах Сервера администрирования.

3. Для просмотра информации о событии откройте свойства события одним из следующих способов:

   - Дважды нажмите левой клавишей мыши по событию.
   - По правой клавише мыши откройте контекстное меню события и выберите пункт **Свойства**.
   - Нажмите на кнопку **Открыть свойства события** справа от списка событий.

Этап 5. Переход к режиму «Белый список»

На этом этапе требуется выполнить следующие действия:

- Включить созданные вами правила контроля запуска программ. Для этого требуется изменить статус работы правил с *Тест* на *Вкл*.
- Включить созданные по умолчанию правила «Доверенные программы обновления» и «Операционная система и ее компоненты». Для этого требуется изменить статус работы правил с *Выкл* на *Вкл*.
- Выключить созданное по умолчанию правило «Разрешить все». Для этого требуется изменить статус работы правил с *Вкл* на *Выкл*.

См. также

Изменение статуса правила контроля запуска программ на стороне Kaspersky Security Center

Чтобы изменить статус работы правила контроля запуска программ, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые компьютеры** дерева консоли откройте папку с названием группы администрирования, в состав которой входят нужные клиентские компьютеры.
3. В панели результатов выберите закладку **Политики**.
4. По правой кнопке мыши откройте контекстное меню политики.
5. В контекстном меню политики выберите пункт **Свойства**.

   Откроется окно свойство политики.
6. В окне свойств политики выберите раздел **Контроль запуска программ**.

   В правой части окна отобразятся параметры компонента Контроль запуска программ.
7. Выберите правило контроля запуска программ, статус работы которого вы хотите изменить.
8. В графе **Статус** выполните одно из следующих действий:
   - Если вы хотите включить использование правила, выберите значение *Вкл*.
   - Если вы хотите выключить использование правила, выберите значение *Выкл*.
   - Если вы хотите, чтобы правило работало в тестовом режиме, выберите значение *Тест*.
9. Нажмите на кнопку **Применить**.

КОНТРОЛЬ АКТИВНОСТИ ПРОГРАММ

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. 20).

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

В ЭТОМ РАЗДЕЛЕ

О Контроле активности программ

Компонент Контроль активности программ 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. 293). 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 Контроль активности программ проверяет целостность программы. Если программа не была изменена, компонент применяет к ней текущие правила контроля программ. Если программа была изменена, Контроль активности программ исследует программу как при первом запуске.

Включение и выключение Контроля активности программ

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. 46);
- из окна настройки параметров программы (см. раздел «Окно настройки параметров программы» на стр. 48).

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 блоке **Контроль рабочего места** выберите раздел 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.

Распределение программ по группам доверия

Во время первого запуска 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 уровня опасности, 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,
  - индекс опасности программ меньше 50,
  - 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,
  - индекс опасности программ находится в диапазоне 51-71,
  - 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,
  - индекс опасности программ находится в диапазоне 71-100,
  - 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, а затем отправляет запрос в базу Kaspersky Security Network (см. раздел «Участие в Kaspersky Security Network» на стр. 293) (при наличии подключения к интернету). Если запись о программе найдена в базе Kaspersky Security Network, то программа помещается в группу доверия, зарегистрированную в базе Kaspersky Security Network.

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.

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 окончательную 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 которого 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 объективное решение о том, в какую группу доверия следует поместить эту программу.

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

1. Откройте окно настройки параметров программы (на стр. 48).
2. В левой части окна в блоке **Контроль рабочего места** выберите раздел 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**.
   - 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.
5. Укажите время, которое отводится для проверки запускаемой программы, в поле **Максимальное время определения группы**.
6. 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 (см. раздел «Изменение правила контроля программы» на стр. 141).

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 (на стр. 48).
2. В левой части окна в блоке **Контроль рабочего места** выберите раздел **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.

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 групп доверия и правил контроля 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 (на стр. 48).
2. В левой части окна в блоке **Контроль рабочего места** выберите раздел **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 группу доверия или группу программ.
5. По правой клавише мыши откройте контекстное меню группы доверия или группы программ.
6. В контекстном меню группы доверия или группы программ выберите пункт **Правила группы**.

   Откроется окно **Правила контроля группы программ**.
7. 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.
8. Для нужного ресурса в графе соответствующего действия по правой клавише мыши откройте контекстное меню.
9. 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.
10. Нажмите на кнопку **OK**.
11. В окне **Программы** нажмите на кнопку **OK**.
12. 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 (на стр. 48).
2. В левой части окна в блоке **Контроль рабочего места** выберите раздел **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 **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 **OK**.
10. В окне **Программы** нажмите на кнопку **OK**.
11. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Загрузка и обновление правил контроля программ из базы Kaspersky Security Network

По умолчанию для программ, найденных в базе Kaspersky Security Network, применяются правила контроля программ, загруженные из этой базы.

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 (на стр. 48).
2. В левой части окна в блоке **Контроль рабочего места** выберите раздел **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 (см. раздел «Изменение правила контроля программы» на стр. 141) или выключить наследование ограничений родительского процесса.

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

1. Откройте окно настройки параметров программы (на стр. 48).
2. В левой части окна в блоке **Контроль рабочего места** выберите раздел **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. По правой клавише мыши откройте контекстное меню программы.

6. В контекстном меню программы выберите пункт **Правила программы**.

   Откроется окно **Правила контроля программы**.

7. В окне **Правила контроля программы** выберите закладку **Исключения**.

8. Установите флажок **Не наследовать ограничения родительского процесса (программы)**.

9. Нажмите на кнопку **OK**.

10. В окне **Программы** нажмите на кнопку **OK**.

11. 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 (на стр. 48).

2. В левой части окна в блоке **Контроль рабочего места** выберите раздел **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. По правой клавише мыши откройте контекстное меню программы и выберите пункт **Правила программы**.

   Откроется окно **Правила контроля программы**.

6. В окне **Правила контроля программы** 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.

Настройка параметров хранения правил контроля неиспользуемых 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 настроить параметры хранения правил контроля неиспользуемых программ, выполните следующие действия:

1. Откройте окно настройки параметров программы (на стр. 48).
2. В левой части окна в блоке **Контроль рабочего места** выберите раздел **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 (на стр. 48).
2. В левой части окна в блоке **Контроль рабочего места** выберите раздел **Контроль активности программ**.

   В правой части окна отобразятся параметры компонента Контроль активности программ.
3. Нажмите на кнопку **Ресурсы**.

   Откроется закладка **Защищаемые ресурсы** окна **Программы**.
4. В левой части закладки **Защищаемые ресурсы** выберите раздел или категорию защищаемых ресурсов, в которые вы хотите добавить новую категорию защищаемых ресурсов.
5. По левой клавише мыши откройте контекстное меню кнопки **Добавить**.
6. В контекстном меню выберите пункт **Категорию**.

   Откроется окно **Категория защищаемых ресурсов**.
7. В окне **Категория защищаемых ресурсов** введите название новой категории защищаемых ресурсов.
8. Нажмите на кнопку **OK**.

   В списке категорий защищаемых ресурсов появится новый элемент.
9. В окне **Программы** нажмите на кнопку **OK**.
10. 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 (на стр. 48).
2. В левой части окна в блоке **Контроль рабочего места** выберите раздел **Контроль активности программ**.

   В правой части окна отобразятся параметры компонента Контроль активности программ.
3. Нажмите на кнопку **Ресурсы**.

   Откроется закладка **Защищаемые ресурсы** окна **Программы**.
4. В левой части закладки **Защищаемые ресурсы** выберите категорию защищаемых ресурсов, в которую вы хотите добавить новый защищаемый ресурс.
5. В верхней левой части закладки **Защищаемые ресурсы** по левой клавише мыши откройте контекстное меню кнопки **Добавить**.
6. В контекстном меню выберите тип ресурса, который вы хотите добавить:
   - **Файл или папку**.
   - **Ключ реестра**.

Откроется окно **Защищаемый ресурс**.

7. В окне **Защищаемый ресурс** в поле **Название** введите название защищаемого ресурса.
8. Нажмите на кнопку **Обзор**.
9. В открывшемся окне задайте необходимые параметры в зависимости от типа добавляемого защищаемого ресурса и нажмите на кнопку **OK**.
10. В окне **Защищаемый ресурс** нажмите на кнопку **OK**.

    На закладке **Защищаемые ресурсы** в списке защищаемых ресурсов выбранной категории появится новый элемент.
11. Нажмите на кнопку **OK**.
12. 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 (на стр. 48).
2. В левой части окна в блоке **Контроль рабочего места** выберите раздел **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 **Программы**.
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** по левой клавише мыши откройте контекстное меню кнопки **Добавить**.

     b. В контекстном меню 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**.

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

     d. Нажмите на кнопку **Обзор**.

     e. 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.

     f. Нажмите на кнопку **OK**.

g. 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**.

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

5. В окне **Программы** нажмите на кнопку **OK**.

6. 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. 20).

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 конфиденциальной информации путем ограничения доступа пользователей к устройствам, установленным или подключенным к компьютеру:

- устройствам памяти (жесткие диски, съемные носители информации, ленточные накопители, CD/DVD-диски);
- 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. 46);
- из окна настройки параметров программы (см. раздел «Окно настройки параметров программы» на стр. 48).

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.

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

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

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

1. Откройте окно настройки параметров программы (на стр. 48).
2. В левой части окна в блоке **Контроль рабочего места** выберите раздел **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 2. Типовые решения о доступе к устройствам

№	Исходные условия	Промежуточные шаги до принятия решения о доступе к устройству			Решение о доступе к устройству
		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.

Изменение правила доступа к устройствам

Чтобы изменить правило доступа к устройствам, выполните следующие действия:

1. Откройте окно настройки параметров программы (на стр. 48).
2. В левой части окна в блоке **Контроль рабочего места** выберите раздел **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 **Все время** с установленными правами на все возможные операции с устройствами.
6. Измените параметры правила доступа к устройствам:

   a. Для изменения списка **Пользователи и / или группы пользователей** используйте кнопки **Добавить**, **Изменить**, **Удалить**.

   b. Для изменения списка расписаний доступа к устройствам используйте кнопки **Создать**, **Изменить**, **Копировать**, **Удалить** в таблице **Права выделенной группы пользователей по расписаниям доступа**.

   c. Выберите пользователя и / или группу пользователей в списке **Пользователи и / или группы пользователей**.

   d. 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.

   e. Для каждого используемого для выбранного пользователя и / или группы пользователей расписания доступа к устройствам 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 интересующих операций.

   f. Повторите пункты с – е для остальных элементов списка **Пользователи и / или группы пользователей**.

   g. Нажмите на кнопку **ОК**.

   После того как вы изменили исходные значения параметров правила доступа к устройствам, параметр доступа к типу устройств принимает значение *Ограничивать правилами*.
7. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Изменение правила доступа к шине подключения

Чтобы изменить правило доступа к шине подключения, выполните следующие действия:

1. Откройте окно настройки параметров программы (на стр. 48).
2. В левой части окна в блоке **Контроль рабочего места** выберите раздел **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 устройств

По умолчанию при добавлении устройства в список доверенных устройств доступ к устройству разрешается всем пользователям (группе пользователей «Все»).

Чтобы добавить устройство в список доверенных устройств, выполните следующие действия:

1. Откройте окно настройки параметров программы (на стр. 48).
2. В левой части окна в блоке **Контроль рабочего места** выберите раздел **Контроль устройств**.

   В правой части окна отобразятся параметры компонента Контроль устройств.
3. В правой части окна выберите закладку **Доверенные устройства**.

4. Нажмите на кнопку **Добавить**.

   Откроется окно **Добавление 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 / или группам пользователей**.

8. В окне **Добавление доверенных устройств** нажмите на кнопку **OK**.

   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.

Изменение параметра Пользователи доверенного устройства

По умолчанию при добавлении устройства в список доверенных устройств доступ к устройству разрешается всем пользователям (группе пользователей «Все»). Вы можете изменить параметр **Пользователи** доверенного устройства.

Чтобы изменить параметр Пользователи доверенного устройства, выполните следующие действия:

1. Откройте окно настройки параметров программы (на стр. 48).

2. В левой части окна в блоке **Контроль рабочего места** выберите раздел **Контроль устройств**.

   В правой части окна отобразятся параметры компонента Контроль устройств.

3. В правой части окна выберите закладку **Доверенные устройства**.

4. Выберите устройство из списка доверенных устройств, параметры которого вы хотите изменить.

5. Нажмите на кнопку **Изменить**.

   Откроется стандартное окно Microsoft Windows **Выбор пользователей или групп**.

6. Измените список пользователей и / или групп пользователей, для которых устройство является доверенным.

7. Нажмите на кнопку **OK**.

8. 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 (на стр. 48).
2. В левой части окна в блоке **Контроль рабочего места** выберите раздел **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 запрете операции над содержимым устройства. Если блокировка доступа к устройству или запрет операции с содержимым устройства, по мнению пользователя, произошла ошибочно, по ссылке из текста сообщения о блокировке пользователь может отправить жалобу администратору локальной сети организации.

Для сообщения о блокировке доступа к устройству или запрете операции над содержимым устройства и письма-жалобы предусмотрены шаблоны. Вы можете изменять шаблоны сообщений.

Чтобы изменить шаблон сообщений Контроля устройств, выполните следующие действия:

1. Откройте окно настройки параметров программы (на стр. 48).
2. В левой части окна в блоке **Контроль рабочего места** выберите раздел **Контроль устройств**.

   В правой части окна отобразятся параметры компонента Контроль устройств.
3. В правой части окна нажмите на кнопку **Шаблоны**.

   Откроется окно **Шаблоны**.
4. Выполните одно из следующих действий:

   - Если вы хотите изменить шаблон сообщения о блокировке доступа к устройству или запрете операции над содержимым устройства, выберите закладку **Блокировка**.
   - Если вы хотите изменить шаблон письма-жалобы администратору локальной сети организации, выберите закладку **Жалоба**.
5. Измените шаблон сообщения о блокировке или письма-жалобы. Для этого используйте кнопки **По умолчанию** и **Переменные**.
6. Нажмите на кнопку **ОК**.
7. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Получение доступа к заблокированному устройству

Пользователь может получить доступ к заблокированному устройству. Для этого нужно сделать запрос из окна настройки компонента Контроль устройств или по ссылке в сообщении о блокировке устройства.

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.

- *Чтобы получить доступ к заблокированному устройству из окна настройки компонента Контроль устройств, выполните следующие действия:*

1. Откройте окно настройки параметров программы (на стр. 48).
2. В левой части окна в блоке **Контроль рабочего места** выберите раздел **Контроль устройств**.

   В правой части окна отобразятся параметры компонента Контроль устройств.
3. Нажмите на кнопку **Запросить доступ**.

   Откроется окно **Запрос доступа к устройству**.
4. Выберите из списка подключенных устройств то устройство, к которому вы хотите получить доступ.
5. Нажмите на кнопку **Получить ключ доступа**.

   Откроется окно **Получение ключа доступа к устройству**.
6. В поле **Длительность доступа** укажите, на какое время вы хотите получить доступ к устройству.
7. Нажмите на кнопку **Сохранить**.

   Откроется стандартное окно Microsoft Windows **Сохранение ключа доступа**.
8. В окне Microsoft Windows **Сохранение ключа доступа** выберите папку, в которую вы хотите сохранить файл с ключом доступа к устройству, и нажмите на кнопку **Сохранить**.
9. Передайте файл с ключом доступа к устройству администратору локальной сети организации.
10. Получите от администратора локальной сети организации код доступа к устройству.
11. В окне **Запрос доступа к устройству** нажмите на кнопку **Активировать код доступа**.

    Откроется стандартное окно Microsoft Windows **Загрузка кода доступа**.
12. В окне Microsoft Windows **Загрузка кода доступа** выберите полученный от администратора локальной сети организации файл с кодом доступа к устройству и нажмите на кнопку **Открыть**.

    Откроется окно **Активация кода доступа к устройству** с информацией о предоставленном доступе.
13. В окне **Активация кода доступа к устройству** нажмите на кнопку **ОК**.

- *Чтобы получить 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 **Получение ключа доступа к устройству**.

2. В поле **Длительность доступа** укажите, на какое время вы хотите получить доступ к устройству.
3. Нажмите на кнопку **Сохранить**.

   Откроется стандартное окно Microsoft Windows **Сохранение ключа доступа**.
4. В окне Microsoft Windows **Сохранение ключа доступа** выберите папку, в которую вы хотите сохранить файл с ключом доступа к устройству, и нажмите на кнопку **Сохранить**.
5. Передайте файл с ключом доступа к устройству администратору локальной сети организации.
6. Получите от администратора локальной сети организации код доступа к устройству.
7. В окне **Запрос доступа к устройству** нажмите на кнопку **Активировать код доступа**.

   Откроется стандартное окно Microsoft Windows **Загрузка кода доступа**.
8. В окне Microsoft Windows **Загрузка кода доступа** выберите полученный от администратора локальной сети организации файл с кодом доступа к устройству и нажмите на кнопку **Открыть**.

   Откроется окно **Активация кода доступа к устройству** с информацией о предоставленном доступе.
9. В окне **Активация кода 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, которой администратор локальной сети организации указывает при формировании кода доступа к устройству.

Создание кода доступа к заблокированному устройству

Чтобы предоставить пользователю временный доступ к заблокированному устройству, требуется код доступа к заблокированному устройству. Код доступа к забловированному устройству вы можете создать на стороне Kaspersky Security Center.

Чтобы создать код доступа к заблокированному устройству, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые компьютеры** дерева консоли откройте папку с названием группы администрирования, в состав которой входит нужный вам клиентский компьютер.
3. В панели результатов выберите закладку **Компьютеры**.
4. В списке клиентских компьютеров выберите компьютер, пользователю которого вы хотите дать временный доступ к заблокированному устройству.
5. В контекстном меню компьютера выберите пункт **Доступ к устройствам и данным в автономном режиме**.

   Откроется окно **Предоставление доступа к устройствам и данным в автономном режиме**.
6. В окне **Предоставление доступа к устройствам и данным в автономном режиме** выберите закладку **Контроль устройств**.
7. На закладке **Контроль устройств** нажмите на кнопку **Обзор**.

Откроется стандартное окно Microsoft Windows **Выбор ключа доступа**.

8. В окне Microsoft Windows **Выбор ключа доступа** выберите файл с ключом доступа, 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**. Параметр определяет период времени, на который вы предоставляете пользователю доступ к заблокированному устройству.

   По умолчанию установлено значение, указанное пользователем при формировании ключа доступа.

10. Укажите значение параметра **Срок активации**. Параметр определяет период времени, в течение которого пользователь может активировать доступ к заблокированному устройству с помощью кода активации.

11. Нажмите на кнопку **Сохранить код доступа**.

    Откроется стандартное окно Microsoft Windows **Сохранение кода доступа**.

12. Выберите папку, в которую вы хотите сохранить файл с кодом 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. 20).

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 «Социальные сети»).

- Централизованное управление доступом к веб-ресурсам.

  При использовании Kaspersky Security Center доступны персональные и групповые настройки доступа к веб-ресурсам.

Все ограничения и запреты на доступ к веб-ресурсам реализуются в виде правил доступа к веб-ресурсам (см. раздел «О правилах доступа к веб-ресурсам» на стр. 161).

Включение и выключение Веб-Контроля

По умолчанию Веб-Контроль включен. Вы можете выключить Веб-Контроль при необходимости.

Включить и выключить компонент можно двумя способами:

- на закладке **Центр управления** главного окна программы (см. раздел «Главное окно программы» на стр. 46);
- из окна настройки параметров программы (см. раздел «Окно настройки параметров программы» на стр. 48).

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.

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

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

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

1. Откройте окно настройки параметров программы (на стр. 48).
2. В левой части окна в блоке **Контроль рабочего места** выберите раздел **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.

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 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. Предустановленны 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 **Правила доступа в порядке приоритета** окна настроек компонента Веб-Контроль. То есть правило, расположенное выше других правил в таблице **Правила доступа в порядке приоритета**, 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 сервиса «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 «Окно настройки параметров программы» на стр. 48)
2. В левой части окна в блоке **Контроль рабочего места** выберите раздел **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 **Правила доступа в порядке приоритета** 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**.

      Если выбран элемент, отличный от **Любое содержание**, откроется блок для выбора категорий содержания и / или категорий типа данных. Установите флажки напротив названий желаемых категорий содержания и / или категорий типа данных.

Установка флажка напротив названия категории содержания и / или категории типа данных означает, что Kaspersky Endpoint Security, в соответствии с правилом, контролирует доступ к веб-ресурсам, принадлежащим выбранным категориям содержания и / или категориям типа данных.

c. В раскрывающемся списке **Применять к адресам** выберите нужный элемент:

- **Ко всем адресам**.
- **К отдельным адресам**.

Если выбран элемент **К отдельным адресам**, откроется блок, в котором требуется создать список адресов веб-ресурсов. Вы можете создавать или изменять список адресов веб-ресурсов, используя кнопки **Добавить**, **Изменить**, **Удалить**.

d. Установите флажок **Укажите пользователей и / или группы** и нажмите на кнопку **Выбрать**.

Откроется стандартное окно Microsoft Windows **Выбор пользователей или групп**.

e. Задайте или измените список пользователей и / или групп пользователей, для которых разрешен или ограничен доступ к веб-ресурсам, описанным в правиле.

f. 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 параметрам правила, Kaspersky Endpoint Security выводит сообщение-предупреждение о возможной нежелательности веб-ресурса. По ссылкам из сообщения-предупреждения пользователь может получить доступ к запрошенному веб-ресурсу.

g. Из раскрывающегося списка **Расписание работы правила** выберите название нужного расписания или на основе выбранного расписания работы правила сформируйте новое расписание. 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 нажмите по ячейкам таблицы, соответствующим 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 нажмите по серым ячейкам таблицы, соответствующим нужному вам времени и дню недели.

   Цвет ячеек изменится на зеленый.

4. Нажмите на кнопку **ОК** или **Сохранить как**, если вы формируете расписание работы правила на основе расписания работы правила «Всегда», сформированного по умолчанию. Нажмите на кнопку **Сохранить как**, если вы формируете расписание работы правила на основе расписания работы правила, сформированного не по умолчанию.

   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 (на стр. 48).

2. В левой части окна в блоке **Контроль рабочего места** выберите раздел **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 предусмотрен сервис «Диагностика правил».

Чтобы проверить работу правил доступа к веб-ресурсам, выполните следующие действия:

1. Откройте окно настройки параметров программы (на стр. 48).

2. В левой части окна в блоке **Контроль рабочего места** выберите раздел **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-ресурсу(ам), 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(ам) (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 (на стр. 48).
2. В левой части окна в блоке **Контроль рабочего места** выберите раздел **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.

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 (на стр. 48).
2. В левой части окна в блоке **Контроль рабочего места** выберите раздел **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 (на стр. 48).
2. В левой части окна в блоке **Контроль рабочего места** выберите раздел **Веб-Контроль**.

   В правой части окна отобразятся параметры компонента Веб-Контроль.

3. Выполните одно из следующих действий:

   - Нажмите на кнопку **Добавить**, если вы хотите создать новое правило доступа к веб-ресурсам.
   - Выберите правило доступа к веб-ресурсам, которое вы хотите изменить. Далее нажмите на кнопку **Изменить**.

   Откроется окно **Правило доступа к веб-ресурсам**.

4. Выполните одно из следующих действий:

   - Если вы создаете новое правило доступа к веб-ресурсам, в раскрывающемся списке **Применять к адресам** выберите элемент **К отдельным адресам**.
   - Если вы изменяете правило доступа к веб-ресурсам, перейдите к пункту 5 инструкции.

5. Нажмите на кнопку  справа от поля со списком адресов веб-ресурсов.

   Если вы создаете новое правило, откроется стандартное окно Microsoft Windows **Открыть файл**.

   Если вы изменяете правило, откроется окно подтверждения действия.

6. Выполните одно из следующих действий:

   - Если вы создаете новое правило доступа к веб-ресурсам, перейдите к пункту 7 инструкции.
   - Если вы изменяете правило доступа к веб-ресурсам, в окне подтверждения действия выполните одно из следующих действий:

     - Если вы хотите добавить к существующим импортируемые элементы списка адресов веб-ресурсов, нажмите на кнопку **Да**.
     - Если вы хотите удалить существующие элементы списка адресов веб-ресурсов и добавить импортируемые, нажмите на кнопку **Нет**.

Откроется стандартное окно Microsoft Windows **Открыть файл**.

7. В окне Microsoft Windows **Открыть файл** выберите файл со списком адресов веб-ресурсов для импорта.
8. Нажмите на кнопку **Открыть**.
9. В окне **Правило доступа к веб-ресурсам** нажмите на кнопку **OK**.

Правила формирования масок адресов веб-ресурсов

Использование *маски адреса веб-ресурса* (далее также «маски адреса») может быть удобно в случаях, когда в процессе создания правила доступа к веб-ресурсам требуется ввести множество схожих адресов веб-ресурсов. Одна грамотно сформированная маска адреса может заменить множество адресов веб-ресурсов.

При формировании маски адреса следует иметь в виду 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.

   Символ ? трактуется как символ знака вопроса, а не любой один символ, как это принято в правилах формирования масок адресов в компоненте Веб-Антивирус.

   Для включения символа * в состав маски адреса нужно вводить два символа *, а не последовательность *, как это принято в правилах формирования масок адресов в компоненте Веб-Антивирус.

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. То есть для таких масок адреса не выполняются правила 5 и 7.

10. При сравнении с маской адреса веб-ресурса не учитываются имя пользователя и пароль, порт соединения и регистр символов.

Таблица 3. 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.
9	www.example.com	http://www.example.com/abc	Да	См. правила 2, 5, 1.
10	example.com	http://www.example.com	Да	См. правила 3, 1.
11	http://example.com/	http://example.com/abc	Да	См. правила 6.
12	http://example.com/*	http://example.com	Да	См. правило 7.
13	http://example.com	https://example.com	Нет	См. правило 8.
14	«example.com»	http://www.example.com	Нет	См. правило 9.
15	«http://www.example.com»	http://www.example.com/abc	Нет	См. правило 9.
16	«*.example.com»	http://www.example.com	Да	См. правила 1, 9.
17	«http://www.example.com/*»	http://www.example.com/abc	Да	См. правила 1, 9.
18	«www.example.com»	http://www.example.com; https://www.example.com	Да	См. правила 9, 8.
19	www.example.com/abc/123	http://www.example.com/abc	Нет	Маска адреса содержит больше информации, чем адрес веб-ресурса.

Изменение шаблонов сообщений Веб-Контроля

В зависимости от действия, заданного в свойствах правил Веб-Контроля, при попытке пользователей получить доступ к веб-ресурсам Kaspersky Endpoint Security выводит сообщение (подменяет ответ HTTP-сервера HTML-страницей с сообщением) одного из следующих типов:

- **Сообщение-предупреждение**. Такое сообщение предупреждает о возможной нежелательности веб-ресурса и / или несоответствии корпоративной политике. Kaspersky Endpoint Security выводит сообщение-предупреждение, если в свойствах правила, описывающего этот веб-ресурс, в раскрывающемся списке **Действие** выбран элемент **Предупреждать**.

  Если, на ваш взгляд, предупреждение ошибочно, по ссылке из сообщения-предупреждения вы можете открыть уже сформированное письмо-жалобу администратору локальной сети организации.

- **Сообщение о блокировке веб-ресурса**. Kaspersky Endpoint Security выводит сообщение о блокировке веб-ресурса, если в свойствах правила, которое описывает этот веб-ресурс, в раскрывающемся списке **Действие** выбран элемент **Запрещать**.

  Если, на ваш взгляд, доступ к веб-ресурсу был заблокирован ошибочно, по ссылке из сообщения о блокировке веб-ресурса вы можете открыть уже сформированное сообщение-жалобу администратору локальной сети организации.

Для сообщения-предупреждения, сообщения о блокировке доступа к веб-ресурсу и письма-жалобы 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 (на стр. 48).
2. В левой части окна в блоке **Контроль рабочего места** выберите раздел **Веб-Контроль**.

   В правой части окна отобразятся параметры компонента Веб-Контроль.
3. В правой части окна нажмите на кнопку **Шаблоны**.

   Откроется окно **Шаблоны**.
4. Выполните одно из следующих действий:

   - Если вы хотите изменить шаблон сообщения-предупреждения, предупреждающего о возможной нежелательности веб-ресурса, выберите закладку **Предупреждение**.
   - Если вы хотите изменить шаблон сообщения о блокировке доступа к веб-ресурсу, выберите закладку **Блокировка**.
   - Если вы хотите изменить шаблон письма-жалобы, выберите закладку **Жалоба**.
5. Измените шаблон сообщения. Для этого используйте кнопки **По умолчанию** и **Переменные**.
6. Нажмите на кнопку **ОК**.
7. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

ШИФРОВАНИЕ ДАННЫХ

Этот раздел содержит информацию о шифровании жестких дисков, съемных носителей и файлов на локальных дисках компьютера и инструкции о том, как настроить и выполнить шифрование данных с помощью Kaspersky Endpoint Security и плагина управления Kaspersky Endpoint Security.

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 показываемой функциональности** установите флажок **Отображать шифрование и защиту данных**.
4. Нажмите на кнопку **OK**.

О шифровании данных

Kaspersky Endpoint Security позволяет шифровать файлы, хранящиеся на локальных дисках компьютера и съемных носителях, съемные носители целиком и жесткие диски. Шифрование данных снижает риски непреднамеренной утечки информации в случае кражи / утери портативного компьютера, съемного носителя или жесткого диска, или при доступе к данным неавторизованных пользователей и программ.

Kaspersky Endpoint Security обеспечивает следующие направления защиты данных:

- **Шифрование файлов на локальных дисках компьютера**. Вы можете сформировать списки из файлов по расширению или группам расширений и папок, расположенных на локальных дисках компьютера, а также указать действие, согласно которому Kaspersky Endpoint Security шифрует файлы, создаваемые отдельными программами. После применения политики Kaspersky Security Center программа Kaspersky Endpoint Security шифрует и расшифровывает файлы, отдельно добавленные в списки для шифрования и расшифровки, файлы, хранящиеся в добавленных в списки для шифрования и расшифровки папках, а также файлы, создаваемые программами.

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

- **Шифрование данных на съемных носителях**. Вы можете указать правило шифрования по умолчанию, в соответствии с которым программа выполняет одинаковое действие по отношению ко всем съемным носителям и указать правила шифрования отдельных съемных носителей.

  Правило шифрования по умолчанию имеет меньший приоритет, чем правила шифрования, определенные для отдельных съемных носителей. Правила шифрования, определенные для съемных носителей с указанной моделью устройства, имеют меньший приоритет, чем правила шифрования, определенные для съемных носителей с указанным идентификатором устройства.

  Чтобы выбрать правило шифрования файлов на съемном носителе, Kaspersky Endpoint Security проверяет, известны ли модель устройства и его идентификатор. Далее программа выполняет одно из следующих действий:

  - Если известна модель устройства, программа применяет правило шифрования, определенное для съемных носителей с известной моделью устройства, если такое правило есть. В противном случае программа применяет правило шифрования по умолчанию.

  - Если известен идентификатор устройства, программа применяет правило шифрования, определенное для съемных носителей с известным идентификатором устройства, если такое правило есть. В противном случае программа применяет правило шифрования по умолчанию.

  - Если известны и модель устройств, и идентификатор устройства, программа применяет правило шифрования, определенное для съемных носителей с известным идентификатором устройства, если такое правило есть. В противном случае программа применяет правило шифрования, определенное для съемных носителей с известной моделью устройства. Если для съемных носителей с известной моделью устройства не задано правило шифрования, программа применяет правило шифрования по умолчанию.

  - Если неизвестны ни модель устройства, ни идентификатор устройства, программа применяет правило шифрования по умолчанию.

  Программа позволяет подготовить съемный носитель для работы с зашифрованными на нем файлами в портативном режиме. После включения портативного режима становится доступной работа с зашифрованными файлами на съемных носителях, подключенных к компьютеру с недоступной функциональностью шифрования.

  Программа выполняет указанное в правиле шифрования действие при применении политики Kaspersky Security Center.

В случае истечения срока действия лицензии, нарушения Лицензионного соглашения, удаления ключа или удаления программы Kaspersky Endpoint Security 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 на компьютере функциональности шифрования файлов файл остается незашифрованным.

- **Управление правами доступа программ к зашифрованным файлам**. Для любой программы вы можете определить правило доступа к зашифрованным файлам, запрещающее доступ к зашифрованным файлам или разрешающее доступ к зашифрованным файлам только в виде шифротекста.

- **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 архивы. Такие архивы можно безопасно передавать по сети или на съемных носителях.

- **Шифрование жестких дисков**. 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 посекторно, при применении политики Kaspersky Security Center. Подробнее о применении политики Kaspersky Security Center вы можете прочитать в *Руководстве администратора для Kaspersky Security Center.* Программа шифрует сразу все логические разделы жестких дисков.

  После шифрования жестких дисков при последующем входе в операционную систему доступ к ним, а также загрузка операционной системы возможны только после прохождения процедуры аутентификации с помощью агента аутентификации. Для этого требуется ввести имя и пароль, которые установлены для учетной записи пользователя системным администратором локальной сети организации с помощью задач управления учетными записями агента аутентификации, запущенных из Kaspersky Security Center. 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 логина 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 зашифрованы, Kaspersky Endpoint Security формирует дубликаты учетных записей агента аутентификации. Для их удаления требуется использовать утилиту klmover с ключом -dupfix. Утилита klmover поставляется со сборкой Kaspersky Security Center. Подробнее о ее работе читайте в *Руководстве администратора для Kaspersky Security Center*.

  Доступ к зашифрованным жестким дискам возможен только с компьютеров, на которых установлена программа Kaspersky Endpoint Security с доступной функциональностью шифрования жестких дисков. Это условие сводит к минимуму вероятность утечки информации, хранящейся на зашифрованном жестком диске, при использовании зашифрованного жесткого диска вне локальной сети организации.

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 файлам или съемным носителям у администратора локальной сети организации.

- Восстановить доступ к зашифрованным устройствам 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 Сервером администрирования, под управлением которого оказался компьютер с зашифрованными объектами.

В процессе шифрования программа создает служебные файлы. Для их хранения требуется свободное пространство на жестком диске компьютера. Если свободного пространства на жестком диске недостаточно, то шифрование не запускается до тех пор, пока вы не освободите пространство на жестком диске.

См. также

Получение доступа к зашифрованным файлам при отсутствии связи с Kaspersky Security Center 186

Получение и активация ключа доступа к зашифрованным съемным носителям 203

Восстановление доступа к зашифрованному жесткому диску или съемному носителю с помощью утилиты восстановления 204

Смена алгоритма шифрования

Алгоритм шифрования, который Kaspersky Endpoint Security использует для шифрования данных, зависит от установленного модуля шифрования.

Чтобы сменить алгоритм шифрования, выполните следующие действия:

1. Расшифруйте объекты, которые программа Kaspersky Endpoint Security зашифровала до начала процедуры смены алгоритма шифрования.

   В противном случае не гарантируется работа с объектами, зашифрованными с помощью алгоритма шифрования, который вы хотите сменить.

2. Удалите модуль шифрования (см. раздел «Удаление модуля шифрования» на стр. 44).

3. Установите другой модуль шифрования (см. раздел «Установка модуля шифрования» на стр. 36).

Особенности функциональности шифрования файлов

При использовании функциональности шифрования съемных носителей и файлов на локальных дисках компьютера следует иметь в виду следующие особенности:

- Политика Kaspersky Security Center с заданными параметрами шифрования съемных носителей формируется для определенной группы управляемых компьютеров. Поэтому результат применения политики шифрования / расшифровки съемных носителей зависит от того, к какому компьютеру подключен съемный носитель.

- Kaspersky Endpoint Security не выполняет шифрование / расшифровку файлов со статусом доступа «только чтение», хранящихся на съемных носителях.

- 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 в ней 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 носителей поддерживаются следующие типы устройств:
  - съемные носители, 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. 20).

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

Шифрование 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 компьютеры** дерева консоли 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 вам политику в списке политик.
5. Выполните одно из следующих действий:
   - По правой клавише мыши вызовите контекстное меню политики. Выберите пункт **Свойства**.
   - Нажмите на ссылку **Изменить параметры политики** справа от списка политик.

   Откроется окно **Свойства: <Название политики>**.
6. Выберите раздел **Шифрование файлов и папок**.
7. В правой части окна выберите закладку **Шифрование**.
8. В раскрывающемся списке **Правила шифрования по умолчанию** выберите элемент **Согласно правилам**.
9. На закладке **Шифрование** по левой кнопке мыши вызовите контекстное меню кнопки **Добавить**:
   a. Выберите пункт **Стандартные папки** контекстного меню кнопки **Добавить**, чтобы добавить в список для шифрования файлы из папок, предложенных специалистами «Лаборатории Касперского».

      Откроется окно **Выбор стандартных папок**. Окно содержит список папок локальных профилей пользователей, предложенных для шифрования специалистами «Лаборатории Касперского».

   b. Выберите пункт **Папку вручную** контекстного меню кнопки **Добавить**, чтобы добавить в список для шифрования папку, путь к которой введен вручную.

      Откроется окно **Добавление папки вручную**.

   c. Выберите пункт **Файлы по расширению** контекстного меню кнопки **Добавить**, чтобы в список для шифрования добавить расширения файлов. Kaspersky Endpoint Security шифрует файлы указанных расширений на всех локальных дисках компьютера.

      Откроется окно **Добавление / изменение списка расширений файлов**.

   d. Выберите пункт **Файлы по группе(ам) расширений** контекстного меню кнопки **Добавить**, чтобы в список для шифрования добавить группы расширений файлов. Kaspersky Endpoint Security шифрует файлы расширений, перечисленных в группах расширений.

      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 список для шифрования и не включенные в список для расшифровки (см. раздел «Формирование списка файлов для расшифровки» на стр. 177).

Если один и тот же файл добавлен и в список для шифрования, и в список для 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 параметры (путь к файлу / название файла / расширение файла) изменяются и удовлетворяют в результате параметрам объектов, добавленных в список для шифрования.

Kaspersky Endpoint Security откладывает шифрование открытых файлов до тех пор, пока они не будут закрыты.

Когда пользователь создает новый файл, параметры которого удовлетворяют параметрам объектов, добавленных в список для 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 список для шифрования.

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 компьютеры** дерева консоли 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 в списке политик.
5. Выполните одно из следующих действий:
   - По правой клавише мыши вызовите контекстное меню политики. Выберите пункт **Свойства**.
   - Нажмите на ссылку **Изменить параметры политики** справа от списка политик.

   Откроется окно **Свойства: <Название политики>**.
6. Выберите раздел **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 списка файлов для расшифровки» на стр. 177).
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 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.

Формирование списка файлов для расшифровки

Чтобы сформировать список файлов для расшифровки, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые компьютеры** дерева консоли 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 в списке политик.
5. Выполните одно из следующих действий:
   - По правой клавише мыши вызовите контекстное меню политики. Выберите пункт **Свойства**.
   - Нажмите на ссылку **Изменить параметры политики** справа от списка политик.

   Откроется окно **Свойства: <Название политики>**.
6. Выберите раздел **Шифрование файлов и папок**.
7. В правой части окна выберите закладку **Расшифровка**.
8. В раскрывающемся списке **Правила шифрования по умолчанию** выберите элемент **Согласно правилам**.
9. На закладке **Расшифровка** по левой кнопке мыши вызовите контекстное меню кнопки **Добавить**:
   a. Выберите пункт **Стандартные папки** контекстного меню кнопки **Добавить**, чтобы добавить в список для расшифровки файлы из папок, предложенных специалистами «Лаборатории Касперского».

      Откроется окно **Выбор стандартных папок**.
   b. Выберите пункт **Папку вручную** контекстного меню кнопки **Добавить**, чтобы добавить в список для расшифровки папку, путь к которой введен вручную.

      Откроется окно **Добавление папки вручную**.
   c. Выберите пункт **Файлы по расширению** контекстного меню кнопки **Добавить**, чтобы в список для расшифровки добавить расширения файлов. Kaspersky Endpoint Security не шифрует файлы указанных расширений на всех локальных дисках компьютера.

      Откроется окно **Добавление / изменение списка расширений файлов**.
   d. Выберите пункт **Файлы по группе(ам) расширений** контекстного меню кнопки **Добавить**, чтобы в список для расшифровки добавить группы расширений файлов. Kaspersky Endpoint Security не шифрует файлы расширений, перечисленных в группах расширений.

Откроется окно **Выбор групп расширений файлов**.

10. В окне **Свойства: <Название политики>** нажмите на кнопку **OK**, чтобы сохранить внесенные изменения.

Если один и тот же файл добавлен и в список для шифрования, и в список для расшифровки, то Kaspersky Endpoint Security не шифрует этот файл, если он не зашифрован, и расшифровывает, если он зашифрован.

Шифрование съемных носителей

Шифрование съемных носителей доступно, если программа Kaspersky Endpoint Security установлена на компьютере под управлением операционной системы Microsoft Windows для рабочих станций. Шифрование съемных носителей 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. 20).

Этот раздел содержит информацию о шифровании съемных носителей и инструкции о том, как настроить и выполнить шифрование съемных носителей с помощью Kaspersky Endpoint Security и плагина управления Kaspersky Endpoint Security.

В этом разделе

Шифрование съемных носителей

Чтобы зашифровать съемные носители, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые компьютеры** дерева консоли откройте папку с названием группы администрирования, для которой вы хотите настроить шифрование съемных носителей.
3. В рабочей области выберите закладку **Политики**.
4. Выберите нужную вам политику в списке политик.
5. Выполните одно из следующих действий:
   - По правой клавише мыши вызовите контекстное меню политики. Выберите пункт **Свойства**.
   - Нажмите на ссылку **Изменить параметры политики** справа от списка политик.

   Откроется окно **Свойства: <Название политики>**.
6. Выберите раздел **Шифрование съемных носителей**.

7. В раскрывающемся списке **Правило по умолчанию** выберите действие, которое по умолчанию выполняет Kaspersky Endpoint Security со всеми съемными носителями, подключаемыми к компьютерам из выбранной группы администрирования:

   - **Шифровать весь носитель**. Если выбран этот вариант, то при применении политики Kaspersky Security Center с заданными параметрами шифрования съемных носителей Kaspersky Endpoint Security посекторно шифрует содержимое съемных носителей. Таким образом, зашифрованными оказываются не только файлы, которые хранятся на съемном носителях, но и файловые системы съемных носителей, включая имена файлов и структуры папок на съемных носителях. Уже зашифрованные съемные носители Kaspersky Endpoint Security повторно не шифрует.

     Этот вариант шифрования обеспечивается функциональностью шифрования жестких дисков программы Kaspersky Endpoint Security.

   - **Шифровать все файлы**. Если выбран этот вариант, то при применении политики Kaspersky Security Center с заданными параметрами шифрования съемных носителей Kaspersky Endpoint Security шифрует все файлы, которые хранятся на съемных носителях. Уже зашифрованные файлы Kaspersky Endpoint Security повторно не шифрует. Программа не шифрует файловые системы съемных носителей, включая имена зашифрованных файлов и структуры папок.

   - **Шифровать только новые файлы**. Если выбран этот вариант, то при применении политики Kaspersky Security Center с заданными параметрами шифрования съемных носителей Kaspersky Endpoint Security шифрует только те файлы, которые были добавлены на съемные носители или которые хранились на съемных носителях и были изменены после последнего применения политики Kaspersky Security Center.

   - **Расшифровывать весь носитель**. Если выбран этот вариант, то при применении политики Kaspersky Security Center с заданными параметрами шифрования съемных носителей Kaspersky Endpoint Security расшифровывает все зашифрованные файлы, которые хранятся на съемных носителях, 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 вариант, то при применении политики Kaspersky Security Center с заданными параметрами шифрования съемных носителей Kaspersky Endpoint Security не шифрует и не расшифровывает файлы на съемных носителях.

8. Сформируйте (см. раздел «Добавление правил шифрования для съемных носителей» на стр. 180) правила шифрования файлов на съемных носителях, 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 носитель или съемный носитель уже подключен, Kaspersky Endpoint Security информирует пользователя о том, что к съемному носителю применяется правило шифрования, в соответствии с которым данные съемного носителя будут зашифрованы.

Если для шифрования данных на съемном носителе 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 носителя чтением.

- Оставляет данные незашифрованными, если пользователь не дает ответ на запрос на шифрование, ограничивает доступ к файлам съемного носителя чтением и повторно запрашивает подтверждение шифрования данных при последующем применении политики Kaspersky Security Center или при последующем подключении съемного носителя.

Политика Kaspersky Security Center с заданными параметрами шифрования данных съемных носителей формируется для определенной группы управляемых компьютеров. Поэтому результат шифрования данных съемных носителей зависит от того, к какому компьютеру подключен съемный носитель.

Если во время шифрования данных пользователь инициирует безопасное извлечение съемного носителя, Kaspersky Endpoint Security прерывает шифрование данных и позволяет извлечь съемный носитель до завершения операции шифрования.

Добавление правил шифрования для съемных носителей

Чтобы добавить правила шифрования для съемных носителей, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.

2. В папке **Управляемые компьютеры** дерева консоли откройте папку с названием группы администрирования, для которой вы хотите добавить правила шифрования для съемных носителей.

3. В рабочей области выберите закладку **Политики**.

4. Выберите нужную вам политику в списке политик.

5. Выполните одно из следующих действий:

   - По правой клавише мыши вызовите контекстное меню политики. Выберите пункт **Свойства**.

   - Нажмите на ссылку **Изменить параметры политики** справа от списка политик.

   Откроется окно **Свойства: <Название политики>**.

6. Выберите раздел **Шифрование съемных носителей**.

7. Выполните следующие действия:

   - По левой кнопке мыши вызовите контекстное меню кнопки **Добавить** и выберите пункт **Из списка доверенных устройств данной политики**, чтобы добавить правила шифрования для съемных носителей, которые находятся в списке доверенных устройств компонента Контроль устройств.

     Откроется окно **Добавление устройств из списка доверенных устройств**.

     Выполните следующие действия:

     a. В графе **Тип устройств** установите флажки напротив названий тех съемных носителей в таблице, для которых вы хотите создать правила шифрования.

     b. В раскрывающемся списке **Правило шифрования для выбранных устройств** выберите действие, которое выполняет Kaspersky Endpoint Security с файлами, хранящимися на выбранных съемных носителях.

     c. Установите флажок **Портативный режим**, если вы хотите, чтобы перед шифрованием Kaspersky Endpoint Security выполнял подготовку съемных носителей к работе с зашифрованными на них файлами в портативном режиме. Портативный режим позволяет работать с зашифрованными файлами съемных носителей на компьютерах с недоступной функциональностью шифрования.

d. В раскрывающемся списке **Действие для устройств, выбранных ранее** выберите действие, которое выполняет Kaspersky Endpoint Security с правилами шифрования, которые были определены для съемных носителей ранее.

e. Нажмите на кнопку **OK**.

Записи с параметрами созданных правил шифрования отобразятся в таблице **Правила, заданные вручную**.

- По левой кнопке мыши вызовите контекстное меню кнопки **Добавить** и выберите пункт **Из списка устройств Kaspersky Security Center**, чтобы добавить правила шифрования для съемных носителей, которые находятся в списке Kaspersky Security Center.

  Откроется окно **Добавление устройств из списка Kaspersky Security Center**.

  Выполните следующие действия:

  a. Задайте фильтры для вывода списка устройств в таблице. Для этого укажите значения параметров **Выводить в таблице устройства, для которых определено**, **Тип устройства**, **Название**, **Компьютер**.

  b. Нажмите на кнопку **Обновить**.

  c. В графе **Тип устройств** установите флажки напротив названий тех съемных носителей, для которых вы хотите создать правила шифрования.

  d. В раскрывающемся списке **Правило шифрования для выбранных устройств** выберите действие, которое выполняет Kaspersky Endpoint Security с файлами, хранящимися на выбранных съемных носителях.

  e. Установите флажок **Портативный режим**, если вы хотите, чтобы перед шифрованием Kaspersky Endpoint Security выполнял подготовку съемных носителей к работе с зашифрованными на них файлами в портативном режиме. Портативный режим позволяет работать с зашифрованными файлами съемных носителей на компьютерах с недоступной функциональностью шифрования.

  f. В раскрывающемся списке **Действие для устройств, выбранных ранее** выберите действие, которое выполняет Kaspersky Endpoint Security с правилами шифрования, которые были определены для съемных носителей ранее.

  g. Нажмите на кнопку **OK**.

  Записи с параметрами созданных правил шифрования отобразятся в таблице **Правила, заданные вручную**.

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

Добавленные правила шифрования съемных носителей будут применены к съемным носителям, подключенным к любым компьютерам, работающим под управлением измененной политики Kaspersky Security Center.

Изменение правил шифрования для съемных носителей

Чтобы изменить правило шифрования для съемного носителя, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.

2. В папке **Управляемые компьютеры** дерева консоли откройте папку с названием группы администрирования, для которой вы хотите изменить правило шифрования для съемного носителя.

3. В рабочей области выберите закладку **Политики**.

4. Выберите нужную вам политику в списке политик.

5. Выполните одно из следующих действий:

   - По правой клавише мыши вызовите контекстное меню политики. Выберите пункт **Свойства**.
   - Нажмите на ссылку **Изменить параметры политики** справа от списка политик.

   Откроется окно **Свойства: <Название политики>**.

6. Выберите раздел **Шифрование съемных носителей**.
7. В списке съемных носителей, для которых определены правила шифрования, выберите запись о нужном вам съемном носителе.
8. Нажмите на кнопку **Задать правило**, чтобы изменить правило шифрования для этого съемного носителя.

   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 носителе.
10. Нажмите на кнопку **OK**, чтобы сохранить внесенные изменения.

Измененные правила шифрования съемных носителей будут применены к съемным носителям, подключенным к любым компьютерам, работающим под управлением измененной политики Kaspersky Security Center.

Расшифровка съемных носителей

Чтобы расшифровать съемные носители, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые компьютеры** дерева консоли откройте папку с названием группы администрирования, для которой вы хотите настроить расшифровку съемных носителей.
3. В рабочей области выберите закладку **Политики**.
4. Выберите нужную вам политику в списке политик.
5. Выполните одно из следующих действий:

   - По правой клавише мыши вызовите контекстное меню политики. Выберите пункт **Свойства**.
   - Нажмите на ссылку **Изменить параметры политики** справа от списка политик.

   Откроется окно **Свойства: <Название политики>**.

6. Выберите раздел **Шифрование съемных носителей**.
7. Если вы хотите расшифровать все зашифрованные файлы, хранящиеся на съемных носителях, в раскрывающемся списке **Правило по умолчанию** выберите действие **Расшифровывать весь носитель**.
8. Если вы хотите расшифровать данные, хранящиеся на отдельных съемных носителях, измените правила шифрования съемных носителей, данные которых вы хотите расшифровать. Для этого выполните следующие действия:

   a. В списке съемных носителей, для которых определены правила шифрования, выберите запись о нужном вам съемном носителе.

b. Нажмите на кнопку **Задать правило**, чтобы изменить правило шифрования для этого съемного носителя.

   Откроется контекстное меню кнопки **Задать правило**.

c. В контекстном меню кнопки **Задать правило** выберите пункт **Расшифровывать все файлы**.

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.*

Сразу после применения политики, если пользователь подключает съемный носитель или съемный носитель уже подключен, Kaspersky Endpoint Security информирует пользователя о том, что к съемному носителю применяется правило шифрования, в соответствии с которым зашифрованные файлы, хранящиеся на съемном носителе, а также файловая система съемного носителя, 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 носителях формируется для определенной группы управляемых компьютеров. Поэтому результат расшифровки данных на съемных носителях зависит от того, к какому компьютеру подключен съемный носитель.

Если во время расшифровки данных пользователь инициирует безопасное извлечение съемного носителя, Kaspersky Endpoint Security прерывает расшифровку данных и позволяет извлечь съемный носитель до завершения операции расшифровки.

Включение портативного режима для работы с зашифрованными файлами на съемных носителях

Чтобы включить портативный режим для работы с зашифрованными файлами на съемных носителях, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.

2. В папке **Управляемые компьютеры** дерева консоли откройте папку с названием группы администрирования, для которой вы хотите включить портативный режим для работы с зашифрованными файлами на съемных носителях.

3. В рабочей области выберите закладку **Политики**.

4. Выберите нужную вам политику в списке политик.

5. Выполните одно из следующих действий:

   - По правой клавише мыши вызовите контекстное меню политики. Выберите пункт **Свойства**.
   - Нажмите на ссылку **Изменить параметры политики** справа от списка политик.

   Откроется окно **Свойства: <Название политики>**.

6. Выберите раздел **Шифрование съемных носителей**.

7. Установите флажок **Портативный режим**.

   Портативный режим доступен только для шифрования всех или только новых файлов.

8. Нажмите на кнопку **OK**.

9. Примените политику.

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

После включения портативного режима становится доступной работа с зашифрованными файлами на съемных носителях, подключенных к компьютеру с недоступной функциональностью 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 компьютеры** дерева консоли 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 вам политику в списке политик.
5. Выполните одно из следующих действий:
   - По правой клавише мыши вызовите контекстное меню политики. Выберите пункт **Свойства**.
   - Нажмите на ссылку **Изменить параметры политики** справа от списка политик.

   Откроется окно **Свойства: <Название политики>**.
6. Выберите раздел **Шифрование файлов и папок**.
7. В правой части окна выберите закладку **Правила для программ**.
8. Если вы хотите для формирования правил доступа программ к зашифрованным файлам выбрать программы из списка Kaspersky Security Center, по левой кнопке мыши вызовите контекстное меню кнопки **Добавить** и выберите пункт **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**, **Группа**, **Период добавления**.

   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 **Правила для программ(ы)** выберите правило, которое будет определять доступ программ к зашифрованным файлам, или действие, которое будет выполнять Kaspersky Endpoint Security над файлами, которые создают эти программы.

   e. В раскрывающемся списке **Действие для программ, выбранных ранее** выберите действие, которое выполняет Kaspersky Endpoint Security над правилами доступа программ 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**.

9. Если вы хотите для формирования правил доступа программ к зашифрованным файлам выбрать программы вручную, по левой кнопке мыши вызовите контекстное меню кнопки **Добавить** и выберите пункт **Программы вручную**.

   Откроется окно **Добавление / изменение списка названий исполняемых файлов программ**.

   Выполните следующие действия:

   a. В поле ввода введите название или список названий исполняемых файлов программ с их расширениями. Нажмите на кнопку **Добавить из списка Kaspersky Security Center**, если вы хотите добавить названия исполняемых файлов программ из списка Kaspersky Security Center.

   b. В поле **Описание** введите описание списка программ.

   c. В раскрывающемся списке **Правила для программ(ы)** выберите правило, которое будет определять доступ программ к зашифрованным файлам, или действие, которое будет выполнять Kaspersky Endpoint Security над файлами, которые создают эти программы.

   d. Нажмите на кнопку **OK**.

   Информация о правиле доступа программ к зашифрованным файлам отобразится в таблице на закладке **Правила для программ**.

10. Нажмите на кнопку **OK**, чтобы сохранить внесенные изменения.

Работа с зашифрованными файлами при ограниченной функциональности шифрования файлов

Функциональность шифрования файлов может быть ограничена в следующих случаях:

- На компьютере пользователя присутствуют зашифрованные ключи для доступа к зашифрованным файлам, но нет связи с Kaspersky Security Center для работы с ключами. В этом случае для получения доступа к зашифрованным файлам пользователю требуется запросить доступ к зашифрованным файлам у администратора локальной сети организации.

- Функциональность шифрования недоступна по действующей лицензии или выявлены проблемы, связанные с лицензированием. В этом случае требуется активировать программу по новой лицензии, которая допускает использование функциональности шифрования файлов.

  Если срок действия лицензии истек, то программа не шифрует новые данные, а старые зашифрованные данные остаются зашифрованными и доступными для работы.

- С компьютера пользователя удалена программа Kaspersky Endpoint Security. Доступ к зашифрованным файлам на локальных дисках и съемных носителях в этом случае открыт, но содержимое файлов отображается как зашифрованное. Пользователь может работать с файлами, помещенными в зашифрованные архивы (см. раздел «Создание зашифрованных архивов» на стр. 188), созданные на компьютере с установленной программой Kaspersky Endpoint Security, а также с файлам, хранящимися на съемных носителях, для которых разрешена работа в портативном режиме (см. раздел «Включение портативного режима для работы с зашифрованными файлами на съемных носителях» на стр. 183).

В этом разделе

Получение доступа к зашифрованным файлам при отсутствии связи с Kaspersky Security Center

При применении политики Kaspersky Security Center и последующем шифровании файлов Kaspersky Endpoint Security получает ключ доступа к зашифрованным файлам. С помощью этого ключа пользователь, работающий под любой из учетных записей Windows, которая была активной во время шифрования файлов, может получать прямой доступ к зашифрованным файлам. Для доступа к зашифрованным файлам пользователям, работающим под учетными записями Windows, которые были неактивны во время шифрования файлов, требуется связь с Kaspersky Security Center. При ее отсутствии для доступа к зашифрованным файлам на локальных дисках компьютера пользователю требуется запросить один ключ доступа, для доступа к зашифрованным файлам на съемных носителях пользователю требуется запросить ключ доступа к зашифрованным файлам для каждого съемного носителя.

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 носителе, если вы обратились к файлу, хранящемуся на съемном носителе. 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 способом, отличным от передачи по электронной почте.

3. Получите файл ключа доступа к зашифрованным файлам, созданный и переданный (см. раздел «Создание и передача пользователю файла ключа доступа к зашифрованным файлам» на стр. 187) 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. По ссылке **Существуют активные запросы** откройте окно **Статус доступа к файлам и устройствам**. В окне отображается список всех запросов доступа к зашифрованным файлам.

c. В окне **Статус доступа к файлам и устройствам** выберите номер запроса, для которого вы получили файл ключа доступа к зашифрованным файлам.

d. Нажмите на кнопку **Обзор**, чтобы загрузить полученный файл ключа доступа к зашифрованным файлам.

   Откроется стандартное окно Microsoft Windows **Выбор файла ключа доступа**.

e. 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 файла выбранного запроса доступа к зашифрованным файлам.

f. Нажмите на кнопку **Открыть**.

g. В окне **Статус доступа к файлам и устройствам** 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 носителе, если файл запроса доступа к зашифрованным файлам был сформирован при обращении к файлу, хранящемуся на съемном носителе. Для получения доступа к зашифрованным файлам, хранящимся на других съемных носителях, требуется получить отдельный файл ключа доступа для этих съемных носителей.

Создание и передача пользователю файла ключа доступа к зашифрованным файлам

Чтобы создать и передать пользователю файл ключа доступа к зашифрованным файлам, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.

2. В папке **Управляемые компьютеры** дерева консоли откройте папку с названием группы администрирования, к которой принадлежит компьютер пользователя, запросившего доступ к зашифрованным файлам.

3. В рабочей области выберите закладку **Компьютеры**.

4. На закладке **Компьютеры** выделите в списке компьютер пользователя, запросившего доступ к зашифрованным файлам, и по правой клавише мыши откройте контекстное меню.

5. В контекстном меню выберите пункт **Доступ к устройствам и данным в автономном режиме**.

   Откроется окно **Предоставление доступа к устройствам и данным в автономном режиме**.

6. В окне **Предоставление доступа к устройствам и данным в автономном 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, запросившего доступ к зашифрованным файлам, и нажмите на кнопку **Открыть**.

   Kaspersky Security Center формирует 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 способом, отличным от передачи по электронной почте.

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 носителе. 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 носителе 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.

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 компьютеры** дерева консоли 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 в списке политик.

5. Выполните одно из следующих действий:

   - По правой клавише мыши вызовите контекстное меню политики. Выберите пункт **Свойства**.

   - Нажмите на ссылку **Изменить параметры политики** справа от списка политик.

   Откроется окно **Свойства: <Название политики>**.

6. Выберите раздел **Общие параметры шифрования**.

7. В блоке **Шаблоны н**ажмите на кнопку **Сообщения**.

   Откроется окно **Шаблоны**.

8. Выполните следующие действия:

   - Если вы хотите изменить шаблон почтового 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**. По нажатию на кнопку **Отправить по почте** окна **Доступ к файлу запрещен** автоматически формируется почтовое сообщение пользователя. Это сообщение пользователь отправляет администратору локальной сети организации вместе с файлом запроса доступа к зашифрованным файлам.

- Если вы хотите изменить шаблон почтового сообщения администратора, выберите закладку **Сообщение администратора**. Это почтовое сообщение автоматически формируется по нажатию на кнопку **Отправить по почте** окна **Предоставление доступа к зашифрованным файлам** и приходит к пользователю после предоставления ему доступа к зашифрованным файлам.

9. Измените шаблоны сообщений. Для этого используйте кнопки **По умолчанию** и **Переменные**.

10. Нажмите на кнопку **OK**.

11. В окне **Свойства: <Название политики>** нажмите на кнопку **OK**, чтобы сохранить внесенные изменения.

Шифрование жестких дисков

Шифрование жестких дисков доступно, если программа Kaspersky Endpoint Security установлена на компьютере под управлением операционной системы Microsoft Windows для рабочих станций. Шифрование жестких 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. 20).

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

Шифрование жестких дисков

Перед шифрованием жестких дисков компьютера настоятельно рекомендуем убедиться в том, что компьютер не заражен. Для этого запустите полную проверку или проверку важных областей компьютера (см. раздел «Проверка компьютера» на стр. 220). Шифрование жесткого диска компьютера, зараженного руткитом, может привести к неработоспособности компьютера.

Чтобы зашифровать жесткие диски, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.

2. В папке **Управляемые компьютеры** дерева консоли откройте папку с названием группы администрирования, для которой вы хотите настроить шифрование жестких дисков.

3. В рабочей области выберите закладку **Политики**.

4. Выберите нужную вам политику в списке политик.

5. Выполните одно из следующих действий:

   - По правой клавише мыши вызовите контекстное меню политики. Выберите пункт **Свойства**.

   - Нажмите на ссылку **Изменить параметры политики** справа от списка политик.

   Откроется окно **Свойства: <Название политики>**.

6. Выберите раздел **Шифрование жестких дисков**.

7. В раскрывающемся списке **Правило шифрования по умолчанию** выберите действие, которое по умолчанию выполняет Kaspersky Endpoint Security с жесткими дисками:

   - **Шифровать все жесткие диски**. Если выбран этот вариант, то при применении политики Kaspersky Security Center программа шифрует все жесткие диски.

   - **Расшифровывать все жесткие диски**. Если выбран этот вариант, то при применении политики Kaspersky Security Center программа расшифровывает все зашифрованные жесткие диски.

   - **Оставлять без изменений**. Если выбран этот вариант, то при применении политики Kaspersky Security Center программа не шифрует и не расшифровывает жесткие диски.

8. Сформируйте (см. раздел «Формирование списка жестких дисков для исключения из шифрования» на стр. 192) список жестких дисков, которые вы не хотите шифровать.

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.*

После старта задачи шифрования жестких дисков Kaspersky Endpoint Security шифрует все, что записывается на жесткие диски.

Если во время выполнения задачи 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 выполнения задачи 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 выполнения задачи 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.

Формирование списка жестких дисков для исключения из шифрования

Чтобы сформировать список жестких дисков для исключения из шифрования, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые компьютеры** дерева консоли 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 вам политику в списке политик.
5. Выполните одно из следующих действий:
   - По правой клавише мыши вызовите контекстное меню политики. Выберите пункт **Свойства**.
   - Нажмите на ссылку **Изменить параметры политики** справа от списка политик.

   Откроется окно **Свойства: <Название политики>**.
6. Выберите раздел **Шифрование жестких дисков**.

   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.
7. 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** задайте фильтры для вывода списка устройств в таблице. Для этого укажите значения параметров **Название**, **Компьютер**.
   c. Нажмите на кнопку **Обновить**.
   d. В графе **Тип устройств** установите флажки напротив названий тех жестких дисков в таблице, которые вы хотите добавить в список жестких дисков для исключения из шифрования.
   e. Нажмите на кнопку **OK**.

   Записи о выбранных жестких дисках отобразятся в таблице **Не шифровать следующие жесткие диски**.
8. Если вы хотите удалить записи о жестких дисках, добавленных в список жестких дисков для исключения из шифрования, выберите одну или несколько записей в таблице **Не шифровать следующие жесткие диски** и нажмите на кнопку **Удалить**.

   Чтобы выбрать несколько записей в таблице, выделяйте их, удерживая клавишу **CTRL**.
9. Нажмите на кнопку **OK**, чтобы сохранить внесенные изменения.

Расшифровка жестких дисков

Чтобы расшифровать жесткие диски, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые компьютеры** дерева консоли откройте папку с названием группы администрирования, для которой вы хотите настроить расшифровку жестких дисков.
3. В рабочей области выберите закладку **Политики**.
4. Выберите нужную вам политику в списке политик.
5. Выполните одно из следующих действий:
   - По правой клавише мыши вызовите контекстное меню политики. Выберите пункт **Свойства**.
   - Нажмите на ссылку **Изменить параметры политики** справа от списка политик.

   Откроется окно **Свойства: <Название политики>**.
6. Выберите раздел **Шифрование жестких дисков**.
7. Выполните одно из следующих действий:
   - В раскрывающемся списке **Правило шифрования по умолчанию** выберите элемент **Расшифровать 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. 192) те зашифрованные жесткие диски, которые вы хотите расшифровать.
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.*

Если во время расшифровки 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 расшифровку жестких дисков.

Если во время расшифровки 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 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.

Изменение справочных текстов агента аутентификации

Чтобы изменить справочные тексты агента аутентификации, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.

2. В папке **Управляемые компьютеры** дерева консоли 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 вам политику в списке политик.

5. Выполните одно из следующих действий:

   - По правой клавише мыши вызовите контекстное меню политики. Выберите пункт **Свойства**.
   - Нажмите на ссылку **Изменить параметры политики** справа от списка политик.

   Откроется окно **Свойства: <Название политики>**.

6. Выберите раздел **Общие параметры шифрования**.

7. В блоке **Шаблоны** нажмите на кнопку **Справка**.

   Откроется окно **Справочные тексты агента аутентификации**.

8. Выполните следующие действия:

   - Выберите закладку **Загрузка**, если вы хотите изменить справочный текст, отображающийся в окне агента аутентификации на этапе ввода имени и пароля учетной записи агента аутентификации.
   - Выберите закладку **Смена пароля**, если вы хотите изменить справочный текст, отображающийся в окне агента аутентификации на этапе смены пароля учетной записи агента аутентификации.
   - Выберите закладку **Восстановление пароля**, если вы хотите изменить справочный текст, отображающийся в окне агента аутентификации на этапе восстановления пароля учетной записи агента аутентификации.

9. Измените справочные тексты. При необходимости используйте кнопку **Восстановить исходный текст**.

10. Нажмите на кнопку **OK**.

11. В окне **Свойства: <Название политики>** нажмите на кнопку **OK**, чтобы сохранить внесенные изменения.

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. Вы можете создать (см. раздел «Создание групповой задачи» на стр. 285) групповую задачу 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.

В ЭТОМ РАЗДЕЛЕ

УПРАВЛЕНИЕ УЧЕТНЫМИ ЗАПИСЯМИ АГЕНТА АУТЕНТИФИКАЦИИ С ПОМОЩЬЮ ГРУППОВЫХ ЗАДАЧ

Чтобы управлять учетными записями агента аутентификации с помощью групповой задачи, выполните следующие действия:

1. Создайте (см. раздел «Создание групповой задачи» на стр. 285) групповую задачу управления учетными записями агента аутентификации.
2. Откройте (см. раздел «Изменение параметров задачи» на стр. 287) раздел **Параметры** окна **Свойства: <название групповой 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. 197).
4. Добавьте команды для изменения учетных записей агента аутентификации (см. раздел «Добавление команды для изменения учетной записи агента аутентификации в групповой задаче» на стр. 198).
5. Добавьте команды для удаления учетных записей агента аутентификации (см. раздел «Добавление команды для удаления учетной записи агента аутентификации в групповой задаче» на стр. 199).
6. Если требуется, измените добавленные команды для управления учетными записями агента аутентификации. Для этого в таблице **Команды для управления учетными записями 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 аутентификации** выберите одну или несколько команд и нажмите на кнопку **Удалить**.

   Чтобы выбрать несколько записей в таблице, выделяйте их, удерживая клавишу **CTRL**.

8. В окне свойств групповой задачи нажмите на кнопку **OK**, чтобы сохранить внесенные изменения.
9. Запустите групповую задачу (см. раздел «Запуск, остановка, приостановка и возобновление выполнения задачи» на стр. 286).

Команды по управлению учетными записями агента аутентификации, добавленные в групповую задачу, будут выполнены.

Управление учетными записями агента аутентификации с помощью локальной задачи Шифрование (управление учетными записями)

Чтобы управлять учетными записями агента аутентификации с помощью локальной задачи Шифрование (управление учетными записями), выполните следующие действия:

1. Откройте (см. раздел «Изменение параметров задачи» на стр. 287) раздел **Параметры** окна **Свойства: Шифрование (управление учетными записями)**.

2. Если требуется, измените ранее созданные учетные записи агента аутентификации. Для этого выполните следующие действия:

   a. Выберите в таблице учетную запись агента аутентификации и нажмите на кнопку **Изменить**.

      Откроется окно **Добавление учетной записи пользователя**.

   b. Измените параметры учетной записи агента аутентификации.

   c. В окне **Добавление учетной записи пользователя** нажмите на кнопку **OK**.

   d. Повторите пункты a – c инструкции при необходимости.

   В таблицу добавится команда для изменения учетной записи агента аутентификации.

3. Если требуется, удалите ранее созданные учетные записи агента аутентификации. Для этого выберите в таблице запись с информацией о ранее созданной с помощью команды добавления учетной записи агента аутентификации и нажмите на кнопку **Удалить**.

   В таблицу добавится команда для удаления учетной записи агента аутентификации.

4. Добавьте команды для создания учетных записей агента аутентификации (см. раздел «Добавление команды для создания учетной записи агента аутентификации» на стр. 197).

5. Если требуется, измените команды для добавления учетных записей агента аутентификации. Для этого выполните следующие действия:

   a. Выберите в таблице команду для добавления учетной записи агента аутентификации и нажмите на кнопку **Изменить**.

      Откроется окно **Добавление учетной записи пользователя**.

   b. Измените параметры команды для добавления учетной записи агента аутентификации.

   c. В окне **Добавление учетной записи пользователя** нажмите на кнопку **OK**.

   d. Повторите пункты a – c инструкции при необходимости.

6. Если требуется, удалите команды для добавления учетных записей агента аутентификации. Для этого выберите команду для добавления учетной записи агента аутентификации и нажмите на кнопку **Удалить**.

7. В окне свойств локальной задачи нажмите на кнопку **OK**, чтобы сохранить внесенные изменения.

8. Запустите локальную задачу *Шифрование (управление учетными записями)* (см. раздел «*Запуск, остановка, приостановка и возобновление выполнения задачи*» на стр. 286).

Параметры измененных в свойствах локальной задачи ранее созданных учетных записей агента аутентификации будут изменены. Учетные записи агента аутентификации, удаленные из локальной задачи, будут удалены из списка учетных записей агента аутентификации. Команды для создания учетных записей агента аутентификации, добавленные в локальную задачу, будут выполнены.

Добавление команды для создания учетной записи агента аутентификации

Чтобы добавить команду для создания учетной записи агента аутентификации, выполните следующие действия:

1. Выполните одно из следующих действий:

   - Откройте (см. раздел «Изменение параметров задачи» на стр. 287) раздел **Параметры** окна **Свойства: <название групповой задачи управления учетными записями агента аутентификации>**, если вы хотите добавить команду для создания учетной записи агента аутентификации в свойствах групповой задачи. Далее в контекстном меню кнопки **Добавить** выберите пункт **Команду для добавления учетной записи**.

   - Откройте (см. раздел «Изменение параметров задачи» на стр. 287) раздел **Параметры** окна **Шифрование (управление учетными записями)**, если вы хотите добавить команду для создания учетной записи агента аутентификации в свойствах локальной задачи *Шифрование (управление учетными записями)*. Далее нажмите на кнопку **Добавить**.

   Откроется окно **Добавление учетной записи пользователя**.

2. В окне **Добавление учетной записи пользователя** в поле **Учетная запись Windows** укажите имя учетной записи пользователя Microsoft Windows, на основе которой будет создана учетная запись для агента аутентификации. 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 SID учетной записи пользователя.

   Если вы не определяете SID по кнопке **Разрешить**, то SID будет определен в момент выполнения задачи на компьютере.

   Определение SID учетной записи пользователя Microsoft Windows на этапе добавления команды для создания учетной записи агента аутентификации может быть удобно для того, чтобы проверить корректность веденного вручную имени учетной записи пользователя Microsoft Windows. В случае если введенная учетная запись пользователя Microsoft Windows не существует, находится в недоверенном домене или не существует на компьютере, для которого изменяется локальная задача *Шифрование (управление учетными записями),* то задача управления учетными записями агента аутентификации будет завершена с ошибкой.

4. 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)*.

5. В поле **Имя пользователя** введите имя учетной записи агента аутентификации, которое требуется вводить при прохождении процедуры аутентификации для доступа к зашифрованным жестким дискам.

6. В поле **Пароль** введите пароль учетной записи агента аутентификации, который требуется вводить при прохождении процедуры аутентификации для доступа к зашифрованным жестким дискам.

7. В поле **Описание команды** введите информацию об учетной записи агента аутентификации, необходимую вам для работы с командой.

8. 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.

   - Выберите вариант **Не требовать смену пароля**, если вы хотите, чтобы программа не требовала сменить пароль от пользователя, в первый раз проходящего процедуру аутентификации под учетной записью, указанной в команде.

9. 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.

10. В окне **Добавление учетной записи пользователя** нажмите на кнопку **OK**.

Добавление команды для изменения учетной записи агента аутентификации в групповой задаче

Чтобы добавить команду для изменения учетной записи агента аутентификации в групповой задаче, выполните следующие действия:

1. В разделе **Параметры** окна **Свойства: <название групповой задачи управления учетными записями агента аутентификации>** в контекстном меню кнопки **Добавить** выберите пункт **Команду для изменения учетной записи**.

2. Откроется окно **Изменение учетной записи пользователя**.

3. 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**.

4. Если вы ввели имя учетной записи пользователя Microsoft Windows вручную, нажмите на кнопку **Разрешить**, чтобы определить SID учетной записи пользователя.

   Если вы не определяете SID по кнопке **Разрешить**, то SID будет определен в момент выполнения задачи на компьютере.

   Определение SID учетной записи пользователя Microsoft Windows на этапе добавления команды для изменения учетной записи агента аутентификации может быть удобно для того, чтобы проверить корректность веденного 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.

5. Установите флажок **Изменить имя пользователя** и введите новое имя для 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.

6. Установите флажок **Изменить пароль** и введите новый пароль для 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 пароль на указанный в поле ниже.

7. 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.

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 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.

11. Установите правило доступа к аутентификации в агенте аутентификации.

12. В окне **Изменение учетной записи пользователя** нажмите на кнопку **OK**.

Добавление команды для удаления учетной записи агента аутентификации в групповой задаче

Чтобы добавить команду для удаления учетной записи агента аутентификации в групповой задаче, выполните следующие действия:

1. В разделе **Параметры** окна **Свойства: <название групповой 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 SID учетной записи пользователя.

   Если вы не определяете SID по кнопке **Разрешить**, то SID будет определен в момент выполнения задачи на компьютере.

   Определение SID учетной записи пользователя Microsoft Windows на этапе добавления команды для удаления учетной записи агента аутентификации может быть удобно для того, чтобы проверить корректность веденного 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**.

Включение использования технологии единого входа (SSO)

Чтобы включить использование технологии единого входа (SSO), выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые компьютеры** дерева консоли 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 вам политику в списке политик.
5. Выполните одно из следующих действий:
   - По правой клавише мыши вызовите контекстное меню политики. Выберите пункт **Свойства**.
   - Нажмите на ссылку **Изменить параметры политики** справа от списка политик.

   Откроется окно **Свойства: <Название политики>**.
6. Выберите раздел **Общие параметры шифрования**.
7. В разделе **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.*

Получение доступа к зашифрованным жестким дискам и съемным носителям

Получить доступ к зашифрованным жестким дискам и съемным носителям можно одним из следующих способов:

- Пройти процедуру аутентификации. Если жесткие диски зашифрованы, перед загрузкой операционной системы загружается агент аутентификации. С помощью агента аутентификации требуется пройти процедуру аутентификации для получения доступа к зашифрованным жестким дискам и загрузки операционной системы.

  После успешного прохождения процедуры аутентификации предоставляется доступ к зашифрованным дискам, загружается операционная система. При последующих перезагрузках операционной системы требуется повторно проходить процедуру аутентификации.

  Возможны случаи, когда пользователь не может пройти процедуру аутентификации. Например, если пользователь забыл имя и / или пароль учетной записи агента аутентификации. В этом случае пользователь может восстановить имя и пароль учетной записи агента аутентификации. Для этого требуется сформировать запрос и ввести ответ для восстановления имени и пароля учетной записи агента аутентификации.

- Получить и активировать ключ доступа к зашифрованным съемным носителям. В случае если зашифрованные съемные носители подключены к компьютеру с установленной программой Kaspersky Endpoint Security и доступной функциональностью шифрования жестких дисков и если в момент первого обращения к зашифрованному съемному носителю на этом компьютере связь с Kaspersky Security Center отсутствует или компьютер находится под управлением сервера администрирования, отличного от того, под управлением которого он был во время шифрования, пользователь может запросить у администратора локальной сети организации ключ доступа к зашифрованным съемным носителям.

  После того как пользователь активировал ключ доступа к зашифрованному съемному носителю, Kaspersky Endpoint Security на этом компьютере предоставляет доступ к этому съемному носителю при последующих обращениях, даже если связь с Kaspersky Security Center отсутствует.

- Восстановить доступ к зашифрованным жестким дискам и съемным носителям с помощью утилиты восстановления зашифрованных устройств (далее также «утилиты восстановления»). В случае если по каким-либо причинам процедура аутентификации проходит неуспешно, восстановление имени и пароля учетной записи агента аутентификации проходят неуспешно, а получить ключ доступа к зашифрованным съемным носителям невозможно (например, по причине повреждения метаданных), пользователь может восстановить доступ к зашифрованным жестким дискам и съемным носителям с помощью утилиты восстановления. С помощью этой утилиты пользователь может восстановить доступ к зашифрованным жестким дискам и съемным носителям двумя способами: разблокировать жесткие диски и съемные носители, оставив их зашифрованными, или расшифровать их.

Данные, необходимые для восстановления доступа к зашифрованным устройствам с помощью утилиты восстановления, передаются во время восстановления со стороны Kaspersky Security Center. Эти данные в течение некоторого времени находятся в памяти компьютера пользователя в открытом виде. Чтобы снизить вероятность несанкционированного доступа к данным для восстановления доступа к зашифрованным устройствам, рекомендуется выполнять восстановление доступа к зашифрованным устройствам на доверенных компьютерах.

В этом разделе

Восстановление имени и пароля учетной записи агента аутентификации

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 клавишу **F5**, чтобы инициировать процедуру восстановления имени и пароля учетной записи агента аутентификации.

2. Сформируйте 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 «Формирование и передача пользователю блоков ответа на запрос пользователя о восстановлении имени и пароля учетной записи агента аутентификации» на стр. 202) 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 логина 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.

Формирование и передача пользователю блоков ответа на запрос пользователя о восстановлении имени и пароля учетной записи агента аутентификации

Чтобы сформировать и передать пользователю блоки ответа на запрос пользователя о восстановлении имени и пароля учетной записи агента аутентификации, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.

2. В папке **Управляемые компьютеры** дерева консоли 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 **Компьютеры**.

4. На закладке **Компьютеры** выделите в списке 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 **Доступ к устройствам и данным в автономном режиме**.

   Откроется окно **Предоставление доступа к устройствам и данным в автономном режиме**.

6. В окне **Предоставление доступа к устройствам и данным в автономном режиме** выберите закладку **Агент аутентификации**.

7. На закладке **Агент аутентификации** в поле **Имя компьютера** введите имя компьютера пользователя, запросившего восстановление логина и пароля учетной записи агента аутентификации.

8. 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 блоке справа.

9. Продиктуйте содержимое блоков ответа пользователю.

Получение и активация ключа доступа к зашифрованным съемным носителям

Чтобы получить и активировать ключ доступа к зашифрованным съемным носителям, выполните следующие действия:

1. Обратитесь к зашифрованному съемному носителю, доступ к которому вы хотите получить.

   Если связь с Kaspersky Security Center в момент обращения к зашифрованному съемному носителю отсутствует, Kaspersky Endpoint Security формирует файл запроса доступа к съемному носителю.

   Откроется окно **Доступ к съемному носителю запрещен**.

2. Отправьте файл запроса доступа к зашифрованному съемному носителю 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 съемному носителю по электронной почте.

   - Нажмите на кнопку **Сохранить**, чтобы сохранить файл запроса доступа к зашифрованному съемному носителю и передать его администратору локальной сети организации способом, отличным от передачи по электронной почте.

3. Получите файл ключа доступа к зашифрованному съемному носителю, созданный и переданный (см. раздел «Создание и передача пользователю файла ключа доступа к зашифрованному съемному носителю» на стр. 204) вам администратором локальной сети организации.

4. Активируйте ключ доступа к зашифрованному съемному носителю одним из следующих способов:

   - В любом файловом менеджере выделите файл ключа доступа к зашифрованному съемному носителю и откройте его двойным щелчком мыши.

   - Выполните следующие действия:

     a. Откройте главное окно Kaspersky Endpoint Security.

     b. По ссылке **Существуют активные запросы** откройте окно **Статус доступа к файлам и устройствам**. В окне отображается список всех запросов доступа к зашифрованным файлам и съемным носителям.

     c. В окне **Статус доступа к файлам и устройствам** выберите номер запроса, для которого вы получили файл ключа доступа к зашифрованному съемному носителю.

     d. Нажмите на кнопку **Обзор**, чтобы загрузить полученный файл ключа доступа к зашифрованному съемному носителю.

        Откроется стандартное окно Microsoft Windows **Выбор файла ключа доступа**.

     e. В стандартном окне Microsoft Windows **Выбор файла ключа доступа** выберите полученный от администратора локальной сети организации файл с расширением fdertr и названием, совпадающим с названием файла выбранного запроса доступа к зашифрованному съемному носителю.

     f. Нажмите на кнопку **Открыть**.

     g. В окне **Статус доступа к файлам и устройствам** нажмите на кнопку **OK**.

В результате Kaspersky Endpoint Security предоставит доступ к зашифрованному съемному носителю.

Создание и передача пользователю файла ключа доступа к зашифрованному съемному носителю

Чтобы создать и передать пользователю файл ключа доступа к зашифрованному съемному носителю, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые компьютеры** дерева консоли откройте папку с названием группы администрирования, к которой принадлежит компьютер пользователя, запросившего доступ к зашифрованному съемному носителю.
3. В рабочей области выберите закладку **Компьютеры**.
4. На закладке **Компьютеры** выделите в списке компьютер пользователя, запросившего доступ к зашифрованному съемному носителю, и по правой клавише мыши откройте контекстное меню.
5. В контекстном меню выберите пункт **Доступ к устройствам и данным в автономном режиме**.

   Откроется окно **Предоставление доступа к устройствам и данным в автономном режиме**.
6. В окне **Предоставление доступа к устройствам и данным в автономном 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 зашифрованному съемному носителю. 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 зашифрованному съемному носителю по электронной почте.
   - Нажмите на кнопку **Сохранить**, чтобы сохранить файл ключа доступа к зашифрованному съемному носителю и передать его пользователю способом, отличным от передачи по электронной почте.

Восстановление доступа к зашифрованному жесткому диску или съемному носителю с помощью утилиты восстановления

Перед восстановлением доступа к зашифрованному устройству с помощью утилиты восстановления рекомендуется вывести компьютер, на котором будет выполняться процедура, из-под действия политики шифрования Kaspersky Security Center. Это позволяет предотвратить повторное шифрование устройства.

Рекомендуется любыми доступными средствами создавать образы устройств и восстанавливать доступ к ним, а не непосредственно к зашифрованным устройствам. Таким образом вы защитите устройства от их возможной порчи во время восстановления, которая может быть вызвана, например, сбоями в работе компьютера во время восстановления, случайными ошибками администратора локальной сети организации, предоставляющего файлы ключа доступа для расшифровки устройств.

Чтобы восстановить доступ к зашифрованному жесткому диску или съемному носителю с помощью утилиты восстановления, выполните следующие действия:

1. Запустите утилиту восстановления одним из следующих способов:

   - В главном окне программы Kaspersky Endpoint Security нажмите на ссылку **Поддержка**. Далее в окне **Поддержка** нажмите на кнопку **Восстановление зашифрованного устройства**.

   - Запустите файл утилиты восстановления fdert.exe, созданный с помощью программы Kaspersky Endpoint Security (см. раздел «Создание исполняемого файла утилиты восстановления» на стр. 206).

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 его или расшифровать.

   При разблокировке устройство не расшифровывается, но к нему в результате предоставляется прямой доступ. Утилита восстановления предлагает разблокировать устройство, если на компьютере доступна функциональность шифрования Kaspersky Endpoint Security.

   Утилита восстановления предлагает расшифровать устройство, если на комьютере недоступна функциональность шифрования Kaspersky Endpoint Security.

4. Нажмите на кнопку **Исправить MBR**, если в результате диагностики зашифрованного устройства вы получили сообщение о каких-либо проблемах, связанных с главной загрузочной записью устройства (MBR).

   Исправление главной загрузочной записи устройства может ускорить сбор информации, необходимой для разблокировки или расшифровки устройства.

5. Нажмите на кнопку **Разблокировать** / **Расшифровать**.

6. Укажите параметры, необходимые для старта процесса разблокировки / расшифровки устройства. Для этого следуйте указаниям утилиты восстановления.

7. После указания параметров, необходимых для старта процесса разблокировки / расшифровки устройства, в окне **Параметры разблокировки устройства / Параметры расшифровки устройства** нажмите на кнопку **OK**.

Запустится процесс разблокировки / расшифровки устройства.

Создание и передача пользователю файла ключа доступа к зашифрованному жесткому диску или съемному носителю

Чтобы создать и передать пользователю файл ключа доступа к зашифрованному жесткому диску или съемному носителю, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.

2. Откройте папку **Шифрование и защита данных** \ **Зашифрованные устройства** дерева консоли.

   В рабочей области отобразится список зашифрованных устройств.

3. В рабочей области выберите зашифрованное устройство, для которого вы хотите создать файл ключа доступа.

4. По правой клавише мыши откройте контекстное меню и выберите пункт **Предоставить доступ к устройству**.

Откроется окно **Предоставление доступа к устройству**.

5. В окне **Предоставление доступа к устройству** нажмите на кнопку **Обзор**, чтобы загрузить файл запроса доступа к зашифрованному устройству, полученный от пользователя.

   Kaspersky Security Center сформирует файл ключа доступа к зашифрованному устройству.

6. 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 способом, отличным от передачи по электронной почте.

Создание исполняемого файла утилиты восстановления

Чтобы создать исполняемый файл утилиты восстановления, выполните следующие действия:

1. Откройте главное окно программы (на стр. 46).

2. По ссылке **Поддержка**, расположенной левом нижнем углу главного окна программы, откройте окно **Поддержка**.

   Откроется 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.

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. 206).

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 USB-устройство флэш-памяти.

   Инструкцию о создании пользовательского образа среды предустановки Windows вы можете прочитать в справочной документации Microsoft (например, на ресурсе Microsoft TechNet).

Восстановление доступа к зашифрованным данным в случае выхода из строя операционной системы

Чтобы восстановить доступ к зашифрованным данным 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. 22).

3. Установите связь между компьютером и Сервером администрирования Kaspersky Security Center, под управлением которого находился компьютер во время шифрования данных, к которым вы хотите восстановить доступ (см. *Руководство администратора Kaspersky Security Center*).

   Доступ к зашифрованным данным будет предоставлен на тех же условиях, что были до выхода операционной системы из строя.

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 определена 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 дал отказ в ответ на запрос о подтверждении выполнения операции шифрования файлов на съемном носителе.
- *Не поддерживается*. На компьютере недоступна функциональность шифрования данных.

Просмотр статусов шифрования данных компьютера

Чтобы просмотреть статус шифрования данных компьютера, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые компьютеры** дерева консоли откройте папку с названием группы администрирования, в состав которой входит нужный вам компьютер.
3. В рабочей области выберите закладку **Компьютеры**.

   На закладке **Компьютеры** в рабочей области отображаются свойства компьютеров выбранной группы администрирования.
4. На закладке **Компьютеры** 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 носителей, подключенных к компьютеру.

Просмотр статусов 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 папку **Отчеты и уведомления**.

   Справа отобразится рабочая область папки **Отчеты и уведомления**.
3. В рабочей области папки **Отчеты и уведомления** на закладке **Статистика** создайте новую страницу с информационными панелями со статистикой шифрования данных. Для этого выполните следующие действия:

   a. На закладке **Статистика** нажмите на кнопку  .

      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. Выберите раздел **Информационные панели**.

e. Нажмите на кнопку **Добавить**.

Откроется окно **Новая информационная панель**.

f. В окне **Новая информационная панель** в разделе **Состояние защиты** выберите пункт **Шифрование компьютеров**.

g. Нажмите на кнопку **OK**.

Откроется окно **Свойства: Шифрование компьютеров**.

h. Измените при необходимости параметры информационной панели. Для этого воспользуйтесь разделами **Вид** и **Компьютеры** окна **Свойства: Шифрование компьютеров**.

i. Нажмите на кнопку **OK**.

j. Повторите пункты d – h инструкции, при этом в окне **Новая информационная панель** в разделе **Состояние защиты** выберите пункт **Шифрование съемных носителей**.

Добавленные информационные панели отобразятся в списке **Информационные панели** окна **Свойства: Новая страница**.

k. 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**.

l. В окне **Свойства: Статистика** нажмите на кнопку **Закрыть**.

4. На закладке **Статистика** откройте страницу, созданную на предыдущих шагах инструкции.

Отобразятся информационные панели, на которых вы можете просмотреть статусы шифрования компьютеров и съемных носителей.

Просмотр списка ошибок шифрования файлов на локальных дисках компьютера

Чтобы просмотреть список ошибок шифрования файлов на локальных дисках компьютера, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.

2. В папке **Управляемые компьютеры** дерева консоли 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 **Компьютеры**.

4. На закладке **Компьютеры** 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 дереве консоли выберите папку **Отчеты и уведомления**.
3. По правой клавише мыши вызовите контекстное меню папки **Отчеты и уведомления** и выберите пункт **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 компьютеров**.
   - **Отчет о шифровании устройств**.
   - **Отчет об ошибках шифрования**.
   - **Отчет о блокировании доступа к файлам**.

   После завершения работы мастера создания шаблона отчета в папке **Отчеты и уведомления** дерева консоли появится новый шаблон отчета.

5. В папке **Отчеты и уведомления** выберите шаблон отчета, созданный на предыдущих шагах инструкции.

Запустится процесс формирования отчета. Отчет отобразится в рабочей области Консоли администрирования.

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 новые 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.

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 новых 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.

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.

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. 245).

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 к интернету), 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.

См. также

Добавление источника обновлений 213

Выбор региона сервера обновлений 214

Настройка обновления из папки общего доступа 214

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 (на стр. 48).
2. В левой части окна в блоке **Задачи по расписанию** выберите раздел **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

Выбор региона сервера обновлений

Чтобы выбрать регион сервера обновлений, выполните следующие действия:

1. Откройте окно настройки параметров программы (на стр. 48).
2. В левой части окна в блоке **Задачи по расписанию** выберите раздел **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 **OK**.
7. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

См. также

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 (на стр. 48).
2. В левой части окна в блоке **Задачи по расписанию** выберите раздел **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 (на стр. 48).
2. В левой части окна в блоке **Задачи по расписанию** выберите раздел **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

Выбор режима запуска задачи обновления

Чтобы выбрать режим запуска задачи обновления, выполните следующие действия:

1. Откройте окно настройки параметров программы (на стр. 48).
2. В левой части окна в блоке **Задачи по расписанию** выберите раздел **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 значение 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 **ОК**.
7. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

См. также

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 вас 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 (на стр. 48).
2. В левой части окна в блоке **Задачи по расписанию** выберите раздел **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 учетное имя пользователя, права которого требуется использовать для доступа к источнику обновлений.
6. В поле **Пароль** введите пароль пользователя, права которого требуется использовать для доступа к источнику обновлений.
7. Нажмите на кнопку **OK**.
8. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Запуск и остановка задачи обновления

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

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

Чтобы запустить или остановить задачу обновления, выполните следующие действия:

1. Откройте главное окно программы.
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 (на стр. 48).
2. В левой части окна в блоке **Задачи по расписанию** выберите раздел **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

Проверка компьютера на вирусы и другие программы, представляющие угрозу, является важным фактором для обеспечения безопасности компьютера. Требуется регулярно проверять компьютер на вирусы и другие программы, представляющие угрозу, 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 в процессе проверки компьютера на вирусы и другие программы, представляющие угрозу.

В ЭТОМ РАЗДЕЛЕ

О ЗАДАЧАХ ПРОВЕРКИ

Для поиска вирусов и других программ, представляющих угрозу, в состав Kaspersky Endpoint Security включены следующие задачи:

- **Полная проверка**. Тщательная проверка всей системы. По умолчанию Kaspersky Endpoint Security проверяет следующие объекты:
  - системная память;
  - объекты, загрузка которых осуществляется при старте операционной системы;
  - резервное хранилище операционной системы;
  - все жесткие и съемные диски.
- **Проверка важных областей**. По умолчанию Kaspersky Endpoint Security проверяет объекты, загрузка которых осуществляется при старте операционной системы.
- **Выборочная проверка**. Kaspersky Endpoint Security проверяет объекты, выбранные пользователем. Вы можете проверить любой объект из следующего списка:
  - системная память;
  - объекты, загрузка которых осуществляется при старте операционной системы;
  - резервное хранилище операционной системы;
  - почтовые базы;
  - все жесткие, съемные и сетевые диски;
  - любой выбранный файл.

Задача полной проверки и задача проверки важных областей являются специфическими. Для этих задач не рекомендуется изменять списки объектов для проверки.

После запуска задач проверки 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. 46).
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 файлов.

  Вы можете выбрать один из предустановленных уровней безопасности файлов или настроить параметры уровня безопасности файлов самостоятельно. После того как вы изменили параметры уровня безопасности файлов, вы всегда можете вернуться к рекомендуемым параметрам уровня безопасности файлов.

- 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).

- Настроить проверку составных файлов.

- Настроить использование методов проверки.

  Во время своей работы Kaspersky Endpoint Security использует сигнатурный анализ. В процессе сигнатурного анализа Kaspersky Endpoint Security сравнивает найденный объект с записями в базах программы. В соответствии с рекомендациями специалистов «Лаборатории Касперского» 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 новые вредоносные объекты, записей о которых еще нет в базах Kaspersky Endpoint Security.

- Настроить использование технологий проверки.

  Вы 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.

- 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 файлов

Для выполнения задач проверки Kaspersky Endpoint Security применяет разные наборы параметров. Такие наборы параметров называют *уровнями безопасности файлов*. Предустановленно три уровня безопасности файлов: **Высокий**, **Рекомендуемый**, **Низкий**. Параметры уровня безопасности файлов **Рекомендуемый** считаются оптимальными, они рекомендованы специалистами «Лаборатории Касперского».

Чтобы изменить уровень безопасности файлов, выполните следующие действия:

1. Откройте окно настройки параметров программы (на стр. 48).
2. В левой части окна в блоке **Задачи по расписанию** выберите раздел 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 установить один из предустановленных уровней безопасности файлов (**Высокий**, **Рекомендуемый**, **Низкий**), выберите его при помощи ползунка.
   - Если вы хотите настроить уровень безопасности файлов самостоятельно, нажмите на кнопку **Настройка** и задайте параметры в открывшемся окне с названием задачи проверки.

     После того как вы самостоятельно настроили уровень безопасности файлов, название уровня безопасности файлов в блоке **Уровень безопасности** изменится на **Другой**.
   - Если вы хотите изменить уровень безопасности файлов 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 (на стр. 48).
2. В левой части окна в блоке **Задачи по расписанию** выберите раздел 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: 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: Информировать**.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Формирование области проверки

Под областью проверки подразумевается местоположение и тип файлов (например, все жесткие диски, объекты автозапуска, почтовые базы), которые проверяет Kaspersky Endpoint Security во время выполнения задачи проверки.

Чтобы сформировать область проверки, требуется выполнить следующие действия:

- Сформировать список объектов для проверки.
- Выбрать тип проверяемых файлов.

Чтобы сформировать список объектов для проверки, выполните следующие действия:

1. Откройте окно настройки параметров программы (на стр. 48).
2. В левой части окна в блоке **Задачи по расписанию** выберите раздел с названием нужной задачи проверки: **Полная проверка**, **Проверка важных областей**.

   В правой части окна отобразятся параметры выбранной задачи проверки.
3. Нажмите на кнопку **Объекты проверки**.

   Откроется окно **Объекты для проверки**.
4. В списке **Объекты для проверки** выполните одно из следующих действий:
   - Нажмите на кнопку **Добавить**, если вы хотите добавить новый объект в список объектов для проверки.

- Если вы хотите изменить местоположение объекта, выберите объект в списке объектов для проверки и нажмите на кнопку **Изменить**.

  Откроется окно **Выбор объекта для проверки**.

- Если вы хотите удалить объект из списка объектов для проверки, выберите объект в списке объектов для проверки и нажмите на кнопку **Удалить**.

  Откроется окно подтверждения удаления.

Вы не можете удалить или изменить объекты, включенные в список объектов для проверки по умолчанию.

5. Выполните одно из следующих действий:

   - Если вы хотите добавить новый объект или изменить местоположение объекта из списка объектов для проверки, в окне **Выбор объекта для проверки** выберите объект и нажмите на кнопку **Добавить**.

     Все объекты, выбранные в окне **Выбор объекта для проверки**, отобразятся в списке **Область защиты** в окне **Файловый Антивирус**.

     Далее нажмите на кнопку **ОК**.

   - Если вы хотите удалить объект, нажмите на кнопку **Да** в окне подтверждения удаления.

6. При необходимости повторите пункты 4-5 для добавления, изменения местоположения или удаления объектов из списка объектов для проверки.

7. Чтобы исключить объект из списка объектов для проверки, в списке **Область защиты** снимите флажок рядом с ним. Объект остается в списке объектов для проверки, но не проверяется во время выполнения задачи проверки.

8. Нажмите на кнопку **ОК**.

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

Чтобы выбрать тип проверяемых файлов, выполните следующие действия:

1. Откройте окно настройки параметров программы (на стр. 48).

2. В левой части окна в блоке **Задачи по расписанию** выберите раздел с названием нужной задачи проверки: **Полная проверка**, **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. 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, 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 окне с названием задачи проверки нажмите на кнопку **OK**.

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

Оптимизация проверки файлов

Чтобы оптимизировать проверку файлов, выполните следующие действия:

1. Откройте окно настройки параметров программы (на стр. 48).

2. В левой части окна в блоке **Задачи по расписанию** выберите раздел 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 круг проверяемых составных файлов, таким образом увеличив скорость проверки.

Чтобы настроить проверку составных файлов, выполните следующие действия:

1. Откройте окно настройки параметров программы (на стр. 48).

2. В левой части окна в блоке **Задачи по расписанию** выберите раздел 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 или вложенные OLE-объекты, файлы почтовых форматов или защищенные паролем архивы.

6. Если в блоке **Оптимизация проверки** снят флажок **Проверять только новые и измененные файлы**, для каждого типа составного файла вы можете выбрать, следует ли проверять все файлы этого типа или только новые. Для выбора нажмите на ссылку все / новые, расположенную рядом с названием типа составного файла. Ссылка меняет свое значение при нажатии на нее левой клавишей мыши.

   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 большого размера, снимите флажок **Не распаковывать составные файлы большого размера**.

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

   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 (на стр. 48).

2. В левой части окна в блоке **Задачи по расписанию** выберите раздел 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 детализации эвристического анализа: **поверхностный**, **средний** или **глубокий**.

6. Нажмите на кнопку **OK**.

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

Использование технологий проверки

Чтобы использовать технологии проверки, выполните следующие действия:

1. Откройте окно настройки параметров программы (на стр. 48).

2. В левой части окна в блоке **Задачи по расписанию** выберите раздел 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 задачи проверки

Чтобы выбрать режим запуска задачи проверки, выполните следующие действия:

1. Откройте окно настройки параметров программы (на стр. 48).

2. В левой части окна в блоке **Задачи по расписанию** выберите раздел с названием нужной задачи проверки: **Полная проверка**, **Проверка важных областей**, **Выборочная проверка**.

   В правой части окна отобразятся параметры выбранной задачи проверки.

3. Нажмите на кнопку **Режим запуска**.

   Откроется закладка **Режим запуска** окна с названием выбранной задачи.

4. В блоке **Режим запуска** выберите один из следующих вариантов режима запуска задачи проверки:

   - Выберите вариант **Вручную**, если вы хотите запускать задачу проверки вручную.

   - Выберите вариант **По расписанию**, если вы хотите настроить расписание запуска задачи проверки.

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 проверки. Для этого выполните следующие действия:

  a. В раскрывающемся списке **Периодичность** укажите, когда следует запускать задачу проверки. 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 проверки.

  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 **После запуска программы** или **После каждого обновления**, то флажок **Запускать пропущенные задачи** недоступен.

  d. Установите флажок **Приостанавливать проверку, если экранная заставка не включена и разблокирован компьютер**, если вы хотите, чтобы Kaspersky Endpoint Security приостанавливал задачу проверки, когда ресурсы компьютера заняты. Этот вариант расписания запуска задачи проверки 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 от имени учетной записи, с правами 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 (на стр. 48).

2. В левой части окна в блоке **Задачи по расписанию** выберите раздел 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 закладка **Режим запуска** окна с названием выбранной задачи проверки.

4. На закладке **Режим запуска** в блоке **Пользователь** установите флажок **Запускать задачу с правами пользователя**.

5. В поле **Имя** введите учетное 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

В последнее время широкое распространение получили вредоносные программы, которые используют уязвимости операционной системы для распространения через локальные сети и съемные носители информации. 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 (на стр. 48).
2. В левой части окна выберите блок **Задачи по расписанию**.

   В правой части окна отобразятся общие параметры задач по расписанию.
3. В блоке **Проверка съемных дисков при подключении** в раскрывающемся списке **Действия при подключении съемного диска** выберите нужное действие:
   - **Не проверять**.
   - **Полная проверка**.
   - **Быстрая проверка**.
4. Установите флажок **Максимальный размер съемного диска** и укажите в поле рядом значение в мегабайтах, если вы хотите, чтобы Kaspersky Endpoint Security проверял съемные диски, размер которых меньше или равен указанного значения.
5. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Работа с необработанными файлами

Этот раздел содержит инструкции по работе с зараженными и возможно 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 носителе 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. 233);
- восстановить те зараженные файлы, в которых содержится важная информация, а также восстановить файлы со статусом *Вылечен* и *Не заражен* (см. раздел «*Восстановление файлов из списка необработанных файлов*» на стр. 232);
- поместить на карантин файлы со статусом *Возможно зараженный* (см. раздел «*Помещение файла на карантин*» на стр. 257).

Работа со списком необработанных файлов

Список необработанных файлов представлен в виде таблицы.

Работая со списком необработанных файлов, 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 для необработанных файлов

Вы можете вручную запустить задачу выборочной проверки для необработанных файлов, например, если проверка была прервана по какой-либо причине или вы хотите, чтобы Kaspersky Endpoint Security проверил файлы после очередного обновления баз и модулей программы.

Чтобы запустить задачу выборочной проверки для необработанных файлов, выполните следующие действия:

1. Откройте главное окно программы (на стр. 46).
2. По ссылке **Отчеты**, расположенной в верхней части главного окна программы, откройте окно **Отчеты и хранилища**.
3. В окне **Отчеты и хранилища** выберите закладку **Необработанные файлы**.
4. В таблице на закладке **Необработанные файлы** выберите одно или несколько событий о файлах, которые вы хотите проверить. Чтобы выделить 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. Выберите пункт **Перепроверить**.

   После завершения проверки на экране отобразится уведомление о количестве проверенных файлов и количестве обнаруженных в файлах угроз.

Восстановление файлов из списка необработанных файлов

При необходимости вы можете восстановить файлы из списка необработанных файлов.

Специалисты «Лаборатории Касперского» рекомендуют восстанавливать файлы из списка необработанных файлов только в том случае, если файлам присвоен статус *Не заражен*.

Чтобы восстановить файлы из списка необработанных файлов, выполните следующие действия:

1. Откройте главное окно программы (на стр. 46).

2. По ссылке **Отчеты**, расположенной в верхней части главного окна программы, откройте окно **Отчеты и хранилища**.
3. В окне **Отчеты и хранилища** выберите закладку **Необработанные файлы**.
4. Если вы хотите восстановить все файлы, то выполните следующие действия:
   a. По правой клавише мыши в любом месте таблицы на закладке **Необработанные файлы** откройте контекстное меню.
   b. Выберите пункт **Восстановить все**.

      Kaspersky Endpoint Security переместит все файлы из списка необработанных файлов в папки их исходного размещения, если эти папки доступны для записи.
   c. Если при восстановлении папка исходного размещения одного из файлов недоступна для записи, то откроется стандартное окно Microsoft Windows **Сохранить как**. С помощью этого окна вы можете указать нужную папку для сохранения файла.
5. Если вы хотите восстановить один или несколько файлов, то выполните следующие действия:
   a. В таблице на закладке **Необработанные файлы** выберите одно или несколько событий о необработанных файлах, которые вы хотите восстановить из списка необработанных файлов. Чтобы выбрать несколько событий о необработанных файлах, выделяйте их, удерживая клавишу **CTRL**.
   b. Восстановите файлы одним из следующих способов:
      - Нажмите на кнопку **Восстановить**.
      - По правой клавише мыши откройте контекстное меню. Выберите пункт **Восстановить**.

      Kaspersky Endpoint Security переместит выбранные файлы в папки их исходного размещения, если эти папки доступны для записи.
   c. Если при восстановлении папка исходного размещения одного из файлов недоступна для записи, то откроется стандартное окно Microsoft Windows **Сохранить как**. С помощью этого окна вы можете указать нужную папку для сохранения файла.

Удаление файлов из списка необработанных файлов

Вы можете удалить зараженный или возможно зараженный файл, помещенный в список необработанных файлов. Перед тем как удалить файл, Kaspersky Endpoint Security формирует резервную копию файла и сохраняет ее в резервном хранилище на тот случай, если впоследствии вам потребуется восстановить файл (см. раздел «Восстановление файлов из списка необработанных файлов» на стр. 232).

Чтобы удалить файлы из списка необработанных файлов, выполните следующие действия:

1. Откройте главное окно программы (на стр. 46).
2. По ссылке **Отчеты**, расположенной в верхней части главного окна программы, откройте окно **Отчеты и хранилища**.
3. В окне **Отчеты и хранилища** выберите закладку **Необработанные объекты**.
4. В таблице на закладке **Необработанные объекты** выберите одно или несколько событий о файлах, 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. Выберите пункт **Удалить**.

Kaspersky Endpoint Security создает для каждого файла резервную копию и сохраняет ее в резервном хранилище (см. раздел «О карантине и резервном хранилище» на стр. 254). После этого Kaspersky Endpoint Security удаляет выбранные файлы из списка необработанных файлов.

ПОИСК УЯЗВИМОСТЕЙ

Этот раздел содержит информацию о Мониторинге уязвимостей, об особенностях и настройке задачи поиска уязвимостей, а также инструкции по работе со списком уязвимостей, которые обнаружил Kaspersky Endpoint Security в результате выполнения задачи поиска уязвимостей.

В ЭТОМ РАЗДЕЛЕ

О Мониторинге 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 (см. раздел «Аппаратные и программные требования» на стр. 20).

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 особенно актуальна, если задача поиска уязвимостей (см. раздел «О задаче поиска уязвимостей» на стр. 236) 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. 46);
- из окна настройки параметров программы (см. раздел «Окно настройки параметров программы» на стр. 48).

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

1. Откройте главное окно программы (на стр. 46).
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 (на стр. 48).
2. В левой части окна в блоке **Контроль рабочего места** выберите раздел **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.

Просмотр информации об уязвимостях запущенных программ

Компонент Мониторинг уязвимостей предоставляет информацию об уязвимостях запущенных программ. Эта информация 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. 20).

Чтобы просмотреть информацию об уязвимостях запущенных программ, выполните следующие действия:

1. Откройте главное окно программы (на стр. 46).
2. Выберите закладку **Центр управления**.
3. Нажмите клавишей мыши на блок **Контроль рабочего места**.

   Блок **Контроль рабочего места** раскроется.
4. Нажмите на кнопку **Мониторинг активности программ**.

Откроется закладка **Мониторинг активности программ** окна **Программы**. В таблице **Мониторинг активности программ** представлена сводная информация об активности запущенных программ в операционной системе. Статус уязвимости запущенных программ, который определил компонент Мониторинг уязвимостей, отображается в графе **Статус 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. 236) 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. 245).

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. 46).
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*.

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 (на стр. 48).
2. В левой части окна в блоке **Задачи по расписанию** выберите раздел **Поиск уязвимостей**.

   В правой части окна отобразятся параметры задачи поиска уязвимостей.
3. В блоке **Объекты для 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 **Дополнительные области 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 задачи поиска уязвимостей

Чтобы выбрать режим запуска задачи поиска уязвимостей, выполните следующие действия:

1. Откройте окно настройки параметров программы (на стр. 48).
2. В левой части окна в блоке **Задачи по расписанию** выберите раздел **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.

Настройка запуска 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 (на стр. 48).

2. В левой части окна в блоке **Задачи по расписанию** выберите раздел **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 учетное имя 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 с найденными уязвимостями

Этот раздел содержит инструкции о работе со списком уязвимостей, которые обнаружил Kaspersky Endpoint Security в результате выполнения задачи поиска уязвимостей.

В этом разделе

Об уязвимостях

Kaspersky Endpoint Security записывает сведения о результатах выполнения задачи поиска уязвимостей (см. раздел «О задаче поиска уязвимостей» на стр. 236) в список уязвимостей. Эти сведения включают данные об источнике уязвимости, ее уровень важности и рекомендации по ее устранению.

Если пользователь просмотрел выбранные уязвимости и выполнил рекомендуемые действия для их устранения, то Kaspersky Endpoint Security присваивает уязвимостям статус *Исправленные*.

Если пользователю нужно, чтобы в списке уязвимостей не отображались записи о каких-либо уязвимостях, то он может 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 важности уязвимости. Выделяют следующие уровни важности найденных уязвимостей:

  - Значок . **Критический**. К этому уровню важности относятся очень опасные уязвимости, которые должны быть закрыты немедленно. Злоумышленники активно применяют уязвимости этой группы для заражения операционной системы компьютера или причинения вреда персональным данным пользователя. Специалисты «Лаборатории Касперского» рекомендуют своевременно выполнять все действия этой группы для устранения угрозы.

  - Значок . **Важный**. К этому уровню важности относятся важные уязвимости, которые должны быть закрыты в ближайшее время. В данный момент не зафиксировано активного использования уязвимости. Злоумышленники могут начать использовать уязвимости этой группы для заражения операционной системы компьютера или причинения вреда персональным данным пользователя. Специалисты «Лаборатории Касперского» рекомендуют выполнять действия этой группы для обеспечения оптимальной защиты компьютера и персональных данных пользователя.

  - Значок . **Предупреждение**. К этому уровню важности относятся уязвимости, устранение которых можно отложить. Злоумышленники не станут активно использовать уязвимости этой группы в данный момент, однако в будущем такие уязвимости могут поставить безопасность компьютера под угрозу.

- Название программы, в которой обнаружена уязвимость.

- Папка размещения уязвимого файла.
- Информация о производителе программного обеспечения согласно электронной цифровой подписи.
- Решение Kaspersky Endpoint Security по устранению уязвимости.

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;
- исправить уязвимость;
- 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

Повторный запуск задачи поиска уязвимостей

Чтобы проверить уязвимости, найденные ранее, вы можете повторно запустить задачу поиска уязвимостей. Это может потребоваться, например, если задача поиска уязвимостей была прервана по какой-либо причине или вы хотите, чтобы Kaspersky Endpoint Security проверил файлы после очередного обновления баз и модулей программы (см. раздел «Об обновлении баз и модулей программы» на стр. 211).

Чтобы повторно запустить задачу поиска уязвимостей, выполните следующие действия:

1. Откройте главное окно программы (на стр. 46).
2. По ссылке **Отчеты**, расположенной в верхней части главного окна программы, откройте окно **Отчеты и хранилища**.
3. В окне **Отчеты и хранилища** выберите закладку **Уязвимости**.

   Закладка **Уязвимости** содержит список уязвимостей, которые обнаружил Kaspersky Endpoint Security в результате выполнения задачи поиска уязвимостей.
4. Нажмите на кнопку **Перепроверить**.

   Kaspersky Endpoint Security заново проверит все уязвимости 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. 46).
2. По ссылке **Отчеты**, расположенной в верхней части главного окна программы, откройте окно **Отчеты и хранилища**.
3. В окне **Отчеты и 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 **Исправление уязвимости**. Блок содержит сведения об этой уязвимости и рекомендации по ее исправлению.

   Для каждой выбранной уязвимости доступна следующая информация:

   - Название программы, в которой обнаружена уязвимость.
   - Версия программы, в которой обнаружена уязвимость.
   - Критичность 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 скачать 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 **Исправление уязвимости** 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. 243).

Чтобы скрыть запись в списке уязвимостей, выполните следующие действия:

1. Откройте главное окно программы (на стр. 46).

2. По ссылке **Отчеты**, расположенной в верхней части главного окна программы, откройте окно **Отчеты и хранилища**.

3. В окне **Отчеты и 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 **Исправление уязвимости**. Блок содержит сведения об этой уязвимости и рекомендации по ее исправлению.

5. Нажмите на кнопку **Скрыть**.

   Kaspersky Endpoint Security присвоит выбранной уязвимости статус *Скрытая*.

   Если флажок **Скрытые** установлен, выбранная запись об уязвимости перемещается в конец списка уязвимостей и выделяется серым цветом.

   Если флажок **Скрытые** снят, выбранная запись об уязвимости не отображается в списке уязвимостей.

Фильтрация списка уязвимостей по уровню важности уязвимостей

Чтобы отфильтровать список уязвимостей по уровню важности уязвимостей, выполните следующие действия:

1. Откройте главное окно программы (на стр. 46).

2. По ссылке **Отчеты**, расположенной в верхней части главного окна программы, откройте окно **Отчеты и хранилища**.

3. В окне **Отчеты и 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 важность** находятся значки, обозначающие уровень важности уязвимостей. Отфильтруйте список уязвимостей по уровню важности уязвимостей одним из следующих способов:

   - Выделите значки, если хотите, чтобы записи об уязвимостях с таким уровнем важности отображались в списке уязвимостей.

   - Снимите выделение для значков, если хотите, чтобы записи об уязвимостях с таким уровнем важности не отображались в списке уязвимостей.

В списке уязвимостей отобразятся записи об уязвимостях с указанным уровнем важности. Заданные вами условия фильтрации записей в списке уязвимостей сохраняются после того, как вы закрыли окно **Отчеты и 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. 46).

2. По ссылке **Отчеты**, расположенной в верхней части главного окна программы, откройте окно **Отчеты и хранилища**.

3. В окне **Отчеты и 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**, ес ли 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 **Отчеты и хранилища**.

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, выполнении каждой задачи проверки, задачи обновления и задачи поиска уязвимостей, а также о работе программы в целом фиксируется в отчете.

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. События, зарегистрированные в работе разных компонентов или задач, имеют разный набор атрибутов.

Вы можете сформировать отчеты следующих типов:

- 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 какому-либо отдельному компоненту или задаче Kaspersky Endpoint Security.
- Отчет «Общий отчет защиты». Содержит информацию о событиях, возникающих в ходе работы следующих компонентов Kaspersky Endpoint Security:
  - Файловый Антивирус.
  - Почтовый Антивирус.
  - Веб-Антивирус.
  - IM-Антивирус.
  - Мониторинг системы.
  - Сетевой экран.
  - Защита от сетевых атак.
- Отчет о работе компонента или задачи Kaspersky Endpoint Security. Содержит информацию о событиях, возникающих в ходе работы выбранного компонента или задачи Kaspersky Endpoint Security.

Выделяют следующие уровни важности событий:

- Значок . **Информационные события**. События справочного характера, как правило, не содержащие важной информации.
- Значок . **Важные события**. События, на которые нужно обратить внимание, поскольку они отражают важные ситуации в работе Kaspersky Endpoint Security.
- Значок . **Критические события**. События критической важности и отказа функционирования программы, 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;
- отображать и скрывать сгруппированные данные;
- 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 по компонентам и задачам Kaspersky Endpoint Security, объединенным в группы. Kaspersky Endpoint Security удаляет все записи выбранных отчетов от наиболее ранней записи до момента инициирования удаления.

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 (на стр. 48).
2. В левой части окна в блоке **Дополнительные параметры** выберите раздел **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 (на стр. 48).
2. В левой части окна в блоке **Дополнительные параметры** выберите раздел **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.

ФОРМИРОВАНИЕ ОТЧЕТОВ

Чтобы сформировать отчеты, выполните следующие действия:

1. Откройте главное окно программы (на стр. 46).
2. По ссылке **Отчеты**, расположенной в верхней части главного окна программы, откройте окно **Отчеты и хранилища**.

   Откроется закладка **Отчеты** окна **Отчеты и хранилища**.

   По умолчанию на закладке **Отчеты** отображается отчет «Системный аудит».
3. Если вы хотите сформировать отчет «Все компоненты защиты», в левой части окна **Отчеты и хранилища** 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 и хранилища** 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 отчета в отдельном блоке

Вы можете посмотреть подробную информацию о событии отчета, представленную в отдельном блоке.

Чтобы просмотреть информацию о событии отчета в отдельном блоке, выполните следующие действия:

1. Откройте главное окно программы (на стр. 46).

2. По ссылке **Отчеты**, расположенной в верхней части главного окна программы, откройте окно **Отчеты и хранилища**.

   Откроется закладка **Отчеты** окна **Отчеты и хранилища**.

   По умолчанию на закладке **Отчеты** отображается отчет «Системный аудит». Этот отчет содержит информацию о регистрируемых событиях, возникающих в ходе работы программы в целом, а также в процессе взаимодействия пользователя с программой.

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, воспользуйтесь функциями фильтрации, поиска и сортировки, чтобы найти нужное событие в отчете.

5. Выберите найденное событие в отчете.

   В нижней части окна отобразится блок, который содержит атрибуты этого события и информацию о его уровне важности.

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. 46).
2. По ссылке **Отчеты**, расположенной в верхней части главного окна программы, откройте окно **Отчеты и хранилища**.

   Откроется закладка **Отчеты** окна **Отчеты и хранилища**.

   По умолчанию на закладке **Отчеты** отображается отчет «Системный аудит». Этот отчет содержит информацию о регистрируемых событиях, возникающий в ходе работы программы в целом, а также в процессе взаимодействия пользователя с программой.
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 (на стр. 48).
2. В левой части окна в блоке **Дополнительные параметры** выберите раздел **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.
     - IM-Антивирус.
     - Сетевой экран.
     - Защита от сетевых атак.
   - **Отчет задач проверки**. Содержит информацию о выполненных задачах проверки:
     - Полная проверка.
     - Проверка важных областей.
     - Выборочная проверка.
   - **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.
     - Мониторинг уязвимостей.
     - Контроль устройств.
     - Веб-Контроль.
   - **Данные Мониторинга системы**. Содержит информацию о работе Мониторинга системы.
   - **Отчет о шифровании данных**.
5. Нажмите на кнопку **ОК**.

СЕРВИС УВЕДОМЛЕНИЙ

Этот раздел содержит информацию о сервисе уведомлений, оповещающих пользователя о событиях в работе Kaspersky Endpoint Security, а также инструкции о том, как настроить доставку уведомлений.

В ЭТОМ РАЗДЕЛЕ

Об уведомлениях Kaspersky Endpoint Security

В процессе работы Kaspersky Endpoint Security возникают различного рода события. Они могут иметь информационный характер или нести важную информацию. Например, событие может уведомлять 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 событий Kaspersky Endpoint Security.

Kaspersky Endpoint Security может доставлять уведомления одним из следующих способов:

- Выводить уведомления на экран с помощью всплывающих сообщений в области уведомлений панели задач Microsoft Windows.
- Доставлять уведомления по электронной почте.

Вы можете настроить способы доставки уведомлений. Способ доставки уведомлений устанавливается для каждого типа событий.

Настройка сервиса уведомлений

Вы можете выполнить следующие действия для настройки сервиса уведомлений:

- Настроить параметры журналов событий, где Kaspersky Endpoint Security сохраняет события.
- Настроить доставку уведомлений на экран.
- Настроить доставку уведомлений по электронной почте.

Работая с таблицей событий для настройки сервиса уведомлений, вы можете выполнять следующие действия:

- фильтровать события сервиса уведомлений по значениям граф или по условиям сложного фильтра;
- использовать функцию поиска событий сервиса уведомлений;
- сортировать события сервиса уведомлений;
- изменять порядок и набор граф, отображаемых в списке событий сервиса уведомлений.

В этом разделе

Настройка параметров журналов событий

Чтобы настроить параметры журналов событий, выполните следующие действия:

1. Откройте окно настройки параметров программы (на стр. 48).
2. В левой части окна в блоке **Дополнительные параметры** выберите раздел **Интерфейс**.

   В правой части окна отобразятся параметры пользовательского интерфейса.
3. В блоке **Уведомления** нажмите на кнопку **Настройка**.
4. 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 задачи.
5. В левой части окна выберите компонент или задачу, для которой вы хотите настроить параметры журналов событий.
6. В графах **Сохранять в локальном журнале** и **Сохранять в журнале событий Windows** установите флажки напротив нужных событий.

   События графы **Сохранять в локальном журнале** выводятся в журнал событий Kaspersky Endpoint Security. События графы **Сохранять в журнале Windows** выводятся в журнал событий Microsoft Windows.
7. Нажмите на кнопку **ОК**.
8. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Настройка доставки уведомлений на экран и по электронной почте

Чтобы настроить доставку уведомлений на экран и по электронной почте, выполните следующие действия:

1. Откройте окно настройки параметров программы (на стр. 48).
2. В левой части окна в блоке **Дополнительные параметры** выберите раздел **Интерфейс**.

   В правой части окна отобразятся параметры пользовательского интерфейса.
3. В блоке **Уведомления** нажмите на кнопку **Настройка**.
4. 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 задачи.

5. В левой части окна выберите компонент или задачу, для которой вы хотите настроить доставку уведомлений.

6. В графе **Уведомлять на экране** установите флажки напротив нужных событий.

   Информация о выбранных событиях доставляется на экран в виде всплывающих сообщений в области уведомлений панели задач Microsoft Windows.

7. В графе **Уведомлять по почте** установите флажки напротив нужных событий.

   Информация о выбранных событиях доставляется по электронной почте.

8. Нажмите на кнопку **Настройка почтовых уведомлений**.

   Откроется окно **Настройка почтовых уведомлений**.

9. Установите флажок **Отправлять почтовые сообщения о событиях**, чтобы включить доставку информации о событиях в работе Kaspersky Endpoint Security, отмеченных в графе **Уведомлять по почте**.

10. Укажите параметры доставки почтовых уведомлений.

11. Нажмите на кнопку **ОК**.

12. В окне **Настройка почтовых уведомлений** нажмите на кнопку **ОК**.

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

Просмотр журнала событий Microsoft Windows

- *Чтобы просмотреть журнал событий Microsoft Windows,*

  выберите **Пуск → Настройка → Панель управления → Администрирование → Просмотр событий**.

РАБОТА С КАРАНТИНОМ И РЕЗЕРВНЫМ ХРАНИЛИЩЕМ

Этот раздел содержит инструкции о том, как настроить параметры карантина и резервного хранилища и как работать с карантином и резервным хранилищем.

В ЭТОМ РАЗДЕЛЕ

О КАРАНТИНЕ И РЕЗЕРВНОМ ХРАНИЛИЩЕ

Карантин – это список возможно зараженных файлов. *Возможно зараженные файлы* – это файлы, которые могут содержать вирусы и другие программы, представляющие угрозу, или их модификации.

Когда Kaspersky Endpoint Security помещает возможно зараженный файл на карантин, он выполняет не копирование файла, а его перемещение: программа удаляет файл с жесткого диска или из почтового сообщения и сохраняет файл в специальном хранилище данных. Файлы на карантине хранятся в специальном формате и не представляют опасности.

Kaspersky Endpoint Security может обнаружить и поместить на карантин возможно зараженный файл в процессе проверки на вирусы и другие программы, представляющие угрозу (см. раздел «Проверка компьютера» на стр. 220), а также в ходе работы компонентов защиты Файловый Антивирус (см. раздел «О Файловом Антивирусе» на стр. 60), Почтовый Антивирус (см. раздел «О Почтовом Антивирусе» на стр. 73) и Мониторинг системы (на стр. 70).

Kaspersky Endpoint Security помещает файлы на карантин в следующих случаях:

- Код файла похож на код известной угрозы, но частично изменен или напоминает по структуре вредоносную программу, и не зафиксирован в базах Kaspersky Endpoint Security. В этом случае файл помещается на карантин в результате эвристического анализа в ходе работы Файлового Антивируса и Почтового Антивируса, а также в процессе проверки на вирусы и другие программы, представляющие угрозу. Механизм эвристического анализа редко приводит к ложным срабатываниям.

- Последовательность совершаемых файлом действий является опасной. В этом случае файл помещается на карантин в результате анализа его поведения компонентом защиты Мониторинг системы.

Пользователь может самостоятельно поместить на карантин файл, который подозревает в заражении вирусами и другими программами, представляющими угрозу.

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 обезвредить ее. По этой причине рекомендуется проверять файлы, находящиеся на карантине, после каждого обновления баз и модулей программы.

НАСТРОЙКА ПАРАМЕТРОВ КАРАНТИНА И РЕЗЕРВНОГО ХРАНИЛИЩА

Хранилище данных включает в себя карантин и резервное хранилище. Вы можете выполнить следующие действия для настройки параметров карантина и резервного хранилища:

- Настроить максимальный срок хранения файлов на карантине и копий файлов в резервном хранилище.

  По умолчанию максимальный срок хранения файлов, помещенных на карантин, и копий файлов в резервном хранилище составляет 30 дней. По истечении максимального срока хранения Kaspersky Endpoint Security удаляет наиболее старые файлы из хранилища данных. Вы можете отменить ограничение по времени или изменить максимальный срок хранения файлов.

- Настроить максимальный размер карантина и резервного хранилища.

  По умолчанию максимальный размер карантина и резервного хранилища составляет 100 МБ. После достижения максимального размера Kaspersky Endpoint Security автоматически удаляет наиболее старые файлы из карантина и резервного хранилища таким образом, чтобы не превышался его максимальный размер. Вы можете отменить ограничение на максимальный размер карантина и резервного хранилища или изменить максимальный размер.

В ЭТОМ РАЗДЕЛЕ

НАСТРОЙКА МАКСИМАЛЬНОГО СРОКА ХРАНЕНИЯ ФАЙЛОВ НА КАРАНТИНЕ И В РЕЗЕРВНОМ ХРАНИЛИЩЕ

Чтобы настроить максимальный срок хранения файлов на карантине и в резервном хранилище, выполните следующие действия:

1. Откройте окно настройки параметров программы (на стр. 48).

2. В левой части окна в блоке **Дополнительные параметры** выберите раздел **Отчеты и хранилища**.

3. Выполните одно из следующих действий:

   - В правой части окна в блоке **Параметры карантина и резервного хранилища** установите флажок **Хранить объекты не более**, если хотите ограничить срок хранения файлов на карантине и копий файлов в резервном хранилище. В поле справа от флажка **Хранить объекты не более** укажите максимальный срок хранения файлов на карантине и копий файлов в резервном хранилище. По умолчанию максимальный срок хранения файлов на карантине и копий файлов в резервном хранилище составляет 30 дней.

   - В правой части окна в блоке **Параметры карантина и резервного хранилища** снимите флажок **Хранить объекты не более**, если хотите отменить ограничение срока хранения файлов на карантине и копий файлов в резервном хранилище.

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

Настройка максимального размера карантина и резервного хранилища

Чтобы настроить максимальный размер карантина и резервного хранилища, выполните следующие действия:

1. Откройте окно настройки параметров программы (на стр. 48).
2. В левой части окна в блоке **Дополнительные параметры** выберите раздел **Отчеты и хранилища**.
3. Выполните одно из следующих действий:
   - В правой части окна в блоке **Параметры карантина и резервного хранилища** установите флажок **Максимальный размер хранилища**, если хотите ограничить размер карантина и резервного хранилища. В поле справа от флажка **Максимальный размер файла** укажите максимальный размер карантина и резервного хранилища. По умолчанию максимальный размер составляет 100 МБ.
   - В правой части окна в блоке **Параметры карантина и резервного хранилища** снимите флажок **Максимальный размер хранилища**, если хотите отменить ограничение на размер карантина и резервного хранилища.

   По умолчанию ограничение размера карантина и резервного хранилища выключено.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Работа с карантином

Работая с карантином, вы можете выполнять следующие действия с файлами:

- просматривать список файлов, помещенных на карантин в ходе работы Kaspersky Endpoint Security;
- самостоятельно помещать на карантин файлы, которые вы подозреваете в заражении вирусами и другими программами, представляющими угрозу;
- 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;
- открыть папку исходного размещения файла;
- отправлять возможно зараженные файлы для исследования в «Лабораторию Касперского».

Список файлов, помещенных на карантин, представлен в виде таблицы.

Кроме того, вы можете выполнять следующие действия, работая с табличными данными:

- фильтровать события карантина по значениям граф или по условиям сложного фильтра;
- использовать функцию поиска событий карантина;
- сортировать события карантина;
- изменять порядок и набор граф, отображаемых в списке событий карантина;
- группировать события карантина.

Если требуется, вы можете скопировать выбранные события карантина в буфер обмена.

В ЭТОМ РАЗДЕЛЕ

ПОМЕЩЕНИЕ ФАЙЛА НА КАРАНТИН

Kaspersky Endpoint Security автоматически помещает на карантин возможно зараженные файлы, обнаруженные в ходе работы компонентов защиты или во время проверки компьютера на вирусы и другие программы, представляющие угрозу.

Вы можете самостоятельно поместить на карантин файл, который вы подозреваете в заражении вирусами или другими программами, представляющими угрозу.

Вы можете поместить файл на карантин двумя способами:

- с помощью кнопки **Поместить файл на карантин** на закладке **Карантин** окна **Отчеты и хранилища**;
- с помощью пункта контекстного меню, вызванного вами в стандартном окне Microsoft Windows **Мои документы**.

Чтобы поместить файл на карантин с закладки Карантин окна Отчеты и хранилища, выполните следующие действия:

1. Откройте главное окно программы (на стр. 46).
2. По ссылке **Карантин**, расположенной в верхней части главного окна программы, откройте окно **Отчеты и хранилища**.

   Откроется закладка **Карантин** окна **Отчеты и хранилища**.

   Закладка **Карантин** содержит список возможно зараженных файлов, которые Kaspersky Endpoint Security обнаружил в результате выполнения задачи проверки.
3. Нажмите на кнопку **Поместить на карантин**.
4. Откроется стандартное окно Microsoft Windows **Открыть**.
5. Выберите файл, который вы хотите поместить на карантин.
6. Нажмите на кнопку **Открыть**.

   В таблице на закладке **Карантин** отобразится выбранный файл. Доступ к этому файлу блокируется. Файл перемещается из папки исходного размещения на карантин. Файл сохраняется на карантине в закодированном виде, что исключает угрозу заражения операционной системы.

Чтобы поместить файл на карантин из окна Microsoft Windows Мои документы, выполните следующие действия:

1. Дважды щелкните мышью на ярлыке **Мои документы**, расположенном на рабочем столе операционной системы компьютера.

   Откроется стандартное окно Microsoft Windows **Мои документы**.

2. Перейдите в папку с файлом, который вы хотите поместить на карантин.

3. Выберите файл, который вы хотите поместить на карантин.

4. По правой клавише мыши откройте контекстное меню файла.

5. В контекстном меню выберите пункт **Поместить на карантин**.

Доступ к файлу блокируется. Файл перемещается на карантин из папки исходного размещения. Файл сохраняется на карантине в закодированном виде, что исключает угрозу заражения операционной системы.

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. Возможно, после очередного обновления баз и модулей программы Kaspersky Endpoint Security однозначно определит угрозу и обезвредит 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 (на стр. 48).

2. В левой части окна в блоке **Дополнительные параметры** выберите раздел **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 обезвредить ее. Если в настройках 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. 46).
2. По ссылке **Карантин**, расположенной в верхней части главного окна программы, откройте окно **Отчеты и хранилища**.

   Откроется закладка **Карантин** окна **Отчеты и хранилища**.
3. На закладке **Карантин** выберите одно или несколько событий карантина о возможно зараженных файлах, которые вы хотите проверить. Чтобы выбрать несколько событий карантина, выделяйте их, удерживая клавишу **CTRL**.
4. Запустите задачу выборочной проверки файлов одним из следующих способов:
   - Нажмите на кнопку **Перепроверить**.
   - По правой клавише мыши откройте контекстное меню. 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. 46).
2. По ссылке **Карантин**, расположенной в верхней части главного окна программы, откройте окно **Отчеты и хранилища**.

   Откроется закладка **Карантин** окна **Отчеты и хранилища**.
3. Если вы хотите восстановить все файлы, помещенные на карантин, то выполните следующие действия:
   a. По правой клавише мыши в любом месте таблицы на закладке **Карантин** откройте контекстное меню.
   b. 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 одно или несколько событий карантина о файлах, которые вы хотите восстановить из карантина. Чтобы выбрать несколько событий карантина, выделяйте их, удерживая клавишу **CTRL**.
   b. Восстановите файлы одним из следующих способов:
      - Нажмите на кнопку **Восстановить**.
      - По правой клавише мыши откройте контекстное меню. Выберите пункт **Восстановить**.

Kaspersky Endpoint Security переместит выбранные файлы в папки их исходного размещения.

Удаление файлов из карантина

Вы можете удалить файл, помещенный на карантин. Перед тем как удалить файл из карантина, Kaspersky Endpoint Security формирует резервную копию файла и сохраняет ее в резервном хранилище на тот случай, если впоследствии вам потребуется восстановить файл (см. раздел «Восстановление файлов из резервного хранилища» на стр. 261).

Чтобы удалить файлы из карантина, выполните следующие действия:

1. Откройте главное окно программы (на стр. 46).
2. По ссылке **Карантин**, расположенной в верхней части главного окна программы, откройте окно **Отчеты и хранилища**.

   Откроется закладка **Карантин** окна **Отчеты и хранилища**.
3. На закладке **Карантин** выберите одно или несколько событий карантина о возможно зараженных файлах, которые вы хотите удалить из карантина. Чтобы выбрать несколько событий карантина, выделяйте их, удерживая клавишу **CTRL**.
4. Удалите файлы одним из следующих способов:
   - Нажмите на кнопку **Удалить**.
   - По правой клавише мыши откройте контекстное меню. Выберите пункт **Удалить**.

Kaspersky Endpoint Security удаляет выбранные файлы из карантина. Kaspersky Endpoint Security создает для каждого файла резервную копию и сохраняет резервную копию в резервном хранилище.

Отправка возможно зараженных файлов для исследования в «Лабораторию Касперского»

Чтобы вы могли отправить возможно зараженные файлы в «Лабораторию Касперского», на вашем компьютере должна быть установлена почтовая программа и настроено подключение к интернету.

Чтобы отправить возможно зараженные файлы для исследования в «Лабораторию Касперского», выполните следующие действия:

1. Откройте главное окно программы (на стр. 46).
2. По ссылке **Карантин**, расположенной в верхней части главного окна программы, откройте окно **Отчеты и хранилища**.

   Откроется закладка **Карантин** окна **Отчеты и хранилища**.
3. На закладке **Карантин** выберите одно или несколько событий карантина о возможно зараженных файлах, которые вы хотите отправить для исследования в «Лабораторию Касперского». Чтобы выбрать несколько событий карантина, выделяйте их, удерживая клавишу **CTRL**.
4. По правой клавише мыши откройте контекстное меню.
5. Выберите пункт **Отправить в ЛК**.

Откроется окно почтового сообщения той почтовой программы, которая установлена на компьютере. Почтовое сообщение содержит архив с отправляемыми файлами, адрес получателя newvirus@kaspersky.com и тему сообщения «Объект на карантине».

Работа с резервным хранилищем

Если в файле обнаружен вредоносный код, Kaspersky Endpoint Security блокирует файл, удаляет его из папки исходного размещения, затем помещает его копию в резервное хранилище и пытается провести лечение. Если файл удается вылечить, то статус резервной копии файла изменяется на *Вылечен*. После этого вы можете восстановить файл из его вылеченной резервной копии в папку исходного размещения.

В случае обнаружения вредоносного кода в файле, который является частью приложения Windows Store, Kaspersky Endpoint Security не помещает файл 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 приложений Windows Store читайте в *Справочной системе к Microsoft Windows 8*).

Kaspersky Endpoint Security удаляет резервные копии файлов с любым статусом из резервного хранилища автоматически по истечении времени, заданного в параметрах программы.

Также вы можете самостоятельно удалить резервную копию как восстановленного, так и невосстановленного файла.

Список резервных копий файлов представлен в виде таблицы.

Работая с резервным хранилищем, вы можете выполнять следующие действия с резервными копиями файлов:

- просматривать список 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 события резервного хранилища по значениям граф или по условиям сложного фильтра;
- использовать функцию поиска событий резервного хранилища;
- сортировать события резервного хранилища;
- группировать события резервного хранилища;
- изменять порядок и набор граф, отображаемых в списке событий резервного хранилища.

Если требуется, вы можете скопировать выбранные события резервного хранилища в буфер обмена.

В этом разделе

Восстановление файлов из резервного хранилища

Рекомендуется восстанавливать файлы из резервных копий только в том случае, если им присвоен статус *Вылечен*.

Чтобы восстановить файлы из резервного хранилища, выполните следующие действия:

1. Откройте главное окно программы (на стр. 46).
2. По ссылке **Отчеты**, расположенной в верхней части главного окна программы, откройте окно **Отчеты и хранилища**.
3. В окне **Отчеты и хранилища** выберите закладку **Резервное хранилище**.
4. Если вы хотите восстановить все файлы из резервного хранилища, то выполните следующие действия:
   a. По правой кнопки мыши в любом месте таблицы на закладке **Резервное хранилище** откройте контекстное меню.
   b. 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 одно или несколько событий резервного хранилища. Чтобы выбрать несколько событий, выделяйте их, удерживая клавишу **CTRL**.
   b. Нажмите на кнопку **Восстановить**.

Kaspersky Endpoint Security восстановит файлы из выбранных резервных копий в папки их исходного размещения.

Удаление резервных копий файлов из резервного хранилища

Чтобы удалить резервные копии файлов из резервного хранилища, выполните следующие действия:

1. Откройте главное окно программы (на стр. 46).
2. По ссылке **Отчеты**, расположенной в верхней части главного окна программы, откройте окно **Отчеты и хранилища**.
3. В окне **Отчеты и хранилища** выберите закладку **Резервное хранилище**.
4. На закладке **Резервное хранилище** выберите одно или несколько событий резервного хранилища. Чтобы выбрать несколько событий резервного хранилища, выделяйте их, удерживая клавишу **CTRL**.
5. Нажмите на кнопку **Удалить**.

ДОПОЛНИТЕЛЬНАЯ НАСТРОЙКА ПРОГРАММЫ

Этот раздел содержит информацию о настройке дополнительных параметров Kaspersky Endpoint Security.

В ЭТОМ РАЗДЕЛЕ

Доверенная зона

Этот раздел содержит информацию о доверенной зоне и инструкции о том, как настроить правила исключений 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 защиты Kaspersky Endpoint Security.

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.

Правило исключения

Правило исключения – это совокупность условий, при выполнении которых Kaspersky Endpoint Security не проверяет объект на вирусы и другие программы, представляющие угрозу.

Правила исключений 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.

В результате работы Kaspersky Endpoint Security такие программы могут быть заблокированы. Чтобы избежать блокирования, для используемых программ вы можете настроить правила исключения из проверки Kaspersky Endpoint Security. 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 правило исключения, где указать название или маску названия по классификации Вирусной энциклопедии «Лаборатории Касперского».

Правила исключений 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. 268).

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 правилами исключений.

Настройка доверенной зоны

Вы можете выполнить следующие действия для настройки доверенной зоны:

- Создать новое правило исключения.

  Вы можете создать новое правило исключения, при выполнении которого Kaspersky Endpoint Security не проверяет указанные файлы или папки или наличие в них объектов с указанным названием.

- Приостановить работу правила исключения.

  Вы можете временно приостановить использование правила исключения, не удаляя его из списка правил исключений.

- Изменить параметры существующего правила исключения.

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

- Удалить правило исключения.

  Вы можете удалить правило исключения, если вы не хотите, чтобы Kaspersky Endpoint Security применял это правило во время проверки компьютера.

- Сформировать список доверенных программ.

  Вы можете сформировать список доверенных 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.

- Приостановить исключение из проверки Kaspersky Endpoint Security доверенной программы.

  Вы можете временно приостановить исключение доверенной программы из проверки Kaspersky Endpoint Security, не удаляя ее из списка доверенных программ.

В этом разделе

Создание правила исключения

Kaspersky Endpoint Security не проверяет объект, если при запуске одной из задач проверки указан жесткий диск или папка, в которой находится объект. Однако при запуске задачи выборочной проверки именно для этого объекта правило исключения не применяется.

Чтобы создать правило исключения, выполните следующие действия:

1. Откройте окно настройки параметров программы (на стр. 48).
2. В левой части выберите блок **Антивирусная защита**.

   В правой части окна отобразятся параметры антивирусной защиты.
3. В блоке **Исключения и доверенные программы** нажмите на кнопку **Настройка**.

   Откроется окно **Доверенная зона** на закладке **Правила исключений**.
4. Нажмите на кнопку **Добавить**.

   Откроется окно **Правило исключения**.
5. Если вы хотите исключить из проверки Kaspersky Endpoint Security 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 правила**, откройте окно **Название файла или папки**. В этом окне вы можете ввести название файла или папки, маску названия файла или папки или выбрать файл или папку в дереве папок.

   c. После выбора объекта нажмите на кнопку **ОК** в окне **Название файла или папки**.

      Ссылка на добавленный файл или папку появится в блоке **Описание правила** окна **Правило исключения**.
6. Если вы хотите исключить из проверки Kaspersky Endpoint Security 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 правила**, откройте окно **Название объекта**. В этом окне вы можете ввести название или маску названия объекта согласно классификации Вирусной энциклопедии «Лаборатории Касперского».

   c. Нажмите на кнопку **ОК** в окне **Название объекта**.

      Ссылка на добавленное название объекта появится в блоке **Описание правила** окна **Правило исключения**.
7. В поле **Комментарий** введите краткий комментарий к создаваемому правилу исключения.
8. Определите компоненты Kaspersky Endpoint Security, в работе которых должно быть использовано правило исключения:

   a. По ссылке **любые**, расположенной в блоке **Описание правила**, откройте ссылку **выберите компоненты**.

   b. По ссылке **выберите компоненты** откройте окно **Компоненты защиты**. В этом окне вы можете выбрать нужные компоненты.

c. Нажмите на кнопку **ОК** в окне **Компоненты защиты**.

Если компоненты указаны в параметрах правила исключения, то правило исключения применяется при проверке только этими компонентам Kaspersky Endpoint Security.

Если компоненты не указаны в параметрах правила исключения, то правило исключения применяется при проверке всеми компонентами Kaspersky Endpoint Security.

9. Нажмите на кнопку **ОК** в окне **Правило исключения**.

Добавленное правило исключения появится в списке правил исключений закладки **Правила исключений** окна **Доверенная зона**. В блоке **Описание правила** отобразятся заданные параметры этого правила исключения.

10. Нажмите на кнопку **ОК** в окне **Доверенная зона**.

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

Изменение правила исключения

Чтобы изменить правило исключения, выполните следующие действия:

1. Откройте окно настройки параметров программы (на стр. 48).

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

В правой части окна отобразятся параметры антивирусной защиты.

3. В блоке **Исключения и доверенные программы** нажмите на кнопку **Настройка**.

Откроется окно **Доверенная зона** на закладке **Правила исключений**.

4. В списке правил исключений выберите нужное правило исключения.

5. Нажмите на кнопку **Изменить**.

Откроется окно **Правило исключения**.

6. Изменить параметры правила исключения.

7. Нажмите на кнопку **ОК** в окне **Правило исключения**.

В блоке **Описание правила** отобразятся измененные параметры этого правила исключения.

8. Нажмите на кнопку **ОК** в окне **Доверенная зона**.

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

Удаление правила исключения

Чтобы удалить правило исключения, выполните следующие действия:

1. Откройте окно настройки параметров программы (на стр. 48).

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

В правой части окна отобразятся параметры антивирусной защиты.

3. В блоке **Исключения и доверенные программы** нажмите на кнопку **Настройка**.

Откроется окно **Доверенная зона** на закладке **Правила исключений**.

4. В списке правил исключений выберите нужное правило исключения.
5. Нажмите на кнопку **Удалить**.

   Удаленное правило исключения исчезнет из списка правил исключений.
6. Нажмите на кнопку **ОК** в окне **Доверенная зона**.
7. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Запуск и остановка работы правила исключения

Чтобы запустить или остановить работу правила исключения, выполните следующие действия:

1. Откройте окно настройки параметров программы (на стр. 48).
2. В левой части выберите блок **Антивирусная защита**.

   В правой части окна отобразятся параметры антивирусной защиты.
3. В блоке **Исключения и доверенные программы** нажмите на кнопку **Настройка**.

   Откроется окно **Доверенная зона** на закладке **Правила исключений**.
4. В списке правил исключений выберите нужное правило исключения.
5. Выполните одно из следующих действий:

   - Установите флажок рядом с названием правила исключения, если вы запустить работу этого правила исключения.
   - Снимите флажок рядом с названием правила исключения, если вы хотите временно приостановить работу этого правила 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 (на стр. 48).
2. В левой части выберите блок **Антивирусная защита**.

   В правой части окна отобразятся параметры антивирусной защиты.
3. В блоке **Исключения 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 хотите найти программу в списке установленных на компьютере программ. Откроется окно **Выбор программы**.
- Выберите пункт **Обзор**, если хотите указать путь к исполняемому файлу нужной программы. Откроется стандартное окно Microsoft Windows **Открыть**.

В результате выполненных действий откроется окно **Исключения для программы**.

c. Установите флажки для тех видов активности программы, которые не нужно проверять:

- **Не проверять открываемые файлы**.
- **Не контролировать активность программы**.
- **Не наследовать ограничения родительского процесса (программы)**.
- **Не контролировать активность дочерних программ**.
- **Разрешать взаимодействие с интерфейсом программы**.
- **Не проверять сетевой трафик**.

d. Нажмите на кнопку **ОК** в окне **Исключения 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 для программы**.

d. Измените статусы флажков для требуемых видов активности программы.

Если в окне **Исключения для программы** не выбран ни один из видов активности программы, то происходит включение доверенной программы в проверку (см. раздел «Включение и выключение доверенной программы из проверки» на стр. 270). Доверенная программа не удаляется из списка доверенных программ, но флажок для нее снят.

e. Нажмите на кнопку **ОК** в окне **Исключения 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 кнопку **ОК** в окне **Доверенная зона**.

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

Включение и выключение доверенной программы из проверки

Чтобы включить или выключить доверенную программу из проверки, выполните следующие действия:

1. Откройте окно настройки параметров программы (на стр. 48).
2. В левой части выберите блок **Антивирусная защита**.

   В правой части окна отобразятся параметры антивирусной защиты.
3. В блоке **Исключения 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.

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 сервисами программы с удаленного компьютера.

Под управлением 64-разрядных операционных систем и Microsoft Windows Vista 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 (на стр. 48).
2. В левой части окна выберите блок **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 (на стр. 48).
2. В левой части окна выберите блок **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 (на стр. 48).
2. В левой части выберите блок **Антивирусная защита**.

   В правой части окна отобразятся параметры антивирусной защиты.
3. В блоке **Исключения 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 хотите найти программу удаленного администрирования в списке установленных на компьютере программ. Откроется окно **Выбор программы**.
   - Выберите пункт **Обзор**, если хотите указать путь к исполняемому файлу программы удаленного администрирования. Откроется стандартное окно Microsoft Windows **Открыть**.

   В результате выполненных действий откроется окно **Исключения для программы**.
7. Установите флажок **Не контролировать активность программы**.
8. Нажмите на кнопку **ОК** в окне **Исключения для программы**.

   В списке доверенных программ появится добавленная доверенная программа.
9. 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. 274), 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. 211);
- задача полной проверки (см. раздел «О задачах проверки» на стр. 220);
- задача проверки важных областей (см. раздел «О задачах проверки» на стр. 220);
- задача выборочной проверки (см. раздел «О задачах проверки» на стр. 220);
- задача поиска уязвимостей (см. раздел «О задаче поиска уязвимостей» на стр. 236).

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 (см. раздел «Включение и выключение режима энергосбережения» на стр. 276).

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. 275). *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 непредоставлением 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. 275).

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 (на стр. 48).
2. В левой части окна выберите блок **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 (на стр. 48).
2. В левой части окна выберите блок **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.

Включение и выключение технологии лечения активного заражения для файловых серверов

Чтобы включить технологию лечения активного заражения для файловых серверов, выполните следующие действия:

1. Включите технологию лечения активного заражения в свойствах активной политики Kaspersky Security Center. Для этого выполните следующие действия:
   a. Откройте раздел **Основные 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.
2. 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 **Основные 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 (на стр. 48).
2. В левой части окна выберите блок **Дополнительные параметры**.

   В правой части окна отобразятся дополнительные параметры программы.
3. В блоке **Режимы работы** выполните следующие действия:

   - Установите флажок **Не запускать задачи по расписанию при работе от аккумулятора**, если хотите включить режим энергосбережения.

     Если включен режим энергосбережения, 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 поиска уязвимостей.

   - Снимите флажок **Не запускать задачи по расписанию при работе от аккумулятора**, если хотите выключить режим энергосбережения.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Включение и выключение режима передачи ресурсов другим программам

Чтобы включить или выключить режим передачи ресурсов другим программам, выполните следующие действия:

1. Откройте окно настройки параметров программы (на стр. 48).
2. В левой части окна выберите блок **Дополнительные параметры**.

В правой части окна отобразятся дополнительные параметры программы.

3. В блоке **Режимы работы** выполните следующие действия:

   - Установите флажок **Уступать ресурсы другим программам**, если 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 поиска уязвимостей.

   - Снимите флажок **Уступать ресурсы другим программам**, если 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 выключен.

4. Нажмите 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

Персональный 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 пароль и указать операции, для выполнения которых программа должна запрашивать пароль:

- все операции (кроме уведомлений об опасности);
- настройка параметров программы;
- завершение работы программы;
- выключение компонентов защиты и остановка задач проверки;

- выключение компонентов контроля;
- удаление ключа;
- удаление программы.

Включение и выключение защиты паролем

Чтобы включить или выключить защиту паролем, выполните следующие действия:

1. Откройте окно настройки параметров программы (на стр. 48).
2. В левой части окна в блоке **Дополнительные параметры** выберите раздел **Интерфейс**.

   В правой части окна отобразятся параметры пользовательского интерфейса.
3. Если вы хотите ограничить доступ к Kaspersky Endpoint Security с помощью пароля, выполните следующие действия:

   a. Установите флажок **Включить защиту паролем**.

   b. Нажмите на кнопку **Настройка**.

      Откроется окно **Защита паролем**.

   c. В поле **Новый пароль** введите пароль для доступа к программе.

   d. В поле **Подтверждение пароля** повторите пароль.

   e. В блоке **Область действия пароля** укажите операции с программой, для выполнения которых пользователь должен ввести пароль:

      - Выберите параметр **Все операции (кроме уведомлений об опасности)**, если хотите ограничить доступ для всех операций с программой.
      - Выберите параметр **Отдельные операции**, если хотите выборочно указать операции.

   f. Если вы выбрали параметр **Отдельные операции**, установите флажки рядом с названиями нужных операций:

      - **Настройка параметров программы**.
      - **Завершение работы программы**.
      - **Выключение компонентов защиты и остановка задач проверки**.
      - **Выключение компонентов контроля**.
      - **Удаление ключа**.
      - **Удаление / изменение / восстановление программы**.
      - **Восстановление доступа к данным на зашифрованных устройствах**.

   g. Нажмите на кнопку **ОК**.

Рекомендуется с осторожностью использовать пароль для ограничения доступа к программе. Если вы забыли пароль, то для получения инструкций по отмене защиты паролем следует обратиться в Службу технической поддержки «Лаборатории Касперского» (http://support.kaspersky.ru/helpdesk.html).

4. Если вы хотите отменить ограничение доступа к Kaspersky Endpoint Security с помощью пароля, выполните следующие действия:

   a. Снимите флажок **Включить защиту паролем**.

   b. Нажмите на кнопку **Сохранить**.

      Программа проверяет, есть ли защита на операцию отмены ограничения доступа.

      - Если операция отмены ограничения доступа к программе не защищена паролем, то ограничение доступа к Kaspersky Endpoint Security отменяется.

      - Если операция отмены ограничения доступа к программе защищена паролем, то откроется окно **Проверка пароля**. Это окно появляется каждый раз, когда пользователь совершает какую-либо операцию, защищенную паролем.

   c. В поле **Пароль** окна **Проверка пароля** введите пароль.

   d. Установите флажок **Запомнить пароль на эту сессию**, если хотите, чтобы во время текущей сессии работы программа не требовала ввода пароля при попытке выполнения этой операции. При следующем запуске Kaspersky Endpoint Security ограничение доступа к программе будет отменено.

      Снятый флажок **Запомнить пароль на эту сессию** означает, что программа запрашивает пароль каждый раз при попытке выполнения этой операции.

   e. Нажмите на кнопку **ОК**.

5. Нажмите на кнопку **Сохранить** в окне настройки параметров программы, чтобы сохранить внесенные изменения.

Изменение пароля доступа к Kaspersky Endpoint Security

Чтобы изменить пароль доступа к Kaspersky Endpoint Security, выполните следующие действия:

1. Откройте окно настройки параметров программы (на стр. 48).

2. В левой части окна в блоке **Дополнительные параметры** выберите раздел **Интерфейс**.

   В правой части окна отобразятся параметры пользовательского интерфейса.

3. Если защита паролем выключена, установите флажок **Включить защиту паролем**.

4. Нажмите на кнопку **Настройка**.

   Откроется окно **Защита паролем**.

5. В поле **Старый пароль** введите текущий пароль для доступа к программе.

6. В поле **Новый пароль** введите новый пароль для доступа к программе.

7. В поле **Подтверждение пароля** повторите новый пароль.

8. Нажмите на кнопку **ОК**.

   Программа проверяет введенные значения:

   - Если введено верное значение старого пароля, а также совпадают значения нового и подтвержденного пароля, то новый пароль считается установленным.

Окно **Защита паролем** закроется.

- Если введено неверное значение старого пароля, то в поле **Старый пароль** появится всплывающее сообщение с предложением повторить попытку. Для этого выполните шаг 5 инструкции и нажмите на кнопку **ОК**.

  Окно **Защита паролем** закроется.

- Если введено неверное значение подтвержденного пароля, то в поле **Подтверждение пароля** появится всплывающее сообщение с предложением повторить попытку. Для этого выполните шаг 7 инструкции и нажмите на кнопку **ОК**.

  Окно **Защита паролем** закроется.

9. Нажмите на кнопку **Сохранить** в окне настройки параметров программы, чтобы сохранить внесенные изменения.

УПРАВЛЕНИЕ ПРОГРАММОЙ ЧЕРЕЗ KASPERSKY SECURITY CENTER

Этот раздел содержит информацию об управлении программой Kaspersky Endpoint Security через Kaspersky Security Center.

В ЭТОМ РАЗДЕЛЕ

УПРАВЛЕНИЕ ПРОГРАММОЙ KASPERSKY ENDPOINT SECURITY

Программа Kaspersky Security Center предназначена для централизованного решения основных административных задач по управлению системой антивирусной безопасности компьютерных сетей организаций, построенной на основе программ, входящих в состав продуктов Kaspersky Open Space Security. Kaspersky Security Center поддерживает работу во всех сетевых конфигурациях, использующих протокол TCP/IP.

Kaspersky Security Center позволяет удаленно запускать и останавливать Kaspersky Endpoint Security на клиентском компьютере, а также настраивать параметры работы программы.

В ЭТОМ РАЗДЕЛЕ

ЗАПУСК И ОСТАНОВКА KASPERSKY ENDPOINT SECURITY НА КЛИЕНТСКОМ КОМПЬЮТЕРЕ

- *Чтобы запустить или остановить Kaspersky Endpoint Security на клиентском компьютере, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые компьютеры** дерева консоли откройте папку с названием группы администрирования, в состав которой входит нужный вам клиентский компьютер.
3. В рабочей области выберите закладку **Компьютеры**.
4. В списке клиентских компьютеров выберите компьютер, на котором вы хотите запустить или остановить Kaspersky Endpoint Security.

5. Выполните одно из следующих действий:

   - По правой клавише мыши откройте контекстное меню клиентского компьютера. Выберите пункт **Свойства**.
   - В меню **Действия** выберите пункт **Свойства компьютера**.

   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 10 для Windows.

8. Выполните следующие действия:

   - Если вы хотите запустить Kaspersky Endpoint Security, справа от списка программ «Лаборатории Касперского» нажмите на кнопку  или выполните следующие действия:

     a. По правой клавише мыши откройте контекстное меню программы Kaspersky Endpoint Security 10 для Windows и выберите пункт **Свойства** или нажмите на кнопку **Свойства**, расположенную под списком программ «Лаборатории Касперского».

        Откроется окно **Параметры программы Kaspersky Endpoint Security 10 для Windows** на закладке **Общие**.

     b. Нажмите на кнопку **Запустить**.

   - Если вы хотите остановить работу Kaspersky Endpoint Security, справа от списка программ «Лаборатории Касперского» нажмите на кнопку  или выполните следующие действия:

     a. По правой клавише мыши откройте контекстное меню программы Kaspersky Endpoint Security 10 для Windows и выберите пункт **Свойства** или нажмите на кнопку **Свойства**, расположенную под списком программ.

        Откроется окно **Параметры программы Kaspersky Endpoint Security 10 для Windows** на закладке **Общие**.

     b. Нажмите на кнопку **Остановить**.

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 компьютеры** дерева консоли откройте папку с названием группы администрирования, в состав которой входит нужный вам клиентский компьютер.

3. В рабочей области выберите закладку **Компьютеры**.

4. В списке клиентских компьютеров выберите компьютер, для которого вы хотите настроить параметры Kaspersky Endpoint Security.

5. Выполните одно из следующих действий:

   - По правой клавише мыши откройте контекстное меню клиентского компьютера. Выберите пункт **Свойства**.
   - В меню **Действия** выберите пункт **Свойства компьютера**.

   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 10 для Windows.

8. Выполните одно из следующих действий:

   - По правой клавише мыши откройте контекстное меню программы Kaspersky Endpoint Security 10 для Windows. Выберите пункт **Свойства**.

   - Нажмите на кнопку **Свойства** под списком программ «Лаборатории Касперского».

   Откроется окно **Параметры программы «Kaspersky Endpoint Security 10 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 10 для Windows»** стандартны для программы Kaspersky Security Center, их описание 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 их изменение недоступно.

10. В окне **Параметры программы «Kaspersky Endpoint Security 10 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 одну или разные группы администрирования;
- задачи для наборов компьютеров, не входящих в группы администрирования.

Задачи для наборов компьютеров, не входящих в группы администрирования, выполняются только для указанных в параметрах задачи клиентских компьютеров. 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:

- **Инвентаризация**. В процессе выполнения задачи Kaspersky Endpoint Security собирает информацию обо всех исполняемых файлах программ, хранящихся на компьютерах.
- **Обновление**. В процессе выполнения задачи Kaspersky Endpoint Security обновляет базы и модули программы в соответствии с установленными параметрами обновления.
- **Откат обновления**. В процессе выполнения задачи Kaspersky Endpoint Security откатывает последнее обновление баз и модулей.
- **Поиск вирусов**. В процессе выполнения задачи Kaspersky Endpoint Security проверяет на вирусы и другие программы, представляющие угрозу, области компьютера, указанные в параметрах задачи.
- **Добавление ключа**. В процессе выполнения задачи Kaspersky Endpoint Security добавляет ключ, в том числе дополнительный, для активации программы.

Вы можете выполнять следующие действия над задачами:

- запускать, останавливать, приостанавливать и возобновлять выполнение задач;
- создавать новые задачи;
- изменять параметры задач.

Создание локальной задачи

Чтобы создать локальную задачу, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые компьютеры** дерева консоли откройте папку с названием группы администрирования, в состав которой входит нужный вам клиентский компьютер.
3. В рабочей области выберите закладку **Компьютеры**.
4. В списке клиентских компьютеров выберите компьютер, для которого вы хотите создать локальную задачу.
5. Выполните одно из следующих действий:
   - По правой клавише мыши откройте контекстное меню клиентского компьютера. Выберите пункт **Свойства**.
   - В меню **Действия** выберите пункт **Свойства компьютера**.

   Откроется окно свойств клиентского компьютера.

6. Выберите раздел **Задачи**.
7. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи.
8. 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 компьютеры** дерева консоли, если вы хотите создать групповую задачу для всех управляемых программой Kaspersky Security Center компьютеров.
   - В папке **Управляемые компьютеры** дерева консоли выберите папку с названием группы администрирования, в состав которой входят интересующие вас клиентские компьютеры. В рабочей области выберите закладку **Задачи**.
3. Выполните одно из следующих действий:
   - Нажмите на кнопку **Создать задачу**.
   - По правой клавише мыши откройте контекстное меню. Выберите пункт **Создать** → **Задачу**.

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

СОЗДАНИЕ ЗАДАЧИ ДЛЯ НАБОРА КОМПЬЮТЕРОВ

Чтобы создать задачу для набора компьютеров, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.
2. Откройте папку **Задачи для наборов компьютеров** дерева консоли.
3. Выполните одно из следующих действий:
   - Нажмите на кнопку **Создать задачу**.
   - По правой клавише мыши откройте контекстное меню. Выберите пункт **Создать** → **Задачу**.

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

Запуск, остановка, приостановка и возобновление выполнения задачи

Если на клиентском компьютере запущена программа (см. раздел «Запуск и остановка Kaspersky Endpoint Security на клиентском компьютере» на стр. 281) 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 компьютеры** дерева консоли откройте папку с названием группы администрирования, в состав которой входит нужный вам клиентский компьютер.
3. В рабочей области выберите закладку **Компьютеры**.
4. В списке клиентских компьютеров выберите компьютер, на котором вы хотите запустить / остановить / приостановить / возобновить выполнение локальной задачи.
5. Выполните одно из следующих действий:
   - По правой клавише мыши откройте контекстное меню клиентского компьютера. Выберите пункт **Свойства**.
   - В меню **Действия** выберите пункт **Свойства компьютера**.

   Откроется окно свойств клиентского компьютера.
6. Выберите закладку **Задачи**.

   В правой части окна отобразится список локальных задач.
7. Выберите локальную задачу, выполнение которой вы хотите запустить / остановить / приостановить / возобновить.
8. Выполните одно из следующих действий:
   - По правой клавише мыши откройте контекстное меню локальной задачи. Выберите пункт **Запустить** / **Остановить** / **Приостановить** / **Возобновить**.
   - Нажмите на кнопку  /  справа от списка локальных задач, чтобы запустить или остановить локальную задачу.
   - Нажмите на кнопку **Свойства** под списком локальных задач. Откроется окно **Свойства задачи <Название задачи>**. Далее на закладке **Общие** окна **Свойства задачи <Название задачи>** 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 компьютеры** дерева консоли 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 отобразится список групповых задач.

4. В списке групповых задач выберите групповую задачу, выполнение которой вы хотите запустить / остановить / приостановить / возобновить.

5. Выполните одно из следующих действий:

   - По правой клавише мыши откройте контекстное меню групповой задачи. Выберите пункт **Запустить** / **Остановить** / **Приостановить** / **Возобновить**.

   - Нажмите на кнопку  /  справа от списка групповых задач, чтобы запустить или остановить групповую задачу.

Чтобы запустить / остановить / приостановить / возобновить выполнение задачи для набора компьютеров, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.

2. В папке **Задачи для наборов компьютеров** дерева консоли выберите задачу для набора компьютеров, выполнение которой вы хотите запустить / остановить / приостановить / возобновить.

3. Выполните одно из следующих действий:

   - По правой клавише мыши откройте контекстное меню задачи для набора компьютеров. Выберите пункт **Запустить** / **Остановить** / **Приостановить** / **Возобновить**.

   - Нажмите на кнопку  /  справа от списка задач для наборов компьютеров, чтобы запустить или остановить задачу для набора компьютеров.

ИЗМЕНЕНИЕ ПАРАМЕТРОВ ЗАДАЧИ

Параметры задачи Kaspersky Endpoint Security, которые вы можете настроить через интерфейс Kaspersky Security Center, аналогичны параметрам задачи, которые вы можете настроить через локальный интерфейс Kaspersky Endpoint Security. Вы можете настроить параметры задачи на этапе создания задачи или изменить параметры задачи после ее создания.

Чтобы изменить параметры локальной задачи, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.

2. В папке **Управляемые компьютеры** дерева консоли откройте папку с названием группы администрирования, в состав которой входит нужный вам клиентский компьютер.

3. В рабочей области выберите закладку **Компьютеры**.

4. В списке клиентских компьютеров выберите компьютер, для которого вы хотите настроить параметры Kaspersky Endpoint Security.

5. Выполните одно из следующих действий:

   - По правой клавише мыши откройте контекстное меню клиентского компьютера. Выберите пункт **Свойства**.

   - В меню **Действия** выберите пункт **Свойства компьютера**.

   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. Выполните одно из следующих действий:

   - По правой клавише мыши откройте контекстное меню задачи. Выберите пункт **Свойства**.

   - Нажмите на кнопку **Свойства**.

   Откроется окно **Свойства: <Название локальной задачи>**.

9. В окне **Свойства: <Название локальной задачи>** выберите раздел **Параметры**.

10. Измените параметры локальной задачи.

11. В окне **Свойства: <Название локальной задачи>** нажмите на кнопку **OK**, чтобы сохранить внесенные изменения.

Чтобы изменить параметры групповой задачи, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.

2. В папке **Управляемые компьютеры** откройте папку с названием нужной группы администрирования.

3. В рабочей области выберите закладку **Задачи**.

   В нижней части панели задач отобразится список групповых задач.

4. Выберите в списке групповых задач нужную групповую задачу.

5. Выполните одно из следующих действий:

   - По правой клавише мыши откройте контекстное меню задачи. Выберите пункт **Свойства**.

   - Нажмите на кнопку **Изменить параметры задачи**, которая находится справа от списка групповых задач.

   Откроется окно **Свойства: <Название групповой задачи>**.

6. В окне **Свойства: <Название групповой задачи>** выберите раздел **Параметры**.

7. Измените параметры групповой задачи.

8. В окне **Свойства: <Название групповой задачи>** нажмите на кнопку **OK**, чтобы сохранить внесенные изменения.

Чтобы изменить параметры задачи для набора компьютеров, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.

2. В папке **Задачи для наборов компьютеров** дерева консоли выберите задачу для набора компьютеров, параметры которой вы хотите изменить.

3. Выполните одно из следующих действий:

   - По правой клавише мыши откройте контекстное меню задачи для набора компьютеров. Выберите пункт **Свойства**.

   - Нажмите на кнопку **Изменить параметры задачи**, которая находится справа от списка задач для наборов компьютеров.

Откроется окно **Свойства: <Название задачи для набора компьютеров>**.

4. В окне **Свойства: <Название задачи для набора компьютеров>** выберите раздел **Параметры**.

5. Измените параметры задачи для набора компьютеров.

6. В окне **Свойства: <Название задачи для набора компьютеров>** нажмите на кнопку **ОК**, чтобы сохранить внесенные изменения.

Все закладки окна свойств задач, кроме закладки **Параметры**, стандартны для программы Kaspersky Security Center. Их подробное описание вы можете прочитать в *Руководстве администратора для Kaspersky Security Center*. Закладка **Параметры** содержит специфические параметры Kaspersky Endpoint Security, ее содержимое варьируется в зависимости от выбранного типа и вида задачи.

УПРАВЛЕНИЕ ПОЛИТИКАМИ

Этот раздел содержит информацию о создании и настройке политик для Kaspersky Endpoint Security 10 для Windows. Более подробную информацию о концепции управления политиками через 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.

Параметры, заданные политикой, вы можете переопределять для отдельных компьютеров в группе администрирования. Вы можете это сделать локально, при помощи программы Kaspersky Endpoint Security. Локально вы можете переопределить значения только тех параметров, 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, и 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.

Вы можете выполнять следующие действия над политикой:

- создавать политику;
- изменять параметры политики;
- 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 компьютеры** дерева консоли, если вы хотите создать политику для всех управляемых программой Kaspersky Security Center компьютеров.
   - В папке **Управляемые компьютеры** дерева консоли 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. 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 компьютеры** дерева консоли 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. Выполните одно из следующих действий:
   - По правой клавише мыши вызовите контекстное меню политики. Выберите пункт **Свойства**.
   - Нажмите на кнопку **Изменить политику**, которая находится справа от списка политик.

   Откроется окно **Свойства: <Название политики>**.

Параметры политики для Kaspersky Endpoint Security 10 для Windows включают в себя параметры задач (см. раздел «Изменение параметров задачи» на стр. 287) и параметры программы (см. раздел «Настройка параметров Kaspersky Endpoint Security» на стр. 282). В разделах **Защита** и **Контроль** окна **Свойства: <Название политики>** представлены параметры задач, а в разделе **Дополнительные параметры** представлены параметры программы.

Для включения (см. раздел «Включение отображения параметров компонентов контроля и шифрования в политике Kaspersky Security Center» на стр. 291) отображения параметров шифрования данных и компонентов контроля в свойствах 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 **OK**, чтобы сохранить внесенные изменения.

ВКЛЮЧЕНИЕ ОТОБРАЖЕНИЯ ПАРАМЕТРОВ КОМПОНЕНТОВ КОНТРОЛЯ И ШИФРОВАНИЯ В ПОЛИТИКЕ KASPERSKY SECURITY CENTER

Чтобы включить отображение параметров компонентов контроля и 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 показываемой функциональности** выполните следующие действия:

   - установите флажок **Отображать компоненты контроля**, если вы хотите включить отображение параметров компонентов контроля в окне мастера 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 окне мастера создания политики Kaspersky Security Center и в ее свойствах.

4. Нажмите на кнопку **OK**.

ПРОСМОТР ЖАЛОБ ПОЛЬЗОВАТЕЛЕЙ В ХРАНИЛИЩЕ СОБЫТИЙ KASPERSKY SECURITY CENTER

Функциональность компонентов Контроль запуска программ (см. раздел «Изменение шаблонов сообщений Контроля запуска программ» на стр. 129), Контроль устройств (см. раздел «Изменение шаблонов сообщений Контроля устройств» на стр. 155) и Веб-Контроль (см. раздел «Изменение шаблонов сообщений Веб-Контроля» на стр. 169) предоставляет пользователям локальной сети организации, на компьютерах которых установлен Kaspersky Endpoint Security, возможность отправлять жалобы.

Возможны два способа доставки жалобы от пользователя:

- В виде события в хранилище событий Kaspersky Security Center. Сообщение-жалоба пользователя передается в хранилище событий Kaspersky Security Center, если Kaspersky Endpoint Security, установленный на компьютере пользователя, работает под активной политикой.

- В виде электронного письма. Письмо-жалоба пользователя передается в виде электронного письма, если Kaspersky Endpoint Security, установленный на компьютере пользователя, работает не под политикой или под мобильной политикой.

Чтобы просмотреть жалобу пользователя в хранилище событий Kaspersky Security Center, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.

2. Откройте папку **Выборки событий \ События \ Предупреждения** дерева консоли.

   В рабочей области Kaspersky Security Center отображается список всех событий-предупреждений, в том числе и жалоб, приходящих от пользователей локальной сети организации. Рабочая область Kaspersky Security Center располагается справа от дерева консоли.

3. Выберите в списке событий событие-жалобу.

4. Откройте свойства события одним из следующих способов:

   - Дважды нажмите левой клавишей мыши по событию в списке.

   - По правой клавише мыши откройте контекстное меню события. В контекстное меню события выберите пункт **Свойства**.

   - Нажмите на кнопку **Открыть свойства события** справа от списка событий.

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 сбора этих данных предназначена сеть *Kaspersky Security Network*.

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

Участие пользователей в Kaspersky Security Network позволяет «Лаборатории Касперского» оперативно собирать информацию о типах и источниках новых угроз, разрабатывать способы их нейтрализации, уменьшать количество ложных срабатываний.

Кроме того, участие в Kaspersky Security Network обеспечивает доступ к данным о репутации программ и веб-сайтов.

Когда вы участвуете в Kaspersky Security Network, определенная статистика, полученная в результате работы Kaspersky Endpoint Security на компьютере пользователя, автоматически отправляется в «Лабораторию Касперского». Также для дополнительной проверки в «Лабораторию Касперского» могут отправляться файлы (или их части), в отношении которых существует риск использования их злоумышленником для нанесения вреда компьютеру или данным.

Если компьютер работает под управлением Сервера администрирования Kaspersky Security Center, возможно использовать службу *KSN Proxy.*

KSN Proxy – это служба, обеспечивающая взаимодействие между инфраструктурой Kaspersky Security Network и компьютером пользователя.

Использование службы KSN Proxy предоставляет следующие возможности:

- Компьютер пользователя может выполнять запросы к KSN и передавать в KSN информацию, даже если он не имеет прямого доступа к интернету.
- Служба KSN Proxy кэширует 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 политик *Kaspersky Security Center* (см. раздел «*Управление политиками*» на стр. 289).

Сбор, обработка и хранение персональных данных пользователя не производится. О данных, которые Kaspersky Endpoint Security передает в Kaspersky Security Network, пользователь может прочитать в KSN-соглашении.

Участие в Kaspersky Security Network добровольное. Решение об участии в Kaspersky Security Network принимается на этапе установки Kaspersky Endpoint Security, его можно изменить его в любой момент (см. раздел «Включение и выключение использования Kaspersky Security Network» на стр. 294).

Включение и выключение использования Kaspersky Security Network

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

1. Откройте окно настройки параметров программы (на стр. 48).
2. В левой части окна в блоке **Дополнительные параметры** выберите раздел **Параметры KSN**.

   В правой части окна отобразятся параметры Kaspersky Security Network.
3. Выполните одно из следующих действий:
   - Установите флажок **Использовать KSN в продукте**, если вы хотите включить использование сервисов Kaspersky Security Network.
   - Снимите флажок **Использовать KSN в продукте**, если вы хотите выключить использование сервисов 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 **Репутационный сервис KSN**.

   Откроется окно **Kaspersky Security Network**.

   В левой части окна **Kaspersky Security Network** отображается режим подключения к сервисам Kaspersky Security Network в виде круглой кнопки **KSN**:
   - Если Kaspersky Endpoint Security подключен к сервисам Kaspersky Security Network, то кнопка **KSN** имеет зеленый цвет. Под кнопкой **KSN** отображается статус *Включено.* В правой части окна отображается статистика о репутации файлов и веб-ресурсов.

     Сбор 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 не подключен к сервисам Kaspersky Security Network, то кнопка **KSN** имеет серый цвет. Под кнопкой **KSN** отображается статус *Выключено*.

Подключение к Kaspersky Security Network может отсутствовать по следующим причинам:

- ваш компьютер не подключен к интернету;
- вы не участвуете в Kaspersky Security Network;
- программа не активирована или срок действия лицензии истек;
- выявлены проблемы, связанные с ключом. Например, ключ попал в черный список ключей.

ОБРАЩЕНИЕ В СЛУЖБУ ТЕХНИЧЕСКОЙ ПОДДЕРЖКИ

Этот раздел содержит информацию о способах получения технической поддержки и о том, какие условия требуются для получения помощи от Службы технической поддержки.

В ЭТОМ РАЗДЕЛЕ

Способы получения технической поддержки

Если вы не нашли решения вашей проблемы в документации к программе или в одном из источников информации о программе (см. раздел «Источники информации о программе» на стр. 15), рекомендуем обратиться в Службу технической поддержки «Лаборатории Касперского». Сотрудники Службы технической поддержки ответят на ваши вопросы об установке и использовании программы.

Прежде чем обратиться в Службу технической поддержки, ознакомьтесь с правилами предоставления технической поддержки (http://support.kaspersky.ru/support/rules).

Вы можете связаться со специалистами Службы технической поддержки одним из следующих способов:

- Позвонить по телефону. Этот способ позволяет проконсультироваться по телефону со специалистами русскоязычной или интернациональной Службы технической поддержки.
- Отправить запрос через систему Kaspersky CompanyAccount на веб-сайте Службы технической поддержки. Этот способ позволяет вам связаться со специалистами Службы технической поддержки через форму запроса.

Сбор информации для Службы технической поддержки

После того как вы проинформируете специалистов Службы технической поддержки 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 собрать необходимую информацию. Собранную информацию вы можете загрузить на сервер «Лаборатории Касперского» или сохранить на жесткий диск и отправить позже в удобное для вас время.

В этом разделе

Создание файла трассировки

Чтобы создать файл трассировки, выполните следующие действия:

1. Откройте главное окно программы (на стр. 46).
2. По ссылке **Поддержка**, расположенной в нижней части главного окна программы, откройте окно **Поддержка**.
3. В окне **Поддержка** нажмите на кнопку **Трассировка системы**.

   Откроется окно **Информация для поддержки**.
4. 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)**.
5. Чтобы запустить процесс трассировки, нажмите на кнопку **Включить**.
6. Воспроизведите ситуацию, в которой у вас возникает проблема.
7. Чтобы остановить процесс трассировки, нажмите на кнопку **Выключить**.

После создания файла трассировки вы можете перейти к загрузке результатов трассировки на сервер «Лаборатории Касперского» (см. раздел «Отправка файлов данных на сервер Службы технической поддержки» на стр. 297).

Отправка файлов данных на сервер Службы технической поддержки

Архив с информацией об операционной системе, трассировками и дампами памяти требуется отправить специалистам Службы технической поддержки «Лаборатории Касперского».

Чтобы загрузить файлы данных на сервер Службы технической поддержки, вам понадобится номер запроса. Этот номер доступен в вашем Персональном кабинете на веб-сайте Службы технической поддержки при наличии активного запроса.

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

1. Откройте главное окно программы (на стр. 46).
2. По ссылке **Поддержка**, расположенной в нижней части главного окна программы, откройте окно **Поддержка**.
3. В окне **Поддержка** нажмите на кнопку **Трассировка системы**.

Откроется окно **Информация для поддержки**.

4. В окне **Информация для поддержки** в блоке **Действия** нажмите на кнопку **Загрузить информацию для поддержки на сервер**.

   Откроется окно **Загрузка информации для поддержки на сервер**.

5. В окне **Загрузка информации для поддержки на сервер** установите флажки рядом с теми файлами, которые вы хотите отправить в Службу технической поддержки.

6. Нажмите на кнопку **Отправить**.

   Откроется окно **Номер запроса**.

7. В окне **Номер запроса** укажите номер, присвоенный вашему запросу при обращении в Службу технической поддержки через Персональный кабинет.

8. Нажмите на кнопку **ОК**.

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

Сохранение файлов данных на жестком диске

Если связаться со Службой технической поддержки по какой-либо причине невозможно, вы можете сохранить файлы данных на компьютере и впоследствии отправить их через Персональный кабинет.

Чтобы сохранить файлы данных на жестком диске, выполните следующие действия:

1. Откройте главное окно программы (на стр. 46).

2. По ссылке **Поддержка**, расположенной в нижней части главного окна программы, откройте окно **Поддержка**.

3. В окне **Поддержка** нажмите на кнопку **Трассировка системы**.

   Откроется окно **Информация для поддержки**.

4. В окне **Информация для поддержки** в блоке **Действия** нажмите на кнопку **Загрузить информацию для поддержки на сервер**.

   Откроется окно **Загрузка информации для поддержки на сервер**.

5. В окне **Загрузка информации для поддержки на сервер** установите флажки рядом с теми файлами данных, которые вы хотите отправить в Службу технической поддержки.

6. Нажмите на кнопку **Отправить**.

   Откроется окно **Номер запроса**.

7. В окне **Номер запроса** нажмите на кнопку **Отмена**.

8. В открывшемся окне подтвердите, что хотите сохранить файлы данных на жестком диске, нажав на кнопку **Да**.

   Откроется стандартное окно Microsoft Windows для сохранения архива.

9. В поле **Имя файла** задайте название архива и нажмите на кнопку **Сохранить**.

Техническая поддержка по телефону

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

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

Получение технической поддержки через Kaspersky CompanyAccount

Kaspersky CompanyAccount - это веб-сервис (https://companyaccount.kaspersky.com), предназначенный для отправки и отслеживания запросов в «Лабораторию Касперского».

Для доступа к Kaspersky CompanyAccount вам требуется зарегистрироваться на странице регистрации (https://support.kaspersky.com/companyaccount/registration) и получить логин и пароль. Для этого вам понадобится указать код активации или файл ключа.

В Kaspersky CompanyAccount вы можете выполнять следующие действия:

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

Электронный запрос в Службу технической поддержки

Вы можете отправить электронный запрос в Службу технической поддержки на русском, английском и других языках.

В полях формы электронного запроса вам нужно указать следующие сведения:

- тип запроса;
- название и номер версии программы;
- текст запроса.

Если требуется, вы также можете прикрепить к форме электронного запроса файлы.

Специалист Службы технической поддержки направляет ответ на ваш вопрос через систему Kaspersky CompanyAccount по адресу электронной почты, который вы указали при регистрации.

Электронный запрос в Вирусную лабораторию

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

Вы можете направлять в Вирусную лабораторию запросы следующих типов:

- *Неизвестная вредоносная программа* – вы подозреваете, что файл содержит вирус, но Kaspersky Endpoint Security не определяет этот файл как зараженный.

Специалисты Вирусной лаборатории анализируют присылаемый вредоносный код и при обнаружении неизвестного ранее вируса добавляют его описание в базу данных, доступную при обновлении антивирусных программ.

- *Ложное срабатывание антивируса* – Kaspersky Endpoint Security определяет файл как зараженный, но вы уверены, что файл не содержит вирусов

Вы также можете направлять запросы в Вирусную лабораторию со страницы с формой запроса (http://support.kaspersky.ru/virlab/helpdesk.html), не регистрируясь в Kaspersky CompanyAccount. При этом вам не требуется указывать код активации программы. Приоритет заявок, созданных через форму запроса, ниже, чем у запросов, созданных через Kaspersky CompanyAccount.

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 Windows-программ из состава продуктов компании. Для Novell®-, Unix- и Mac®-программ «Лаборатории Касперского» существуют 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.

Архив

Файл, «содержащий» в себе один или несколько файлов, которые в свою очередь также могут быть архивами.

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».

Базы

Базы данных, которые содержат информацию об угрозах компьютерной безопасности, известных «Лаборатории Касперского» на момент выпуска баз. Записи в базах позволяют обнаруживать в проверяемых объектах вредоносный код. Базы формируются специалистами «Лаборатории Касперского» и обновляются каждый час.

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 компьютеров, объединенных в соответствии с выполняемыми функциями и устанавливаемым на них набором программ «Лаборатории Касперского». Компьютеры 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

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 компьютера, Обновление баз.

Зараженный файл

Файл, внутри которого содержится вредоносный код (при проверке файла был обнаружен код известной угрозы). Специалисты «Лаборатории Касперского» не рекомендуют вам работать с такими файлами, поскольку это может привести к заражению вашего компьютера.

К

Карантин

Папка, в которую программа «Лаборатории Касперского» помещает обнаруженные возможно зараженные файлы. Файлы на карантине хранятся в зашифрованном виде, чтобы избежать их воздействия на компьютер.

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.

Ложное срабатывание

Ситуация, когда незараженный файл определяется программой «Лаборатории Касперского» как зараженный ввиду того, что его код напоминает код вируса.

М

Маска файла

Представление названия и расширения файла общими символами.

Для формирования маски файла можно использовать любые символы, допустимые в названиях файлов, в том числе специальные:

- ***** – символ, заменяющий нуль или более нуля любых символов;
- **?** – символ, заменяющий любой один символ.

Следует иметь в виду, что название и расширение файла всегда пишутся через точку.

Н

Нормализованная форма адреса веб-ресурса

Нормализованной формой адреса веб-ресурса называется текстовое представление адреса веб-ресурса, полученное в результате применения нормализации. Нормализация – процесс, в результате которого текстовое представление адреса веб-ресурса изменяется в соответствии с определенными правилами (например, исключение из текстового представления адреса веб-ресурса 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

Обновление

Процедура замены / добавления новых файлов (баз или программных модулей), получаемых с серверов обновлений «Лаборатории Касперского».

Объекты автозапуска

Набор программ, необходимых для запуска и корректной работы установленных на вашем компьютере операционной системы и программного обеспечения. Каждый раз при старте операционная система запускает эти объекты. Существуют вирусы, способные поражать именно такие объекты, что может привести, например, к блокированию запуска операционной системы.

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.

Помещение файлов на карантин

Способ обработки возможно зараженного файла, при котором доступ к файлу блокируется, и он перемещается из исходного местоположения в папку карантина, где сохраняется в закодированном виде, что исключает угрозу заражения.

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 первым 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.

Сигнатурный анализ

Технология обнаружения угроз, которая используют 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.

Ф

Фишинг

Вид интернет-мошенничества, заключающийся в рассылке электронных сообщений с целью кражи конфиденциальной информации, как правило, финансового характера.

Ч

Черный список адресов

Список электронных адресов, 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.

Файлам, в которых во время эвристического анализа обнаружен вредоносный код, присваивается статус *возможно зараженный*.

Эвристический анализатор

Функциональность Kaspersky Endpoint Security, выполняющая эвристический анализ.

ЗАО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

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

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

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

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

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

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

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

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

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

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

ИНФОРМАЦИЯ О СТОРОННЕМ КОДЕ

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

УВЕДОМЛЕНИЯ О ТОВАРНЫХ ЗНАКАХ

Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.

Adobe и Acrobat – товарные знаки или зарегистрированные в США и / или других странах товарные знаки Adobe Systems Incorporated.

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

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

Mac – зарегистрированный товарный знак Apple Inc.

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

Mozilla и Thunderbird – товарные знаки Mozilla Foundation.

Novell – товарный знак или зарегистрированный в США и / или других странах товарный знак Novell, Inc.

Radmin и Remote Administrator – зарегистрированные товарные знаки Famatech.

Словесный товарный знак Bluetooth и лого принадлежат Bluetooth SIG, Inc.

ПРЕДМЕТНЫЙ УКАЗАТЕЛЬ

I

А

Б

В

Г

Д

З

И

К

Л

М

Н

О

П

Р

С

У

Ф

Ш

Э