kaspersky

Kaspersky Endpoint Security для Mac

Руководство по эксплуатации

Версия программы: 12.2

Уважаемый пользователь!

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

Дата редакции документа: 10.07.2025

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

О «Лаборатории Касперского» (https://www.kaspersky.ru/about/company)

Kaspersky
Endpoint Security for Mac

Содержание

О Kaspersky Endpoint Security

Приложение Kaspersky Endpoint Security защищает компьютеры под управлением macOS от вредоносного ПО и других угроз компьютерной безопасности.

Защита от файловых угроз

Защита от файловых угроз предотвращает заражение файловой системы компьютера в режиме реального времени, перехватывая и анализируя попытки доступа к файлам. Узнать больше.

Защита от веб-угроз

Защита от веб-угроз предназначена для проверки информации, которая поступает на компьютер и отправляется с него через браузеры Safari, Chrome и Firefox по протоколам HTTP и HTTPS. Узнать больше.

Защита от почтовых угроз

Защита от почтовых угроз проверяет вложения входящих и исходящих сообщений электронной почты на наличие в них вредоносного ПО и других угроз. Компонент обеспечивает защиту компьютера с помощью баз вредоносного ПО, облачной службы Kaspersky Security Network и эвристического анализа. Узнать больше.

Защита от сетевых угроз

Защита от сетевых угроз предотвращает вторжение в операционную систему вашего компьютера. Этот компонент защищает от атак злоумышленников (использующих сканирование портов и подбор паролей), а также от вредоносных программ, устанавливаемых ими (в том числе от вредоносных программ, отправляющих персональные данные преступникам). Узнать больше.

Анализ поведения

Компонент Анализ поведения получает информацию о действиях программ на вашем компьютере и предоставляет ее другим компонентам защиты для повышения их производительности. Он также выполняет выбранное действие в ответ на активность вредоносного ПО. Узнать больше.

Защита от эксплойтов

Компонент Защита от эксплойтов отслеживает программный код, который использует уязвимости на компьютере для получения эксплойтом прав администратора или выполнения вредоносных действий. Узнать больше.

Проверка

Приложение Kaspersky Endpoint Security обнаруживает и обезвреживает вредоносное ПО и другие программы, представляющие угрозу компьютерной безопасности, по вашему запросу в заданной области проверки. Kaspersky Endpoint Security выполняет полную проверку компьютера, быструю проверку важных областей компьютера и проверку заданной области проверки. Узнать больше.

Обновление

Kaspersky Endpoint Security обновляет базы и модули приложения с серверов обновлений "Лаборатории Касперского", из точек распространения или из других источников обновлений, указанных системным администратором, и создает резервную копию всех обновляемых файлов на случай необходимости отката последнего произведенного обновления. Узнать больше.

Резервное хранилище

Kaspersky Endpoint Security каждый раз создает резервные копии зараженных файлов перед их лечением или удалением, чтобы обеспечить возможность восстановить файлы в случае необходимости. Узнать больше.

Отчеты

Kaspersky Endpoint Security создает отчеты о событиях и действиях, связанных с работой компонентов приложения. Узнать больше.

Уведомления

Kaspersky Endpoint Security использует уведомления, чтобы информировать вас о событиях, возникающих в работе приложения. Уведомления также могут сопровождаться звуковым оповещением. Узнать больше.

Центр защиты

Kaspersky Endpoint Security отображает сведения о состоянии защиты компьютера в Центре защиты. Центр защиты позволяет получить информацию о состоянии защиты компьютера и перейти к устранению проблем и угроз компьютерной безопасности. Узнать больше.

Удаленное управление приложением через Kaspersky Security Center

Kaspersky Security Center позволяет удаленно управлять защитой компьютеров, на которых установлен Kaspersky Endpoint Security: получать информацию о текущем состоянии защиты компьютера и удаленно устранять проблемы и угрозы компьютерной безопасности, включать и выключать компоненты защиты (Защиту от файловых угроз, Защиту от веб-угроз, Защиту от сетевых угроз, Анализ поведения), включать или выключать Веб-Контроль, компоненты Managed Detection and Response, Endpoint Detection and Response и Endpoint Detection and Response (KATA), запускать задачи проверки, обновлять базы программы, запускать шифрование загрузочного диска, а также управлять лицензиями и подписками Kaspersky Endpoint Security. Вы можете использовать следующие инструменты для управления Kaspersky Endpoint Security:

- Консоль администрирования Kaspersky Security Center. Узнать больше.
- Kaspersky Security Center Web Console и Cloud Console. Узнать больше.

Примечание: Функциональность, которую поддерживает Kaspersky Endpoint Security, зависит от используемого вами инструмента управления.

Шифрование дисков с помощью FileVault

Kaspersky Endpoint Security позволяет удаленно управлять шифрованием диска FileVault. Шифрование загрузочного диска на компьютере пользователя предотвращает доступ других пользователей к важной информации, которая хранится на диске.

Примечание. Функция Шифрование дисков с помощью FileVault доступна в Kaspersky Security Center 10 SP3 и более поздних версиях. За дополнительной информацией обратитесь в Службу технической поддержки "Лаборатории Касперского".

Веб-Контроль

Вы можете удаленно управлять доступом к сайтам, которые посещают пользователи на удаленном компьютере. Вы можете разрешить или заблокировать доступ к определенным веб-адресам или группам веб-адресов. Вы также можете разрешить или заблокировать доступ к определенным категориям сайтов.

Managed Detection and Response

Компонент Managed Detection and Response взаимодействует с решением Kaspersky Managed Detection and Response, которое обеспечивает непрерывный поиск, обнаружение и устранение угроз, направленных на вашу организацию. Узнать больше.

Endpoint Detection and Response

Компонент Endpoint Detection and Response обеспечивает взаимодействие с решением Kaspersky Endpoint Detection and Response. Решение сочетает автоматическое обнаружение угроз с возможностью реагирования на эти угрозы для противодействия сложным атакам, в том числе новым эксплойтам (exploits), программам-вымогателям (ransomware), бесфайловым атакам (fileless attacks), а также методам, использующим законные системные инструменты. Узнать больше.

Endpoint Detection and Response (KATA)

Компонент Endpoint Detection and Response (KATA) обеспечивает взаимодействие с решением Kaspersky Anti Targeted Attack Platform. Это решение оперативно обнаруживает сложные угрозы, таких как целевые атаки, сложные постоянные угрозы, атаки "нулевого дня" и другие. Узнать больше.

Что нового в этой версии

Эта справка применима для Kaspersky Endpoint Security для Mac версии 12.2.

В Kaspersky Endpoint Security появились следующие новые возможности и улучшения:

- Добавили новые компоненты: Защита от почтовых угроз, Контроль устройств, Сетевой экран, Откат вредоносных действий и Защита от эксплойтов.
- Теперь вы можете выполнить активацию компонента Managed Detection and Response из приложения Kaspersky Endpoint Security.
- Улучшена видимость действий по реагированию для деталей алертов.
- Теперь вы можете управлять компонентом Анализ поведения в Web Console.
- Мы добавили сводки по алертам.
- Теперь вы будете уведомлены о том, что объект является критическим системным объектом, прежде чем будут выполнены какие-либо действия по реагированию.
- Теперь вы можете редактировать файлы IOC непосредственно в Web Console при создании или редактировании параметров задачи Поиск IOC.

- Теперь вы можете перемещать обнаруженные объекты в Карантин из деталей алертов.
- Мы добавили предупреждения об ограниченных действиях для задачи Сетевой изоляции.
- Исправлен ряд ошибок и сделаны некоторые улучшения.

Сравнение функций Kaspersky Endpoint Security в зависимости от инструмента управления в Kaspersky Security Center

Функциональность, которую поддерживает Kaspersky Endpoint Security, зависит от используемого вами инструмента управления (см. таблицу ниже).

Вы можете использовать следующие инструменты для управления Kaspersky Endpoint Security:

- Консоль администрирования Kaspersky Security Center. Оснастка к Microsoft Management Console (MMC), которая устанавливается на рабочее место администратора Kaspersky Security Center.
- Kaspersky Security Center Web Console. Компонент Kaspersky Security Center, который устанавливается на Сервер администрирования. Вы можете работать в Web Console через браузер на любом компьютере, который имеет доступ к Серверу администрирования.
- Kaspersky Security Center Cloud Console. Облачная версия Kaspersky Security Center.

Сравнение функций Kaspersky Endpoint Security

Функция	Kaspersky Security Center		
	Консоль администрирования	Web Console	Cloud Console
Продвинутая защита			
Kaspersky Security Network	✓	✓	✓
Анализ поведения	✓	✓	
Защита от эксплойтов	✓	✓	
Откат вредоносных действий	✓	✓	
Базовая защита			
Защита от файловых угроз	✓	✓	✓
Защита от веб-угроз	✓	✓	✓
Защита от сетевых угроз	✓	✓	✓

Защита от почтовых угроз	✓	✓	
Сетевой экран	✓	✓	
Контроль безопасности			
Веб-Контроль	✓	✓	✓
Контроль устройств	✓	✓	
Шифрование данных			
Шифрование дисков с помощью FileVault	✓	✓	✓
Ключ восстановления	✓	✓	✓

Установка и удаление приложения

Комплект поставки

В комплект поставки входит дистрибутив Kaspersky Endpoint Security, содержащий следующие файлы:

- Файлы, необходимые для установки приложения всеми доступными способами.
- Файл license_<loc>.txt с текстом Лицензионного соглашения.

  В Лицензионном соглашении указано, на каких условиях вы можете использовать приложение.

Распакуйте дистрибутив приложения в формате ZIP, чтобы получить доступ к файлам.

Аппаратные и программные требования

Kaspersky Endpoint Security имеет следующие аппаратные и программные требования:

- тип процессора: Intel, Apple;
- 4 ГБ оперативной памяти (RAM);
- 5 ГБ свободного места на диске;
- Операционная система macOS 13-15;
- доступ в интернет.

Поддерживаемые браузеры:

- Safari;
- Chrome;
- Firefox.

Kaspersky Endpoint Security совместим со следующими средствами виртуализации:

- Parallels Desktop 16 для Mac Business Edition или более поздней версии;
- VMware Fusion 11.5 Professional;
- VMware Fusion 12 Professional;
- VMware Fusion 13 Pro.

Профили MDM могут быть развернуты на серверах Jamf и Apple. Если вы используете другие серверы, см. статью на сайте Службы технической поддержки (База знаний).

Вы можете управлять Kaspersky Endpoint Security через Kaspersky Security Center. Для управления Kaspersky Endpoint Security с помощью плагина управления Консоли администрирования Kaspersky Security Center и веб-плагина Kaspersky Security Center Web Console требуется Kaspersky Security Center 14.2 или более поздней версии.

Примечание. Для управления Kaspersky Endpoint Security для Mac 12.2 через Kaspersky Security Center вам нужно установить Агент администрирования версии 15 на удаленные компьютеры.

Подготовка к установке приложения

Перед установкой приложения на компьютер рекомендуется выполнить следующие действия:

- Убедитесь, что ваш компьютер соответствует аппаратным и программным требованиям.
- Удалите с компьютера Kaspersky Internet Security для Mac или другие программы для поиска вредоносного ПО, чтобы избежать возникновения системных конфликтов и снижения быстродействия операционной системы.

Примечание. Перед удаленной установкой Kaspersky Endpoint Security мы рекомендуем загрузить архив KES_for_macOS11_and_later.zip с сайта Службы технической поддержки "Лаборатории Касперского" и применить конфигурационный профиль KES_for_macOS11_and_later_profile.mobileconfig на клиентском компьютере с помощью инструментов Удаленного управления Apple. Это позволит Kaspersky Endpoint Security получить разрешения на установку расширения ядра и системного расширения, полный доступ к диску и разрешение на настройку сетевых соединений. Чтобы узнать больше о конфигурационном профиле и других опциях, посетите сайт Службы технической поддержки.

Установка Kaspersky Endpoint Security

Важно! Специалисты "Лаборатории Касперского" рекомендуют устанавливать Kaspersky Endpoint Security только способами, описанными в этой справке.

Вы можете установить Kaspersky Endpoint Security одним из следующих способов:

- Локально из дистрибутива, загруженного с сайта "Лаборатории Касперского".
- Удаленно с помощью Apple Remote Desktop.
- Удаленно через Консоль администрирования Kaspersky Security Center.
- Удаленно через Kaspersky Security Center Web Console или Kaspersky Security Center Cloud Console.

  Подробную информацию о развертывании приложений "Лаборатории Касперского" с помощью Kaspersky Security Center Web Console вы можете найти в справке Kaspersky Security Center. Подробную информацию о развертывании приложений "Лаборатории Касперского" с помощью Kaspersky Security Center Cloud Console вы можете найти в справке Kaspersky Security Center Cloud Console.

Стандартная установка Kaspersky Endpoint Security

1. Распакуйте файл дистрибутива приложения с расширением zip.
2. Откройте файл в формате dmg, входящий в состав файлов распакованного архива.
3. В открывшемся окне запустите установку приложения двойным щелчком мыши по кнопке **Установка Kaspersky Endpoint Security**.

   Запустится программа установки Kaspersky Endpoint Security.

4. Нажмите на кнопку **Установить**.

5. Следуйте шагам программы установки, чтобы выполнить установку.

Когда установка приложения завершится, Kaspersky Endpoint Security запустится автоматически. Перезагрузка компьютера не требуется.

Примечание. Если используется этот метод установки, компоненты Endpoint Detection and Response (KATA), Endpoint Detection and Response (Optimum) и Cloud Sandbox не устанавливаются.

Выборочная установка Kaspersky Endpoint Security

1. Распакуйте файл дистрибутива приложения с расширением zip.

2. Откройте файл в формате dmg, входящий в состав файлов распакованного архива.

3. В открывшемся окне запустите установку приложения двойным щелчком мыши по кнопке **Установка Kaspersky Endpoint Security**.

   Запустится программа установки Kaspersky Endpoint Security.

4. Нажмите на кнопку **Настройка**, установите или снимите флажки рядом с компонентами приложения, которые вы не хотите устанавливать, и нажмите на кнопку **Продолжить**.

5. Следуйте шагам программы установки, чтобы выполнить установку.

Когда установка приложения завершится, Kaspersky Endpoint Security запустится автоматически. Перезагрузка компьютера не требуется.

Удаленная установка Kaspersky Endpoint Security с помощью Apple Remote Desktop

1. На вашем Mac выберите **меню Apple** > **Системные настройки** > **Основные** > **Общий доступ**.

2. Установите флажок **Удаленное управление**.

3. На другом Mac, который вы хотите назначить сервером, установите Apple Remote Desktop. Вы можете найти дополнительную информацию об Apple Remote Desktop на сайте Службы поддержки Apple.

4. Откройте Apple Remote Desktop.

5. В левой части окна **Remote Desktop** нажмите **Scanner** и выберите устройства, на которые вы хотите установить Kaspersky Endpoint Security.

6. Нажмите на кнопку **Установить**.

7. В окне запроса учетных данных администратора введите имя администратора и пароль и нажмите **Добавить**.

8. Нажмите на кнопку + и выберите DMG-файл с дистрибутивом Kaspersky Endpoint Security.

9. Нажмите на кнопку **Установить**.

Установка Kaspersky Endpoint Security запустится на выбранных устройствах.

Подготовка приложения к работе

После установки Kaspersky Endpoint Security вы можете выполнить следующие действия:

- Активировать Kaspersky Endpoint Security. После активации приложения Kaspersky Endpoint Security начнет защищать ваш компьютер, вы сможете регулярно обновлять базы и модули приложения, запускать задачи поиска вредоносного ПО, а также отправлять запросы в Службу технической поддержки.

  Компонент Managed Detection and Response активируется отдельно в Консоли администрирования Kaspersky Security Center или в Web Console.

  Если компонент Endpoint Detection and Response не поддерживается вашей текущей лицензией, вам необходимо активировать Kaspersky Endpoint Detection and Response отдельно.

- Проверить состояние защиты компьютера.

- Обновить Kaspersky Endpoint Security.

- Запустить задачу поиска вредоносного ПО.

Удаление Kaspersky Endpoint Security

1. Откройте файл в формате dmg, входящий в дистрибутив приложения.
2. В открывшемся окне запустите удаление приложения двойным щелчком мыши по кнопке **Удаление Kaspersky Endpoint Security**.

   Запустится программа удаления Kaspersky Endpoint Security.
3. В окне программы удаления нажмите на кнопку **Удалить**.
4. В окне запроса учетных данных администратора компьютера введите имя администратора и пароль и подтвердите, что вы хотите удалить Kaspersky Endpoint Security.

   Начнется удаление Kaspersky Endpoint Security.
5. Прочитайте информацию о завершении удаления и нажмите на кнопку **Выйти**, чтобы закрыть программу удаления.

Приложение Kaspersky Endpoint Security теперь удалено с вашего компьютера. По завершении удаления приложения перезагрузка компьютера не требуется.

Первый запуск приложения

Kaspersky Endpoint Security запускается на компьютере сразу после установки приложения. Чтобы сразу начать защищать ваш Mac, приложение попросит вас выполнить следующие действия по ее настройке:

- Предоставить Kaspersky Endpoint Security необходимые разрешения, чтобы защитить ваш Mac от вредоносных программ, сетевых атак и угроз в интернете.

  Подробную информацию о разрешениях, которые вы предоставляете, вы можете узнать, нажав на кнопку ?.
- Активировать Kaspersky Endpoint Security.

Примечание. Для настройки Kaspersky Endpoint Security требуется подключение к интернету.

Первый запуск Kaspersky Endpoint Security

1. Для правильной работы Защиты от файловых угроз и Защиты от веб-угроз в окне **Базовая защита** выполните следующие действия:

- Если вы хотите, чтобы приложение Kaspersky Endpoint Security работало правильно, разрешите проверку каждого файла на вашем Mac. Для этого нажмите на кнопку **Разрешить** рядом с элементом **Полный доступ к диску** и следуйте инструкциям на экране.

- Если вы хотите, чтобы Kaspersky Endpoint Security проверял веб-адреса и сетевые пакеты до того, как они нанесут вред вашему Mac, установите системное расширение. Для этого нажмите на кнопку **Установить** рядом с элементом **Системное расширение** и следуйте инструкциям на экране.

- Если вы хотите, чтобы системное расширение работало корректно, разрешите фильтрацию сетевого трафика. Для этого нажмите на кнопку **Разрешить** рядом с элементом **Фильтрация сетевого трафика** и следуйте инструкциям на экране.

- Если вы хотите, чтобы приложение Kaspersky Endpoint Security искало вредоносные программы и интернет-угрозы в зашифрованном HTTPS-трафике, установите доверенный сертификат. Для этого нажмите на кнопку **Установить** рядом с элементом **Надежный сертификат** и следуйте инструкциям на экране.

Важно! Приложение Kaspersky Endpoint Security не будет работать правильно без предоставления этих разрешений. Вам нужно предоставить все разрешения в окне **Базовая защита**.

2. Нажмите на кнопку **Продолжить**.

Откроется главное окно приложения.

Интерфейс приложения Kaspersky Endpoint Security

Главное окно приложения

Как открыть главное окно приложения

В строке меню нажмите на значок приложения и выберите в контекстном меню значка приложения пункт **Kaspersky Endpoint Security**.

Главное окно приложения Kaspersky Endpoint Security содержит элементы интерфейса, обеспечивающие доступ к основным функциям приложения.

Главное окно приложения разделено на две части:

- Левая часть содержит боковую панель, которая позволяет перемещаться по приложению и быстро получать доступ к его основным функциям.
- Центральная часть отображает содержимое раздела, выбранного на боковой панели, и позволяет управлять данными.

Боковая панель

Боковая панель главного окна приложения имеет следующие опции:

Мониторинг	Нажмите, чтобы открыть страницу **Мониторинг**, на которой представлена информация о том, что Kaspersky Endpoint Security делает для защиты вашего компьютера.
Центр защиты	Нажмите, чтобы просмотреть статус защиты вашего компьютера. Узнать больше.
Безопасность	Нажмите, чтобы просмотреть рабочее состояние установленных компонентов. Узнать больше.
Проверка	Нажмите, чтобы управлять задачами сканирования. Узнать больше.
Обновление	Нажмите, чтобы управлять задачами обновления. Узнать больше.
Лицензия	Нажмите, чтобы активировать приложение или просмотреть информацию о вашей лицензии. Узнать больше.

Элементы управления на странице **Мониторинг**

На странице **Мониторинг** отображается индикатор состояния защиты, а также предоставляется информация о том, что Kaspersky Endpoint Security делает для защиты вашего компьютера, и содержатся следующие элементы управления.

Центр защиты	Сообщает о проблемах с защитой компьютера. Узнать больше.
Отчеты	Позволяет просматривать события, произошедшие в процессе работы приложения, отдельных компонентов и задач. Узнать больше.
Резервное хранилище	Позволяет просмотреть список сохраненных копий зараженных файлов, удаленных приложением. Узнать больше. Узнать больше.

Обнаружение угроз	Позволяет просматривать информацию о технологиях обнаружения угроз, применяемых Kaspersky Endpoint Security, и количестве угроз, обнаруженных с помощью этих технологий.
Kaspersky Security Network	Отображает статус соединения между Kaspersky Endpoint Security и Kaspersky Security Network, а также глобальную статистику Kaspersky Security Network.

Значок Kaspersky Endpoint Security

Сразу после установки Kaspersky Endpoint Security в строке меню появляется значок приложения. Если приложение активировано, значок приложения служит индикатором состояния работы приложения. Если значок приложения активен ( ), все или некоторые компоненты защиты включены. Если значок приложения неактивен ( ), все компоненты защиты выключены.

Открытие контекстного меню значка приложения

В строке меню нажмите на значок приложения.

По умолчанию значок приложения всегда отображается в строке меню. Вы можете удалить значок приложения из строки меню.

Удаление значка приложения из строки меню

1. В строке меню нажмите на значок приложения и выберите пункт **Настройки**.

   Откроется окно настройки приложения.

2. На вкладке **Интерфейс** в блоке **Значок приложения** снимите флажок **Отображать в строке меню**.

Когда вы открываете окно приложения, значок Kaspersky Endpoint Security также отображается в панели **Dock**.

Из контекстного меню значка приложения вы можете перейти в главное окно приложения и выполнить следующие действия:

- отключить защиту компьютера;
- возобновить защиту компьютера;

- открыть Центр защиты;
- запустить задачу быстрой проверки;
- запустить обновление;
- открыть окно настройки приложения;
- завершить работу Kaspersky Endpoint Security.

Окно настройки приложения

Как открыть окно настройки приложения

Выполните одно из следующих действий:

- В строке меню нажмите на значок приложения и выберите пункт **Настройки**.
- В строке меню выберите **Kaspersky Endpoint Security** > **Настройки**.
- Если приложение Kaspersky Endpoint Security запущено, нажмите на значок приложения в панели **Dock** и выберите **Настройки**.

Для быстрого доступа к параметрам приложения вы можете использовать следующие вкладки, расположенные в верхней части окна настройки приложения:

- Базовая. На этой вкладке вы можете включить или выключить защиту компьютера и настроить параметры Защиты от файловых угроз, Защиты от веб-угроз, а также Защиты от сетевых угроз.
- Проверка. На этой вкладке вы можете настроить параметры задач проверки и запуск проверки по расписанию.
- Угрозы. На этой вкладке вы можете выбрать категории обнаруживаемых объектов, сформировать Доверенную зону и настроить параметры резервного хранилища.
- Дополнительно. На этой вкладке вы можете присоединиться к участию в Kaspersky Security Network или отказаться от участия.
- Обновление. На этой вкладке вы можете настроить параметры обновления приложения или вернуться к использованию предыдущей версии баз.
- Интерфейс. На этой вкладке вы можете настроить параметры значка Kaspersky Endpoint Security, уведомлений, отчетов, а также включить или выключить запись отладочной

информации в файл трассировки.

Вы можете запретить пользователям, не имеющим прав администратора компьютера, изменять параметры работы Kaspersky Endpoint Security с помощью кнопки  . Кнопка расположена в нижней части окна настройки приложения. Чтобы изменять параметры работы Kaspersky Endpoint Security, вам нужно ввести учетные данные администратора компьютера.

По кнопке ? вы можете открыть справку Kaspersky Endpoint Security, в которой описаны все параметры текущего окна приложения. Также вы можете открыть справку для текущего окна приложения, выбрав в меню **Справка** пункт **Открыть справку для этого окна**.

Об уведомлениях

Kaspersky Endpoint Security отображает окна уведомлений, чтобы информировать вас о событиях, возникающих в работе приложения. Уведомления могут появляться в Центре уведомлений. Появление уведомлений зависит от настроек Центра уведомлений операционной системы.

События, возникающие в работе Kaspersky Endpoint Security, по уровню важности делятся на три типа:

- *Критические* – события, представляющие серьезную угрозу безопасности компьютера (обнаружение вредоносных объектов, уязвимостей, проблем в работе Kaspersky Endpoint Security). Критические события требуют вашего немедленного внимания. Рекомендуется не выключать уведомления о возникновении критических событий.

- *Важные* – события, которые не требуют ваших немедленных действий, но в дальнейшем могут представлять угрозу для безопасности компьютера.

- *Информационные* – события, носящие информационный характер.

Выключение уведомлений

1. В строке меню нажмите на значок приложения и выберите пункт **Настройки**.

   Откроется окно настройки приложения.

2. На вкладке **Интерфейс** в блоке **Уведомления** снимите флажок **Уведомлять о событиях**.

Включение записи некритических событий

1. В строке меню нажмите на значок приложения и выберите пункт **Настройки**.

   Откроется окно настройки приложения.

2. На вкладке **Интерфейс**, в блоке **Отчеты** установите флажок **Записывать некритические события**, чтобы получать уведомления об информационных событиях Kaspersky Endpoint Security.

Вне зависимости от того, включена или выключена доставка уведомлений, Kaspersky Endpoint Security записывает в отчеты приложения информацию о всех событиях, возникающих в работе приложения.

Уведомления могут сопровождаться звуковым оповещением (например, уведомления об обнаружении вредоносного ПО). Вы можете отключить звуковые оповещения.

Запись некритических событий значительно увеличивает размер файла отчета. События записываются только для Защиты от файловых угроз.

Отключение звукового оповещения при появлении уведомлений

1. В строке меню нажмите на значок приложения и выберите пункт **Настройки**.

   Откроется окно настройки приложения.

2. На вкладке **Интерфейс** в блоке **Уведомления** снимите флажок **Воспроизводить звуковое уведомление при обнаружении вредоносных программ**.

Если при возникновении события вам нужно выполнить действие, Kaspersky Endpoint Security отображает окно уведомления. Например, когда приложение обнаруживает вредоносный объект, оно предлагает вам удалить объект или лечить его. Окно уведомления исчезает с экрана только после выбора одного из предлагаемых действий.

Лицензирование приложения Kaspersky Endpoint Security

О Лицензионном соглашении

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

Важно! Внимательно прочитайте Лицензионное соглашение, прежде чем приступать к использованию приложения.

Вы можете ознакомиться с условиями Лицензионного соглашения следующими способами:

- во время установки Kaspersky Endpoint Security;
- прочитав файл license.txt в папке установки приложения.

Устанавливая Kaspersky Endpoint Security, вы подтверждаете, что понимаете и принимаете условия Лицензионного соглашения. Если вы не принимаете условия Лицензионного соглашения, отмените установку Kaspersky Endpoint Security и не используйте приложение.

О лицензии

Лицензия – это ограниченное по времени право на использование Kaspersky Endpoint Security, предоставляемое вам на условиях заключенного Лицензионного договора (Лицензионного соглашения).

Список доступных функций и срок использования приложения зависят от лицензии, по которой используется приложение.

Предусмотрены следующие типы лицензий:

- *Пробная*

  Бесплатная лицензия, предназначенная для ознакомления с приложением. Пробная лицензия имеет небольшой срок действия.

  По истечении срока действия пробной лицензии Kaspersky Endpoint Security прекращает выполнять все свои функции. Чтобы продолжить использование приложения, вам нужно приобрести коммерческую лицензию.

  Вы можете использовать приложение по пробной лицензии только в течение одного срока пробного использования.

- *Коммерческая*

  Платная лицензия.

  По истечении срока действия коммерческой лицензии приложение прекращает выполнять свои основные функции. Для продолжения работы Kaspersky Endpoint Security вам нужно продлить срок действия коммерческой лицензии. После истечения срока действия лицензии вы не можете далее использовать приложение и должны удалить его с устройства.

  Рекомендуется продлевать срок действия лицензии не позднее даты его окончания, чтобы обеспечить непрерывность защиты устройства от угроз компьютерной безопасности.

О подписке

Подписка на Kaspersky Endpoint Security – это заказ на использование приложения с выбранными параметрами (дата окончания подписки, количество защищаемых устройств). Подписку на Kaspersky Endpoint Security можно зарегистрировать у поставщика услуг (например, у интернет-провайдера). Вы можете управлять подпиской через личный кабинет на сайте поставщика услуг. Например, вы можете продлить или отменить вашу подписку, уменьшить срок подписки, а также изменить количество защищаемых устройств.

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

Если вы используете приложение по ограниченной подписке, по истечении срока действия подписки вам будет предоставлен льготный период для ее продления. В течение льготного периода приложение работает в режиме полной функциональности.

По истечении срока действия подписки на обновления и по истечении льготного периода для продления подписки Kaspersky Endpoint Security продолжает работу, но прекращает обновлять базы приложения.

По истечении срока действия подписки на обновления и защиту и по истечении льготного периода для продления подписки Kaspersky Endpoint Security прекращает защищать ваш компьютер.

Чтобы использовать Kaspersky Endpoint Security по подписке, нужно добавить код активации, предоставленный поставщиком услуг. При использовании приложения по подписке вы не можете применить другой код активации для продления подписки. Другой код активации можно применить только после окончания срока действия подписки или в случае отмены подписки. Чтобы отказаться от подписки, свяжитесь с поставщиком услуг, у которого вы приобрели Kaspersky Endpoint Security.

Примечание. Другой код активации для подписки можно применить только после удаления активного ключа. Подписка не имеет файла ключа. Вы не можете добавить подписку в качестве резервного ключа. Резервный ключ не может быть добавлен при использовании приложения по подписке.

Если вы уже используете Kaspersky Endpoint Security по действующей лицензии, но хотите перейти на использование приложения по подписке, удалите активный ключ, чтобы приложение можно было активировать с помощью ключа по подписке. Код активации, с помощью которого ранее было активировано приложение, можно применить на другом компьютере.

Примечание. Варианты подписки, доступные у разных поставщиков услуг, могут отличаться. Некоторые поставщики услуг могут не предоставлять льготный период на продление подписки.

О Лицензионном сертификате

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

В Лицензионном сертификате содержится следующая информация о предоставляемой лицензии:

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

О ключе

Ключ – последовательность бит, с помощью которой вы можете активировать и затем использовать приложение в соответствии с условиями Лицензионного соглашения. Ключ создается специалистами "Лаборатории Касперского".

Вы можете добавить ключ в приложение одним из следующих способов: применить *файл ключа* или ввести *код активации*. Ключ отображается в интерфейсе приложения в виде уникальной буквенно-цифровой последовательности, после того как вы добавили его в приложение.

Ключ может быть заблокирован "Лабораторией Касперского", если условия Лицензионного соглашения нарушены. Если ключ заблокирован, для работы приложения требуется добавить другой ключ.

Ключ может быть активным и резервным.

Активный ключ – ключ, используемый в текущий момент для работы приложения. Активный ключ может быть добавлен для пробной или коммерческой лицензии, или подписки. В приложении не может быть больше одного активного ключа.

Резервный ключ – ключ, подтверждающий право на использование приложения, но не используемый в текущий момент. Резервный ключ автоматически становится активным, когда заканчивается срок действия лицензии, связанной с текущим активным ключом. Резервный ключ может быть добавлен только при наличии активного ключа.

Ключ для пробной лицензии может быть добавлен только в качестве активного ключа. Ключ для пробной лицензии не может быть добавлен в качестве резервного ключа. Также нельзя добавить резервный ключ, если используется ключ для пробной лицензии.

О коде активации

Код активации – это уникальная последовательность из двадцати латинских букв и цифр. Вы вводите код активации, чтобы добавить лицензионный ключ для активации Kaspersky Endpoint Security. Вы получаете код активации по указанному вами адресу электронной почты после приобретения Kaspersky Endpoint Security или после заказа пробной версии Kaspersky Endpoint Security.

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

Если код активации был потерян после активации приложения, свяжитесь с партнером "Лаборатории Касперского", у которого вы приобрели лицензию.

О файле ключа

Файл ключа – файл с расширением .key, предоставляемый вам "Лабораторией Касперского". Файл ключа предназначен для активации приложения путем добавления лицензионного ключа.

Вы получаете файл ключа по указанному вами адресу электронной почты после приобретения Kaspersky Endpoint Security или после заказа пробной версии Kaspersky Endpoint Security.

Вам не нужно подключаться к серверам активации "Лаборатории Касперского» для активации приложения с помощью файла ключа.

Вы можете восстановить файл ключа, если он был случайно удален. Вам может потребоваться файл ключа, например, для регистрации в Kaspersky CompanyAccount.

Чтобы восстановить файл ключа, выполните любое из следующих действий:

- Обратитесь к продавцу лицензии.

- Получите файл ключа с сайта "Лаборатории Касперского" с помощью имеющегося у вас кода активации.

О предоставлении данных

Лицензионное соглашение

В случае активации Kaspersky Endpoint Security кодом активации, для целей проверки правомерности использования приложения и для предоставления статистической информации о распространении и использовании продуктов "Лаборатории Касперского", вы соглашаетесь в ходе использования Kaspersky Endpoint Security предоставлять в автоматическом режиме следующую информацию:

- тип, версию и локализацию установленного ПО;
- версии установленных обновлений ПО;
- идентификатор компьютера и идентификатор установки ПО на компьютере;
- код активации и уникальный идентификатор активации текущей лицензии;
- тип, версию и разрядность операционной системы;
- название виртуальной среды, если ПО установлено в виртуальной среде;
- идентификаторы компонентов ПО, активных на момент предоставления информации;
- поддерживаемый источник данных;
- таймаут;
- дату и время, установленные на компьютере пользователя;
- версию протокола;
- тип содержимого протокола;
- длину содержимого протокола;
- тип используемой компрессии данных;
- тип подписи тикета активации;
- идентификатор Регионального Центра Активации;
- контрольную сумму кода активации, рассчитанную по алгоритму SHA1;

- хеш-сумму тела тикета, рассчитанную по алгоритму SHA1;
- дату и время создания лицензионного тикета;
- идентификатор активации лицензии;
- идентификатор тикета действующей лицензии;
- идентификатор последовательности лицензионного тикета;
- дату и время активации лицензии;
- дату и время истечения срока действия лицензии;
- статус лицензии;
- версию лицензии;
- уникальный идентификатор компьютера пользователя;
- версию заголовка лицензионного тикета;
- название программы;
- тип передаваемых данных;
- версию схемы передаваемых данных;
- полную версию операционной системы;
- описание используемой виртуальной машины;
- список идентификаторов совместимых приложений.

Если получение обновлений выполняется с серверов "Лаборатории Касперского", для целей улучшения качества работы механизма обновления, вы соглашаетесь периодически предоставлять следующую информацию для идентификации программы во время обновления баз и модулей:

- идентификатор ПО (AppID);
- идентификатор действующей лицензии;
- уникальный идентификатор установки ПО (InstallationID);
- уникальный идентификатор запуска задачи обновления (SessionID);

- версию ПО (BuildInfo).

Положение о Kaspersky Security Network (KSN)

Использование KSN может ускорить реакцию ПО на угрозы информационной и сетевой безопасности. Заявленная цель достигается посредством:

- определения репутации проверяемых объектов;
- выявления новых и сложных для обнаружения угроз информационной и сетевой безопасности, а также их источников;
- оперативного принятия мер по повышению уровня защиты информации, хранимой и обрабатываемой Пользователем с использованием Компьютера;
- уменьшения вероятности ложных срабатываний;
- повышения эффективности работы компонентов ПО;
- расследования заражения на компьютере пользователя;
- улучшения быстродействия продуктов "Лаборатории Касперского";
- получения справочной информации о количестве объектов с известной репутацией;
- своевременного выявления и исправления ошибок, связанных с механизмом установки, удаления и обновления продукта.

При использовании KSN "Лаборатория Касперского" получает и обрабатывает данные в автоматическом режиме. Состав передаваемых пользователем данных зависит от типа установленной лицензии и заданных настроек использования Kaspersky Security Network.

Если вы используете лицензию для 1-4 узлов, то при использовании Kaspersky Security Network "Лаборатория Касперского" будет получать и обрабатывать следующие данные в автоматическом режиме:

- Информация об используемой лицензии: тип лицензии и срок ее действия, количество дней до истечения срока действия лицензии, идентификатор партнера, у которого приобретена лицензия, идентификатор регионального центра активации, контрольная сумма кода активации, хеш-сумма тела тикета, рассчитанная по алгоритму SHA1, дата и время создания лицензионного тикета, идентификатор информации о лицензии, идентификатор лицензионного тикета, идентификатор последовательности лицензионного тикета, уникальный идентификатор компьютера пользователя, дата начала и окончания периода валидности лицензионного тикета, текущее состояние лицензионного тикета, версия заголовка тикета, версия лицензии, идентификатор сертификата подписи заголовка тикета, контрольная сумма файла ключа, серийный номер подписчика заголовка тикета, токен авторизации.

- Полная версия установленного ПО; тип установленного ПО; идентификатор обновления ПО; идентификатор службы репутации; идентификатор типа протокола; идентификатор регионального центра активации; версия списка отозванных заключений службы ПО; идентификатор сработавшей записи в антивирусных базах ПО; временная метка сработавшей записи в антивирусных базах ПО; тип сработавшей записи в антивирусных базах ПО; уникальный идентификатор установки ПО на компьютере; дата активации лицензии; дата окончания срока действия лицензии; идентификатор лицензии; статус лицензии, по которой используется ПО; тип контрольной суммы обрабатываемого объекта; название обнаруженной вредоносной программы или легальной программы, которая может быть использована для нанесения вреда устройству или данным пользователя; контрольная сумма обрабатываемого объекта; контрольная сумма кода активации ПО; полная версия ПО; уникальный идентификатор устройства; идентификатор ПО; контрольная сумма файла ключа, которым активировано ПО; идентификатор информационной модели, примененной при предоставлении лицензии на использование ПО; идентификатор сертификата, которым подписан заголовок лицензионного тикета ПО; дата и время создания лицензионного тикета ПО; контрольная сумма лицензионного тикета ПО; версия лицензионного тикета ПО; версия кода активации ПО; формат данных в запросе к инфраструктуре Правообладателя; идентификатор тикета текущей лицензии; идентификатор компонента ПО; результат действий, выполненных ПО; код ошибки; адрес веб-службы, на который осуществлялось обрабатываемое обращение (веб-адрес, IP); номер порта; веб-адрес источника запроса к веб-службе (referrer); публичный ключ сертификата; отпечаток цифрового сертификата проверяемого объекта и алгоритм хеширования.

Если вы используете лицензию для 5 и более узлов, то при использовании Kaspersky Security Network "Лаборатория Касперского" будет получать и обрабатывать следующие данные в автоматическом режиме:

- Информация о версиях установленной на компьютере операционной системы (ОС) и установленных пакетов обновлений, версия и контрольные суммы (MD5, SHA2-256, SHA1) файла ядра ОС, параметры режима работы ОС; версия ОС, номер сборки ОС, номер обновления ОС, редакция ОС, расширенная информация о редакции ОС; версия пакета обновления ОС; дата и время запуска ОС; время задержки обработки события о совершении действия в ОС в подсистеме поведенческого анализа; количество задержанных событий текущего типа, совершенных в ОС; время задержки обработки события о совершении действия в ОС в подсистеме проактивной защиты; количество обработанных событий, совершенных в ОС; количество обработанных синхронных событий, совершенных в ОС; суммарная задержка всех событий текущего типа, совершенных в ОС; время задержки обработки события о совершении действия в ОС в подсистеме постоянного хранения событий; суммарная задержка всех событий, совершенных в ОС; количество ожидающих синхронных событий, совершенных в ОС; дата и время получения события о совершении действия в ОС.

- Информация о последней неуспешной перезагрузке ОС: количество неуспешных перезагрузок.

- Информация об установленном ПО Правообладателя и состоянии антивирусной защиты компьютера: идентификатор установки ПО (PCID); версия записи в базе данных ПО; уникальный идентификатор установки программы на компьютере, тип программы, идентификатор типа программы, полная версия установленной программы, идентификатор версии настроек программы, идентификатор типа компьютера, уникальный идентификатор компьютера, на котором установлена программа, уникальный идентификатор пользователя в службах Правообладателя, язык локали и ее рабочее состояние, версия установленных компонентов ПО и их рабочее состояние, версия протокола, который используется для подключения к службам Правообладателя; полная версия установленного ПО; тип установленного ПО; идентификатор обновления ПО; идентификатор службы репутации; идентификатор типа протокола; идентификатор регионального центра активации; версия списка отозванных заключений службы ПО; идентификатор сработавшей записи в антивирусных базах ПО; временная метка сработавшей записи в антивирусных базах ПО; тип сработавшей записи в антивирусных базах ПО; уникальный идентификатор установки ПО на компьютере; дата активации лицензии; дата окончания срока действия лицензии; идентификатор лицензии; статус лицензии, по которой используется ПО; тип контрольной суммы обрабатываемого объекта; название обнаруженной вредоносной программы или легальной программы, которая может быть использована для нанесения вреда устройству или данным пользователя; контрольная сумма обрабатываемого объекта; контрольная сумма кода активации ПО; полная версия ПО; идентификатор ПО; контрольная сумма файла ключа, которым активировано ПО; идентификатор информационной модели, примененной при предоставлении лицензии на использование ПО; идентификатор сертификата, которым подписан заголовок лицензионного тикета ПО; дата и время создания лицензионного тикета ПО; контрольная сумма лицензионного тикета ПО; версия лицензионного тикета ПО; версия кода активации ПО; формат данных в запросе к инфраструктуре Правообладателя; идентификатор тикета текущей лицензии; идентификатор компонента ПО; результат действий, выполненных ПО; код ошибки; адрес веб-службы, на который осуществлялось обрабатываемое обращение (веб-адрес, IP); номер порта; веб-адрес источника запроса к веб-службе (referrer); количество циклов обновления и применения антивирусных баз; дата и время последнего обновления и применения антивирусных баз; дата и время выпуска баз ПО; версия компонента ПО; идентификатор обновления ПО; тип установленного ПО; дата и время запуска компонента мониторинг активности; дата и время установки ПО; вероятность отправки статистики компонентом мониторинг активности; код события, обрабатываемого компонентом мониторинг активности дольше стандартного времени обработки; время обработки события в базах, обработка которого компонентом мониторинг активности длилась дольше стандартного времени; максимально допустимое время обработки события компонентом мониторинг активности; время обработки события, обработка которого компонентом мониторинг активности длилась дольше стандартного времени; общее количество событий, обработка которых компонентом мониторинг активности длилась дольше стандартного времени.

- Данные обо всех обрабатываемых объектах и действиях: заключение ПО по обрабатываемому объекту; код каталога файлов; размер обрабатываемого объекта; контрольная сумма (SHA256) обрабатываемого объекта; номер обнаруженного ПО в контексте компонента мониторинг активности; дата и время обнаружения стороннего ПО компонентом мониторинг активности; характеристики обнаружения; идентификатор

сработавшей записи в антивирусных базах ПО; причина обнаружения стороннего ПО компонентом мониторинг активности; контрольная сумма (MD5) обрабатываемого объекта; результат проверки подписи модуля, целостность которого проверяется ПО; имя обрабатываемого объекта; тип сработавшей записи в антивирусных базах ПО; путь к обрабатываемому объекту; имя проверяемого объекта; дата и время проверки; URL-адрес и Referrer, по которому он был загружен; размер проверяемых файлов и пути к ним; признак нахождения в архиве; дата и время создания файла; имя, размер и контрольные суммы (MD5, SHA2-256) упаковщика (если файл был упакован); энтропия файла; тип файла; код типа файла; признак исполняемого файла, идентификатор исполняемого файла и формат исполняемого файла; контрольная сумма объекта (MD5, SHA2-256); тип и значение дополнительной контрольной суммы объекта; данные о ЭЦП (сертификате) объекта: данные об издателе сертификата, количество запусков объекта с момента последней отправки статистики, идентификатор задачи проверки, способ получения информации о репутации объекта, значение фильтра target, технические характеристики по применяемым технологиям обнаружения; путь к обрабатываемому объекту; код каталога файлов.

- Для исполняемых файлов: энтропия разделов файла, признак проверки репутации или подписи файла, название, тип, идентификатор типа, контрольная сумма (MD5) и размер приложения, загруженного проверяемым объектом, путь к приложению и пути к шаблонам, признак нахождения в списке автозапуска, дата записи, список атрибутов, название упаковщика, информация о цифровой подписи приложения: издатель сертификата, название отправляемого файла в формате MIME, дата и время сборки файла.

- Информация о запускаемых программах и их модулях: контрольные суммы запускаемых файлов (MD5, SHA2-256), размер, атрибуты, дата создания, имя упаковщика (если файл был упакован), имена файлов, данные о запущенных в системе процессах (идентификатор процесса в системе (PID), имя процесса, данные об учетной записи, от которой запущен процесс, приложении и команде, запустившей процесс, полный путь к файлам процесса и командная строка запуска, описание приложения, к которому относится процесс (название приложения и данные об издателе), а также данные об используемых цифровых сертификатах и информация, необходимая для проверки подлинности этих сертификатов, или данные об отсутствии цифровой подписи файла), также информация о загружаемых в процессы модулях: их имена, размер, типы, даты создания, атрибуты, контрольные суммы (MD5, SHA2-256, SHA1), пути к ним, информация заголовка PE-файлов, имена упаковщиков (если файл был упакован), информация о наличии и валидности данных этой статистики, идентификатор условия формирования передаваемой статистики.

- В случае обнаружения угрозы или уязвимости, дополнительно к информации об обнаруженном объекте предоставляется информация об идентификаторе, версии и типе записи в антивирусных базах, название угрозы согласно классификации Правообладателя, дата и время последнего обновления антивирусных баз, имя исполняемого файла, контрольная сумма (MD5) файла приложения, запросившего URL-адрес, в котором произошло обнаружение, IP-адрес (IPv4 или IPv6) обнаруженной угрозы, идентификатор уязвимости и класс ее опасности, URL-адрес и Referrer страницы обнаружения уязвимости.

- В случае обнаружения потенциально вредоносного объекта предоставляется информация о данных в памяти процессов.

- Информация о сетевой атаке: IP-адрес атакующего компьютера и номер порта компьютера пользователя, на который была направлена сетевая атака, идентификатор протокола, по которому выполнялась атака, название и тип атаки.

- Информация о сетевых соединениях: версия и контрольные суммы (MD5, SHA2-256, SHA1) файла процесса, открывшего порт, путь к файлу процесса и его цифровая подпись, локальный и удаленный IP-адреса, номера локального и удаленного портов соединения, состояние соединения, время открытия порта.

- URL и IP-адрес веб-страницы, на которой был обнаружен вредоносный или подозрительный контент, имя, размер и контрольная сумма файла, запросившего данный URL, идентификатор, вес и степень применимости правила, по которому был вынесен вердикт, цель атаки.

- Информация об обновлении установленной программы и антивирусных баз: статус завершения задачи обновления, тип ошибки, которая могла произойти при обновлении, число неуспешных завершений обновления, идентификатор компонента программы, который выполняет обновление.

- Информация об использовании Kaspersky Security Network (далее "KSN"): идентификатор KSN, идентификатор ПО, полная версия ПО, обезличенный IP-адрес устройства пользователя, показатели качества выполнения запросов к KSN, показатели качества обработки пакетов для KSN, показатели количества запросов в KSN и информация о типах запросов в KSN, дата и время начала передачи статистики, дата и время окончания передачи статистики, информация об обновлениях конфигурации KSN: идентификатор активной конфигурации, идентификатор полученной конфигурации, код ошибки при обновлении конфигурации.

- Информация о событиях в системных журналах: время события, название журнала, в котором обнаружено событие, тип и категория события, название источника события и его описание.

- Информация для определения репутации файлов, URL-адресов и сертификатов: URL-адрес, для которого запрашивается репутация и Referrer, тип протокола соединения, внутренний идентификатор типа программы, номер используемого порта, идентификатор пользователя, контрольная сумма проверяемого файла (MD5), тип обнаруженной угрозы, информация о записи, которая была использована для обнаружения угрозы (идентификатор записи в антивирусной базе, время создания и тип записи); публичный ключ сертификата; отпечаток цифрового сертификата проверяемого объекта и алгоритм хеширования.

- Данные о территориальной распространенности программы: дата установки и дата активации программы, идентификатор партнера, предоставившего лицензию для

активации программы, идентификатор программы, идентификатор языковой локализации программы, серийный номер лицензии, по которой программа активирована, признак участия в KSN.

- Информация об используемой лицензии: тип лицензии и срок ее действия, количество дней до истечения срока действия лицензии, идентификатор партнера, у которого приобретена лицензия, идентификатор регионального центра активации, контрольная сумма кода активации, хеш-сумма тела тикета, рассчитанная по алгоритму SHA1, дата и время создания лицензионного тикета, идентификатор информации о лицензии, идентификатор лицензионного тикета, идентификатор последовательности лицензионного тикета, уникальный идентификатор компьютера пользователя, дата начала и окончания периода валидности лицензионного тикета, текущее состояние лицензионного тикета, версия заголовка тикета, версия лицензии, идентификатор сертификата подписи заголовка тикета, контрольная сумма файла ключа, серийный номер подписчика заголовка тикета, токен авторизации.

- Информация об установленном на компьютере аппаратном обеспечении: тип, название, модель, версия прошивки, характеристики встроенных и подключенных устройств.

- Информация об устройстве: идентификатор устройства.

- Информация о работе компонента "Веб-Контроль": версия компонента, причина категоризации, дополнительная информация о причине категоризации, категоризированный URL-адрес, IP-адрес хоста заблокированного/категоризированного объекта.

Также для достижения поставленных целей повышения эффективности обеспечиваемой ПО защиты "Лаборатория Касперского" может получать объекты, которые могут использоваться злоумышленниками для нанесения вреда компьютеру или создавать угрозу информационной безопасности. К таким объектам относятся:

- исполняемые и неисполняемые файлы целиком или частично;

- участки оперативной памяти компьютера;

- секторы, участвующие в процессе загрузки операционной системы;

- пакеты данных сетевого трафика;

- веб-страницы и электронные письма, содержащие подозрительные и вредоносные объекты;

- описание классов и экземпляров классов WMI хранилища;

- отчеты об активности приложений.

Такие отчеты об активности приложений содержат следующие данные о файлах и процессах:

- имя, размер и версия отправляемого файла, его описание и контрольные суммы (MD5, SHA2-256, SHA1), идентификатор формата, название его производителя, название приложения, к которому относится файл, полный путь к файлу на компьютере и код шаблона пути, дата и время создания и модификации файла;
- дата и время начала и окончания срока действия сертификата, если отправляемый файл имеет цифровую подпись, дата и время подписания, имя издателя сертификата, информация о владельце сертификата, отпечаток и открытый ключ сертификата и алгоритмы их вычисления, серийный номер сертификата;
- имя учетной записи, от которой запущен процесс;
- контрольные суммы (MD5, SHA2-256, SHA1) имени компьютера, на котором запущен процесс;
- заголовки окон процесса;
- идентификатор антивирусных баз, название обнаруженной угрозы согласно классификации "Лаборатории Касперского";
- информация о лицензии приложения, идентификатор лицензии, ее тип и дата истечения срока действия;
- локальное время компьютера в момент предоставления информации;
- имена и пути к файлам, к которым получал доступ процесс;
- URL- и IP-адреса, к которым обращался процесс;
- URL- и IP-адреса, с которых был получен загруженный файл.

Также для достижения заявленной цели в части предотвращения ложных срабатываний "Лаборатория Касперского" может получать доверенные исполняемые и неисполняемые файлы или их части.

Ознакомление с Положением о Kaspersky Security Network

1. В строке меню нажмите на значок приложения и выберите пункт **Настройки**.

   Откроется окно настройки приложения.

2. На закладке **Дополнительно** нажмите на кнопку **Показать Положение о KSN**.

Kaspersky Endpoint Security сохраняет в Файле трассировки следующую информацию:

- информацию об устройстве и об установленной на нем операционной системе (уникальный идентификатор устройства, тип устройства, MAC-адреса сетевых устройств, тип операционной системы, версию операционной системы);

- информацию о работе приложения и его модулей;

- информацию о подписке (тип подписки, регион);

- информацию о языке интерфейса, идентификатор приложения, кастомизацию приложения, версию приложения, уникальный идентификатор установки приложения, уникальный идентификатор компьютера;

- информацию о состоянии защиты компьютера от вредоносного ПО, а также данные обо всех обработанных и обнаруженных объектах (название детектируемого объекта, дата и время обнаружения, веб-адрес, по которому он был загружен, названия и размер зараженных файлов и пути к ним, IP-адрес атакующего компьютера и номер порта компьютера Пользователя, на который была направлена сетевая атака, перечень активностей вредоносной программы, нежелательные веб-адреса) и соответствующих действиях и решениях ПО и пользователя по ним;

- информацию о загруженных пользователем программах (веб-адреса, атрибуты, размер файлов, сведения о процессе, который загрузил файл);

- информацию о запускаемых программах и их модулях (размер, атрибуты, дата создания, информация заголовка PE, регион, имя, расположение, упаковщики);

- информацию об ошибках и использовании пользовательского интерфейса установленного ПО "Лаборатории Касперского";

- информацию о сетевых соединениях: IP-адрес удаленного компьютера и компьютера Пользователя, номера портов, через которые устанавливалось соединение, сетевой протокол соединения;

- информацию о сетевых пакетах, получаемых и передаваемых компьютером по информационно-телекоммуникационным сетям;

- информацию об отправляемых и принимаемых сообщениях электронной почты и мгновенных сообщениях;

- информацию о посещаемых веб-адресах: данные о логине и пароле для сайта и содержимое файлов cookie (если соединение устанавливалось по открытому протоколу);

- публичный сертификат сервера.

Файлы трассировки содержат только данные, необходимые для устранения неполадок в работе приложения. "Лаборатория Касперского" использует файлы трассировки в целях расследования инцидентов, связанных с ошибками в работе приложения Kaspersky Endpoint Security.

По умолчанию создание файлов трассировки выключено. Вы можете включить создание файлов трассировки в настройках приложения.

Файлы трассировки можно отправить в "Лабораторию Касперского" только вручную. Приложение не отправляет автоматически файлы трассировки в "Лабораторию Касперского".

Вы можете выбрать способ отправки файлов трассировки в "Лабораторию Касперского".

Перед отправкой файлов трассировки в "Лабораторию Касперского" ознакомьтесь с данными, которые в них содержатся.

Важно! Файлы трассировки могут содержать конфиденциальные данные. Отправляя файлы трассировки в "Лабораторию Касперского", вы соглашаетесь с передачей данных, которые в них содержатся, а также выражаете согласие со способом их передачи.

Также для дополнительной проверки в "Лабораторию Касперского" могут отправляться файлы, которые могут использоваться злоумышленником с целью причинения вреда компьютеру или данным пользователя, либо их части.

Полученная информация защищается "Лабораторией Касперского" в соответствии с установленными законом требованиями и действующими правилами "Лаборатории Касперского". Данные передаются по защищенному каналу.

Участие в Kaspersky Security Network является добровольным. Решение об участии вы принимаете на этапе установки приложения. Вы можете изменить свое решение в любой момент.

Активация Kaspersky Endpoint Security

Важно! Прежде чем активировать Kaspersky Endpoint Security, убедитесь, что системные дата и время компьютера соответствует фактическим.

Активация приложения заключается в добавлении ключа в приложение. Компонент Managed Detection and Response активируется отдельно. Чтобы использовать этот компонент, вам необходимо активировать Kaspersky Managed Detection and Response в Консоли администрирования Kaspersky Security Center или в Kaspersky Security Center Web Console.

Если компонент Endpoint Detection and Response не поддерживается вашей текущей лицензией, вам необходимо активировать Kaspersky Endpoint Detection and Response отдельно.

Примечание. Для активации приложения требуется подключение к интернету.

Активация пробной версии приложения

1. Откройте главное окно приложения.
2. На боковой панели главного окна приложения нажмите **Лицензия**.

   Откроется окно **Лицензия**.
3. В окне **Лицензия** нажмите на кнопку **Активировать**.

   Kaspersky Endpoint Security соединится с серверами активации "Лаборатории Касперского" и отправит данные для проверки. В случае успешной проверки приложение получает и добавляет ключ для бесплатной пробной версии.

   Важно! Вы можете активировать пробную версию Kaspersky Endpoint Security только в том случае, если приложение не было ранее активировано на вашем компьютере.

Активация приложения с помощью кода активации

1. Откройте главное окно приложения.
2. На боковой панели главного окна приложения нажмите **Лицензия**.

   Откроется окно **Лицензия**.
3. В окне **Лицензия** введите код активации, полученный при покупке Kaspersky Endpoint Security.
4. Нажмите на кнопку **Активировать**.

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

Приложение соединится с серверами активации "Лаборатории Касперского" и отправит код активации для проверки подлинности. В случае успешного завершения проверки кода активации приложение автоматически получит и добавит лицензионный ключ.

Примечание. В зависимости от кода активации, возможно, вам потребуется заполнить регистрационную форму.

Если код активации не пройдет проверку, появится соответствующее уведомление. В этом случае обратитесь за информацией в компанию, которая предоставила вам этот код активации.

После активации приложения с помощью кода активации в окне **Лицензия** будет отображаться следующая информация:

- статус лицензии или подписки;
- активные ключи;
- резервные ключи (если они были добавлены);
- тип лицензии и количество компьютеров, на которых вы можете использовать приложение по действующей лицензии или подписке;
- функции приложения, доступные по текущей лицензии или подписке;
- дата и время окончания срока действия лицензии;
- количество дней до завершения срока действия лицензии.

Просмотр информации о лицензии

Просмотр информации о лицензии

1. Откройте главное окно приложения.

2. На боковой панели главного окна приложения нажмите **Лицензия**.

Откроется окно **Лицензия**.

В окне **Лицензия** может отображаться следующая информация:

- статус лицензии или подписки;
- активные ключи;
- резервные ключи (если они были добавлены);
- тип лицензии и количество компьютеров, на которых вы можете использовать приложение по действующей лицензии или подписке;
- функции приложения, доступные по текущей лицензии или подписке;
- дата и время окончания срока действия лицензии;
- количество дней до завершения срока действия лицензии.

Управление лицензиями и подписками

Вам нужно продлить лицензию, если истек срок действия лицензии, связанной с активным ключом, а резервный ключ не был добавлен. Когда срок действия лицензии истекает, приложение продолжает работать с ограниченной функциональностью (становятся недоступны обновление приложения, использование Kaspersky Security Network, Веб-Контроль и шифрование диска FileVault через Kaspersky Security Center). Вы по-прежнему можете использовать все компоненты приложения и выполнять поиск вредоносного ПО, но только на основе баз приложения, установленных до даты окончания срока действия лицензии.

Важно! При устаревании баз вредоносного ПО риск заражения вашего компьютера возрастает.

Продление срока действия лицензии

1. На боковой панели главного окна приложения нажмите **Центр защиты**.

   Откроется окно **Центр защиты**.

2. В окне **Центр защиты** нажмите на кнопку **Продлить**.

Откроется веб-страница с информацией о продлении лицензии через интернет-магазин "Лаборатории Касперского» или у партнеров компании. Если вы продлеваете срок действия лицензии через интернет-магазин, код активации Kaspersky Endpoint Security будет отправлен на электронный адрес, который вы указали в форме заказа, по факту оплаты.

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

Если вы используете приложение по неограниченной подписке, Kaspersky Endpoint Security продлевает подписку без вашего участия.

Если вы используете приложение по ограниченной подписке и льготный период для продления подписки закончился, Kaspersky Endpoint Security уведомляет вас об этом и прекращает попытки автоматического продления подписки, а также перестает обновлять базы приложения.

Вы можете продлить подписку вручную, связавшись с поставщиком услуг, у которого вы приобрели Kaspersky Endpoint Security.

Продление подписки

1. Откройте главное окно приложения.
2. На боковой панели главного окна приложения нажмите **Лицензия**.

   Откроется окно **Лицензия**.
3. В окне **Лицензия** нажмите на кнопку **Перейти на сайт поставщика услуг**.

Откроется сайт поставщика услуг.

Иногда статус подписки может становиться неактуальным. В этом случае вам нужно обновить его вручную. Если у вас нет действующей подписки, Kaspersky Endpoint Security прекращает обновлять базы приложения (в случае подписки на обновление) или прекращает защищать компьютер (в случае подписки на обновление и защиту).

Обновление статуса подписки

1. Откройте главное окно приложения.
2. На боковой панели главного окна приложения нажмите **Лицензия**.

Откроется окно **Лицензия**.

3. В окне **Лицензия** нажмите на кнопку .

Сравнение функций приложения в зависимости от типа лицензии для рабочих станций

Набор доступных функций Kaspersky Endpoint Security на рабочих станциях зависят от типа лицензии (см. таблицу ниже).

Сравнение функций Kaspersky Endpoint Security

Функция	Kaspersky Endpoint Security для бизнеса Стандартный	Kaspersky Endpoint Security для бизнеса Расширенный	Kaspersky Total Security	Kaspersky Endpoint Detection and Response Optimum	Kaspersky Optimum Security
Продвинутая защита					
Kaspersky Security Network	✓	✓	✓	✓	✓
Анализ поведения	✓	✓	✓	✓	✓
Защита от эксплойтов	✓	✓	✓	✓	✓
Откат вредоносных действий	✓	✓	✓	✓	✓
Базовая защита					
Защита от файловых угроз	✓	✓	✓	✓	✓
Защита от веб-угроз	✓	✓	✓	✓	✓

Защита от почтовых	✓	✓	✓	✓	✓

Решение типовых задач

Запуск и остановка приложения

Развернуть всё | Свернуть всё

Сразу после установки приложение запускается автоматически и в строке меню появляется значок приложения.

Запуск приложения

В строке меню нажмите на значок приложения и выберите в контекстном меню значка приложения пункт **Kaspersky Endpoint Security**.

Завершение работы приложения

В строке меню нажмите на значок приложения и выберите в контекстном меню значка приложения пункт **Выход**.

После завершения работы приложения его процесс удаляется из оперативной памяти компьютера.

Важно! После завершения работы приложения Kaspersky Endpoint Security компьютер продолжает работать в незащищенном режиме, что повышает риск заражения компьютера и потери данных.

Просмотр сведений о состоянии защиты компьютера

На наличие проблем в защите компьютера указывает индикатор состояния защиты компьютера. Это изображение щита в главном окне приложения. В зависимости от состояния защиты компьютера цвет индикатора может меняться. Когда Kaspersky Endpoint Security обнаруживает угрозы безопасности, в главном окне приложения отображается сообщение об этих угрозах, а цвет индикатора меняется.

Цвет индикатора может изменяться следующим образом:

- **Зеленый**. Ваш компьютер защищен.

  Зеленый цвет индикатора означает, что базы вредоносного ПО базы актуальны, все компоненты приложения работают в соответствии с параметрами, рекомендованными специалистами "Лаборатории Касперского", а вредоносные объекты либо не обнаружены, либо обезврежены.

- **Желтый**. Уровень защиты вашего компьютера снижен.

  Желтый цвет индикатора означает, что приложение Kaspersky Endpoint Security зафиксировало проблему. К таким проблемам относятся незначительные отклонения от рекомендуемых параметров защиты или незначительное устаревание баз приложения.

- **Красный**. Ваш компьютер находится под угрозой заражения.

  Красный цвет индикатора означает наличие серьезных проблем, которые могут привести к заражению компьютера и потере данных. Например, красный цвет может указывать на то, что базы вредоносного ПО приложения сильно устарели, приложение не активировано или обнаружены вредоносные объекты.

  Рекомендуется как можно скорее решить проблемы и устранить угрозы безопасности.

Просмотр рабочего состояния установленных компонентов

Kaspersky Endpoint Security позволяет проверять состояние установленных компонентов приложения в окне **Безопасность**. Индикатор рядом с названием каждого компонента отражает его статус.

Просмотр статуса компонента

1. Откройте главное окно приложения.
2. На боковой панели главного окна приложения нажмите на кнопку **Безопасность**.

   Откроется окно **Безопасность**.

Могут отображаться следующие индикаторы состояния:

🟢	Компонент запущен.
🔒	Компонент запущен и управляется политикой безопасности.
🔴	Компонент неисправен.
🔒	Компонент неисправен и управляется политикой безопасности.

	Компонент выключен.
	Компонент выключен и управляется политикой безопасности.
	Компонент приостановлен.
	Компонент не поддерживается действующей лицензией.

Примечание. Для некоторых компонентов вы также можете воспользоваться меню с тремя точками рядом с названием компонента, чтобы открыть отчет или настроить параметры компонента.

Выключение и возобновление защиты компьютера

По умолчанию Kaspersky Endpoint Security запускается при старте операционной системы и защищает ваш компьютер в течение всего времени работы. Все компоненты защиты (Защита от файловых угроз, Защита от веб-угроз и Защита от сетевых угроз) включены и работают.

Вы можете выключить защиту полностью или выключить некоторые компоненты защиты.

Важно! Специалисты "Лаборатории Касперского" настоятельно рекомендуют не выключать защиту компьютера или компоненты защиты, так как это может привести к заражению компьютера и потере данных.

Если защита компьютера выключена:

- неактивный значок приложения в строке меню;
- индикатор состояния защиты в главном окне приложения красного цвета.

Если выключен один или несколько компонентов защиты, индикатор состояния защиты компьютера красного или желтого цвета.

Примечание. Выключение или приостановка работы компонентов защиты не оказывает влияния на выполнение задач проверки и задачи обновления.

Выключить и снова включить защиту компьютера можно двумя способами:

- в меню значка приложения;

- в окне настройки приложения;
- в меню **Защита**.

Выключение и возобновление защиты компьютера в меню значка приложения

1. В строке меню нажмите на значок приложения и выберите в контекстном меню значка приложения пункт **Выключить защиту**/**Включить защиту**.

   Если вы хотите выключить защиту, появляется окно запроса учетных данных администратора.

2. В окне запроса учетных данных администратора введите имя администратора и пароль и подтвердите, что вы хотите выключить защиту.

Выключение и возобновление защиты компьютера в окне настройки приложения

1. В строке меню нажмите на значок приложения и выберите пункт **Настройки**.

   Откроется окно настройки приложения.

2. На вкладке **Базовая** в блоке **Основное** снимите/установите флажок **Включить защиту**.

Выключение и возобновление защиты компьютера в строке меню

В строке меню выберите **Защита** > **Выключить защиту**/**Включить защиту**.

Важно! Если вы выключили защиту компьютера, то после перезапуска Kaspersky Endpoint Security она не включится автоматически. Вам потребуется включить ее вручную.

Выключение компонента защиты

1. В строке меню нажмите на значок приложения и выберите пункт **Настройки**.

   Откроется окно настройки приложения.

2. На вкладке **Базовая** в блоке **<название компонента>** снимите флажок **Включить <название компонента>**.

Важно! Если вы выключили компонент защиты, то после перезапуска Kaspersky Endpoint Security он не включится автоматически. Вам потребуется включить его вручную.

Включение компонента защиты

1. В строке меню нажмите на значок приложения и выберите пункт **Настройки**.

   Откроется окно настройки приложения.

2. На вкладке **Базовая** в блоке **<название компонента>** установите флажок **Включить <название компонента>**.

Также вы можете включить защиту компьютера или компоненты защиты в Центре защиты. Выключение защиты или компонентов защиты значительно повышает риск заражения компьютера, поэтому информация о выключении защиты отображается в Центре защиты.

Использование Центра защиты

Центр защиты – это функция Kaspersky Endpoint Security, которая позволяет анализировать и устранять имеющиеся проблемы и угрозы компьютерной безопасности.

Как открыть Центр защиты

На боковой панели главного окна приложения нажмите **Центр защиты**.

В Центре защиты вы можете найти информацию об активных угрозах, просмотреть состояние баз приложения, а также получить информацию о состоянии компонентов защиты.

Примечание. Когда системный администратор вашей организации включает Веб-Контроль, чтобы блокировать доступ к опасным веб-ресурсам, Kaspersky Endpoint Security отображает в Центре защиты сообщение **Веб-Контроль включен**.

Для каждой проблемы или угрозы указаны действия, которые вы можете предпринять, чтобы решить проблему или устранить угрозу. Например, если приложение Kaspersky Endpoint Security обнаружило на компьютере зараженные файлы, вы можете нажать **Лечить**. Если базы вредоносного ПО устарели, вы можете нажать на кнопку **Обновить**. Вы можете решить проблему или устранить угрозу сразу или позднее.

Немедленное устранение проблемы или угрозы

Нажмите на кнопку с рекомендуемым действием для устранения проблемы или угрозы.

Приложение выполнит выбранное действие.

Если вы закроете Центр защиты, не устранив серьезные угрозы, индикатор состояния защиты компьютера в главном окне приложения останется красным и будет напоминать вам о нерешенных проблемах.

Запуск задач проверки

В Kaspersky Endpoint Security доступна стандартная задача полной проверки. В рамках этой задачи приложение проверяет память, объекты автозапуска и все внутренние диски компьютера на наличие вирусов и других вредоносных программ.

Запуск полной проверки компьютера

1. На боковой панели главного окна приложения нажмите **Проверка**.

   Откроется окно **Проверка**.

2. Нажмите на кнопку **Полная проверка**.

Полная проверка компьютера запустится.

В Kaspersky Endpoint Security доступна стандартная задача быстрой проверки. В рамках этой задачи приложение проверяет критически важные области компьютера (память, объекты автозапуска и системные папки) на наличие вирусов и других вредоносных программ.

Запуск быстрой проверки компьютера

1. На боковой панели главного окна приложения нажмите **Проверка**.

   Откроется окно **Проверка**.

2. Нажмите на кнопку **Быстрая проверка**.

Быстрая проверка компьютера запустится.

Если вы хотите проверить на вирусы и другие вредоносные программы отдельный объект (один из внутренних дисков, отдельную папку, файл или съемный диск), то можете запустить задачу выборочной проверки.

Проверка отдельного объекта

Выполните одно из следующих действий:

- По правой клавише мыши откройте контекстное меню объекта и выберите пункт **Проверить на вредоносные программы**.
- Перетащите выбранный объект на значок приложения в панели Dock.
- Перетащите выбранный объект в окно **Проверка**.

С результатами выполнения задач проверки вы можете ознакомиться в окне **Отчеты**.

Примечание. Kaspersky Endpoint Security не проверяет файлы, расположенные в хранилищах OneDrive, iCloud и других облачных хранилищах. Исключите эти файлы из области проверки. В противном случае задача проверки может завершиться с ошибкой *Зараженный файл не удален*.

Настройка автоматического запуска проверки компьютера по расписанию

Вы можете сформировать расписание запуска задач быстрой проверки и полной проверки. Kaspersky Endpoint Security выполняет автоматическую проверку всего компьютера или выбранных областей в соответствии с указанным расписанием.

Настройка расписания запуска задачи проверки из окна Проверка

1. На боковой панели главного окна приложения нажмите **Проверка**.

   Откроется окно **Проверка**.

2. Нажмите на кнопку **Расписание проверки**.

   Откроется окно, в котором вы можете настроить параметры расписания.

3. Установите флажок **Полная проверка** или **Быстрая проверка**.

4. Укажите частоту запуска проверки и время запуска.

5. Нажмите **OK**.

Настройка расписания запуска задачи проверки из окна настройки приложения

1. В строке меню нажмите на значок приложения и выберите пункт **Настройки**.

   Откроется окно настройки приложения.

2. На вкладке **Проверка** нажмите на кнопку **Расписание**.

3. В открывшемся окне установите флажки рядом с названием задач, которые вы хотите запускать по расписанию.

4. Настройте частоту и время запуска задачи проверки.

5. Нажмите на кнопку **OK**, чтобы сохранить изменения в расписании запуска задачи проверки.

С результатами выполнения задач проверки можно ознакомиться в окне **Отчеты**.

Обновление баз приложения

Основным источником обновлений Kaspersky Endpoint Security являются специальные серверы обновлений "Лаборатории Касперского". Kaspersky Endpoint Security также может использовать в качестве *источника обновлений* точки распространения, локальные папки или другие веб-серверы.

Примечание. Для успешной загрузки обновлений с серверов обновлений требуется подключение к интернету.

По умолчанию Kaspersky Endpoint Security периодически проверяет наличие обновлений на серверах обновлений "Лаборатории Касперского". Если обновления доступны на сервере, Kaspersky Endpoint Security загружает их в фоновом режиме и устанавливает на компьютер.

Запуск обновления Kaspersky Endpoint Security

1. На боковой панели главного окна приложения, нажмите **Обновление**.

   Откроется окно **Обновление**.

2. Нажмите на кнопку **Обновить**.

Приложение проверит наличие обновлений. Если обновления доступны, приложение загрузит и установит их на ваш компьютер.

Также вы можете запустить задачу обновления одним из следующих способов:

- Нажмите на значок приложения и выберите **Обновление**.
- В строке меню выберите **Защита** > **Обновление**.

Вы можете изменить режим обновления баз Kaspersky Endpoint Security. По умолчанию базы приложения обновляются автоматически.

Включение и выключение автоматической загрузки обновлений баз Kaspersky Endpoint Security

1. В строке меню нажмите на значок приложения и выберите пункт **Настройки**.

   Откроется окно настройки приложения.

2. На вкладке **Обновление** в блоке **Базы** установите/снимите флажок **Загружать обновления автоматически**.

С результатами выполнения задач обновления вы можете ознакомиться в окне **Отчеты**.

Примечание. Функциональность обновлений (включая обновления сигнатур вредоносного ПО и обновления кодовой базы), а также функциональность KSN могут быть недоступны в ПО на территории США.

Что делать, если доступ к файлу заблокирован

Приложение Kaspersky Endpoint Security блокирует доступ к зараженным файлам или программам. Чтобы получить доступ к зараженному файлу, его необходимо вылечить.

Лечение обнаруженного объекта

1. В строке меню выберите **Защита** > **Обнаруженные объекты**.

   Откроется окно **Обнаруженные объекты**.

2. В блоке **Обнаруженные объекты** нажмите на кнопку ••• рядом с файлом, который вы хотите вылечить и выберите **Лечить**.

   Приложение начнет лечение выбранного объекта. Во время лечения объекта приложение отображает окно уведомления, в котором вы можете выбрать действие над объектом.

Лечение всех обнаруженных объектов

1. В строке меню выберите **Защита** > **Обнаруженные объекты**.

   Откроется окно **Обнаруженные объекты**.

2. В блоке **Обнаруженные объекты** нажмите на кнопку **Лечить все**.

   Приложение начнет лечение обнаруженных объектов. Во время лечения объекта приложение отображает окно уведомления, в котором вы можете выбрать действие над объектом. Если при выборе действия вы установите в окне уведомления флажок **Применить во всех подобных случаях**, приложение применит выбранное действие ко всем файлам этого типа.

Если вы уверены в безопасности файлов, доступ к которым блокирует Защита от файловых угроз, то можете включить их в Доверенную зону.

Восстановление удаленного или вылеченного приложением файла

Иногда в процессе лечения зараженных файлов не удается сохранить их целостность. Если вылеченный файл содержал важную информацию, которая в результате лечения стала полностью или частично недоступной, можно попытаться восстановить исходный файл из его резервной копии.

Восстановление удаленного или измененного при лечении файла

1. В строке меню выберите **Защита** > **Обнаруженные объекты**.

   Откроется окно **Обнаруженные объекты**.

2. В блоке **Резервное хранилище** нажмите на кнопку ••• рядом с файлом, который вы хотите восстановить.

   Откроется всплывающее меню.

3. Выберите **Восстановить файл**.

   Откроется окно, в котором вам нужно указать имя файла, тег и папку, в которую он будет восстановлен. По умолчанию уже указаны исходное имя файла и исходное местоположение.

4. Укажите имя файла и папку, в которую нужно его восстановить.

5. Нажмите на кнопку **Сохранить**.

Приложение восстановит файл в указанное местоположение с указанным именем.

Сразу после восстановления вам нужно проверить файл на вредоносное ПО. Возможно, с обновленными антивирусными базами его удастся вылечить без потери целостности.

Важно! Не рекомендуется восстанавливать резервные копии файлов без крайней необходимости, так как это может привести к заражению вашего компьютера.

Просмотр отчета о работе приложения

Вы можете просмотреть отчет Kaspersky Endpoint Security со списком всех обнаруженных объектов на вкладке **Обработанные объекты**. Системные события отображаются на вкладке **Системные события**. Дополнительно, подробный отчет формируется для каждого компонента приложения: Защиты от файловых угроз, Защиты от веб-угроз, Защиты от сетевых угроз, Анализа поведения, задач проверки и обновления.

Открытие окна Отчеты

В строке меню выберите **Защита** > **Отчеты**.

Что делать при появлении окон уведомлений

Уведомления отображаются в окнах уведомлений и информируют вас о событиях в работе приложения, требующих вашего внимания.

При появлении на экране уведомления выберите один из предложенных вариантов действия. Оптимальным вариантом является действие, настроенное в качестве действия по умолчанию специалистами "Лаборатории Касперского".

Расширенная настройка приложения

Область защиты компьютера

Объекты, обнаруживаемые Kaspersky Endpoint Security, подразделяются на категории по различным признакам. Приложение всегда ищет вирусы, черви, троянские программы и вредоносные утилиты. Эти программы могут нанести значительный вред вашему компьютеру. Для повышения безопасности компьютера вы можете расширить список обнаруживаемых объектов, включив контроль за действиями легальных программ, которые могут быть использованы злоумышленником для нанесения вреда вашему компьютеру или данным.

Объекты, защиту от которых обеспечивает Kaspersky Endpoint Security, подразделяются на следующие категории:

- **Вирусы, черви, троянские программы, вредоносные утилиты, рекламные программы и программы автодозвона**.

  Эта категория включает в себя:

  - Все типы вредоносных программ.
  - Программы, которые могут доставить вам неудобство, поскольку отображают рекламные материалы (например, баннеры) на вашем компьютере или заменяют результаты поиска в вашем браузере на рекламные сайты.
  - Программы, которые незаметно устанавливают телефонные соединения через компьютерный модем.

  Защита от них является минимальным необходимым уровнем безопасности. В соответствии с рекомендациями специалистов "Лаборатории Касперского" Kaspersky Endpoint Security всегда контролирует объекты в этой категории.

- **Легальные программы, которые могут быть использованы злоумышленником для нанесения вреда вашему компьютеру или данным**. Эта категория включает в себя легальные программы, которые могут быть использованы злоумышленником для нанесения вреда вашему компьютеру или персональным данным, такие как программы удаленного администрирования.

Выбор категорий обнаруживаемых объектов

1. В строке меню нажмите на значок приложения и выберите пункт **Настройки**.

   Откроется окно настройки приложения.

2. На вкладке **Угрозы** в блоке **Обнаруживаемые объекты** установите флажки рядом с категориями объектов, которые приложение должно обнаруживать.

   Примечание. Kaspersky Endpoint Security всегда защищает ваш компьютер от вирусов, червей, троянских программ, вредоносных утилит, рекламных программ и программ автодозвона. Поэтому снять флажок рядом с этой категорией невозможно.

В зависимости от выбранных категорий обнаруживаемых объектов Kaspersky Endpoint Security полностью или частично использует базы приложения для Защиты от файловых угроз, Защиты от веб-угроз и при выполнении задач проверки.

Примечание. Если Kaspersky Endpoint Security относит программу, которая, по вашему мнению, не является опасной, к вредоносным программам, вы можете добавить ее в Доверенную зону.

Доверенная зона – это перечень объектов, которые Kaspersky Endpoint Security не проверяет и не контролирует. Например, включение объектов в Доверенную зону может потребоваться, если Kaspersky Endpoint Security блокирует доступ к какому-либо файлу, программе или сайту, а вы абсолютно уверены, что эти файл, программа или веб-адрес безвредны.

Файловая и сетевая активность программы (в том числе подозрительная), добавленной в Доверенную зону, не контролируется. При этом Kaspersky Endpoint Security по-прежнему проверяет исполняемый файл и процесс доверенной программы.

Примечание. Когда в настройках политики администратор запрещает редактирование Доверенной зоны, пользователи не могут перейти к настройкам Доверенной зоны.

Добавление файла или папки в список доверенных файлов и папок и удаление из него

1. В строке меню нажмите на значок приложения и выберите пункт **Настройки**.

   Откроется окно настройки приложения.

2. На вкладке **Угрозы** в блоке **Исключения** нажмите на кнопку **Доверенная зона**.

   Откроется окно настройки Доверенной зоны.

3. На вкладке **Файлы и папки** измените список доверенных файлов и папок:

   - Чтобы добавить файл или папку в список:

     a. Нажмите на кнопку **+**.

        Откроется окно, в котором вы можете выбрать файл или папку.

     b. Выберите файл или папку, которую вы хотите добавить.

     c. Нажмите на кнопку **Открыть**.

   - Чтобы удалить файл или папку из списка:

     a. Выберите файл или папку, которую вы хотите удалить из списка доверенных файлов и папок.

     b. Нажмите на кнопку **—**.

4. Нажмите **ОК**.

Добавление веб-адреса в список доверенных веб-адресов и удаление из него

1. В строке меню нажмите на значок приложения и выберите пункт **Настройки**.

   Откроется окно настройки приложения.

2. На вкладке **Угрозы** в блоке **Исключения** нажмите на кнопку **Доверенная зона**.

   Откроется окно настройки Доверенной зоны.

   Вы также можете открыть это окно, нажав на кнопку **Доверенная зона** в разделе **Основное** на вкладке **Базовая**.

3. На вкладке **Веб-адрес** измените список доверенных веб-адресов:

- Чтобы добавить веб-адрес в список:

  a. Нажмите на кнопку +.

  b. Введите веб-адрес, который вы хотите добавить в список.

  c. Нажмите **OK**.

- Чтобы удалить веб-адрес из списка:

  a. Выберите веб-адрес, который вы хотите удалить.

  b. Нажмите на кнопку −.

4. Нажмите **OK**.

По умолчанию список доверенных веб-адресов пуст.

Добавление приложения в список доверенных приложений и удаление из него

1. В строке меню нажмите на значок приложения и выберите пункт **Настройки**.

   Откроется окно настройки приложения.

2. На вкладке **Угрозы** в блоке **Исключения** нажмите на кнопку **Доверенная зона**.

   Откроется окно настройки Доверенной зоны.

   Вы также можете открыть это окно, нажав на кнопку **Доверенная зона** в разделе **Основное** на вкладке **Базовая**.

3. На закладке **Доверенные программы** отредактируйте список доверенных приложений:

   - Чтобы добавить приложение в список:

     a. Нажмите на кнопку +.

     Откроется окно, в котором вы можете указать параметры требуемого приложения.

     b. Укажите следующие параметры приложения, которое вы хотите добавить:

     - **Путь**
     - **Требование к подписи кода**

Примечание. Вы можете ввести значения этих двух параметров вручную или нажать на кнопку **Выбрать** для выбора приложения, которое вы хотите добавить, в открывшемся окне. В этом случае значения этих параметров будут выставлены автоматически.

c. В разделе **Опции** выберите хотя бы один тип активности, который вы хотите, чтобы приложение Kaspersky Endpoint Security не контролировало:

- **Не контролировать активность файлов**
- **Не контролировать сетевую активность**

d. Нажмите **ОК**.

- Чтобы удалить приложение из списка:

a. Выберите приложение, которое хотите удалить.

b. Нажмите на кнопку —.

По умолчанию список доверенных приложений пуст.

Редактирование доверенного приложения

1. В строке меню нажмите на значок приложения и выберите пункт **Настройки**.

   Откроется окно настройки приложения.

2. На вкладке **Угрозы** в блоке **Исключения** нажмите на кнопку **Доверенная зона**.

   Откроется окно настройки Доверенной зоны.

   Вы также можете открыть это окно, нажав на кнопку **Доверенная зона** в разделе **Основное** на вкладке **Базовая**.

3. На вкладке **Доверенные приложения** выберите приложение, которое вы хотите отредактировать.

4. Нажмите на кнопку **Изменить**.

5. В открывшемся окне отредактируйте параметры приложения.

6. Нажмите **ОК**.

Включение контроля доверенных веб-адресов

1. В строке меню нажмите на значок приложения и выберите пункт **Настройки**.

   Откроется окно настройки приложения.

2. На вкладке **Угрозы** в блоке **Исключения** нажмите на кнопку **Доверенная зона**.

   Откроется окно настройки Доверенной зоны.

3. На вкладке **Веб-адрес** снимите флажок рядом с веб-адресом, который приложение Kaspersky Endpoint Security должно контролировать.

4. Нажмите **ОК**.

Защита от файловых угроз

Защита от файловых угроз предотвращает заражение файловой системы компьютера. Компонент запускается при загрузке операционной системы, постоянно находится в оперативной памяти компьютера и проверяет файлы при открытии, сохранении и запуске на вашем компьютере и на всех подключенных дисках на наличие вредоносных программ. Если выключить Защиту от файловых угроз, компонент не будет запускаться при старте операционной системы. Вам потребуется включить Защиту от файловых угроз вручную.

Включение и выключение Защиты от файловых угроз

1. В строке меню нажмите на значок приложения и выберите пункт **Настройки**.

   Откроется окно настройки приложения.

2. На вкладке **Базовая** в блоке **Защита от файловых угроз** установите/снимите флажок **Включить Защиту от файловых угроз**.

   Вы также можете включить Защиту от файловых угроз в Центре защиты. Выключение защиты или компонентов защиты значительно повышает риск заражения компьютера, поэтому информация о выключении защиты отображается в Центре защиты.

Вы можете сформировать область защиты, включив в нее объекты, которые будет проверять Защита от файловых угроз.

Добавление файла или папки в область защиты и удаление из нее

1. В строке меню нажмите на значок приложения и выберите пункт **Настройки**.

   Откроется окно настройки приложения.

2. На вкладке **Базовая** в блоке **Защита от файловых угроз** нажмите на кнопку **Область защиты**.

   Откроется окно со списком объектов, которые проверяет Защита от файловых угроз. По умолчанию Защита от файловых угроз проверяет все объекты, расположенные на внутренних, съемных и сетевых дисках, подключенных к компьютеру.

   > **Примечание.** Чтобы значительно уменьшить время выполнения проверки, вы можете пропустить проверку системного тома "только для чтения". По умолчанию Защита от файловых угроз не проверяет системный том "только для чтения".

3. В блоке **Область защиты** добавьте объекты в область защиты или удалите их из нее:

   - Чтобы добавить файл или папку в область защиты:

     a. Нажмите на кнопку +.

        Откроется всплывающее меню, в котором вы можете выбрать объекты для добавления в область защиты.

     b. Во всплывающем меню выберите элемент **Файлы и папки**.

        Откроется окно, в котором вы можете выбрать файл или папку.

     c. Выберите файл или папку, которую вы хотите добавить в область защиты.

     d. Нажмите на кнопку **Открыть**.

   - Чтобы удалить файл или папку из области защиты:

     a. Выберите объект в списке объектов в области защиты.

     b. Перетащите выбранный объект из окна или нажмите на кнопку —.

4. Если вы хотите, чтобы приложение проверяло системный том "только для чтения", в блоке **Оптимизация** снимите флажок **Пропускать проверку системного тома «только для чтения»**.

Важно! В целях безопасности оптимизация может быть выключена.

5. Нажмите на кнопку **Сохранить**.

Добавление объекта из списка стандартных объектов защиты в область защиты и удаление из нее

1. В строке меню нажмите на значок приложения и выберите пункт **Настройки**.

   Откроется окно настройки приложения.

2. На вкладке **Базовая** в блоке **Защита от файловых угроз** нажмите на кнопку **Область защиты**.

   Откроется окно со списком объектов, которые проверяет Защита от файловых угроз. По умолчанию Защита от файловых угроз проверяет все объекты, расположенные на внутренних, съемных и сетевых дисках, подключенных к компьютеру.

   Примечание. Чтобы значительно уменьшить время выполнения проверки, вы можете пропустить проверку системного тома "только для чтения". По умолчанию Защита от файловых угроз не проверяет системный том "только для чтения".

3. В блоке **Область защиты** добавьте объекты из списка стандартных объектов защиты в область защиты или удалите их из нее:

   - Чтобы добавить объект из списка стандартных объектов защиты в область защиты:

     a. Нажмите на кнопку +.

     Откроется всплывающее меню, в котором вы можете выбрать объекты для добавления в область защиты.

     b. Во всплывающем меню выберите объект, который вы хотите добавить в область защиты (например, **Все внутренние диски**).

   - Чтобы удалить объект из списка стандартных объектов защиты из области защиты:

     a. Выберите объект в списке объектов в области защиты.

b. Перетащите выбранный объект из окна или нажмите на кнопку —.

4. Если вы хотите, чтобы приложение проверяло системный том "только для чтения", в блоке **Оптимизация** снимите флажок **Пропускать проверку системного тома «только для чтения»**.

   Важно! В целях безопасности оптимизация может быть выключена.

5. Нажмите на кнопку **Сохранить**.

Выключение защиты объекта в области защиты

1. В строке меню нажмите на значок приложения и выберите пункт **Настройки**.

   Откроется окно настройки приложения.

2. На вкладке **Базовая** в блоке **Защита от файловых угроз** нажмите на кнопку **Область защиты**.

   Откроется окно со списком объектов, которые проверяет Защита от файловых угроз. По умолчанию Защита от файловых угроз проверяет все объекты, расположенные на внутренних, съемных и сетевых дисках, подключенных к компьютеру.

   Примечание. Чтобы значительно уменьшить время выполнения проверки, вы можете пропустить проверку системного тома "только для чтения". По умолчанию Защита от файловых угроз не проверяет системный том "только для чтения".

3. Снимите флажок рядом с объектом в списке объектов, включенных в область защиты.

4. Нажмите на кнопку **Сохранить**.

Включение проверки системного тома "только для чтения"

1. В строке меню нажмите на значок приложения и выберите пункт **Настройки**.

   Откроется окно настройки приложения.

2. На вкладке **Базовая** в блоке **Защита от файловых угроз** нажмите на кнопку **Область защиты**.

   Откроется окно со списком объектов, которые проверяет Защита от файловых угроз. По умолчанию Защита от файловых угроз проверяет все объекты, расположенные на внутренних, съемных и сетевых дисках, подключенных к компьютеру.

   > **Примечание.** Чтобы значительно уменьшить время выполнения проверки, вы можете пропустить проверку системного тома "только для чтения". По умолчанию Защита от файловых угроз не проверяет системный том "только для чтения".

3. В блоке **Оптимизация** снимите флажок **Пропускать проверку системного тома «только для чтения»**.

   > **Важно!** В целях безопасности оптимизация может быть выключена.

4. Нажмите на кнопку **Сохранить**.

Когда вы или приложение пытаетесь получить доступ к файлу, включенному в область защиты, Защита от файловых угроз ищет информацию об этом файле в базах данных iSwift и на основе этой информации принимает решение о необходимости проверки файла.

При распознавании вредоносных объектов Защита от файловых угроз использует *сигнатурный анализ* (режим поиска угроз на основе описаний угроз, включенных в базы приложения), а также эвристический анализ и другие технологии проверки.

При обнаружении угрозы в файле Kaspersky Endpoint Security определяет тип обнаруженной вредоносной программы (например, *вирус* или *троянская программа*). После этого приложение выводит уведомление об обнаруженном объекте и выполняет над объектом действие в соответствии с настройками Защиты от файловых угроз.

Выбор действия, которое Защита от файловых угроз выполняет при обнаружении зараженного файла

1. В строке меню нажмите на значок приложения и выберите пункт **Настройки**.

   Откроется окно настройки приложения.

2. На вкладке **Базовая** в блоке **Защита от файловых угроз** выберите действие, которое будет выполнять компонент при обнаружении зараженного файла.

Перед лечением или удалением зараженного файла Kaspersky Endpoint Security сохраняет его резервную копию на тот случай, если в дальнейшем понадобится восстановить файл или появится возможность его вылечить.

Информация о работе Защиты от файловых угроз и обо всех обнаруженных объектах записывается в отчет.

Примечание. Если компонент Защита от файловых угроз завершает работу с ошибкой, просмотрите отчет и попробуйте его перезапустить. Если вам не удается решить проблему, обратитесь в Службу технической поддержки.

Просмотр отчета о работе компонента Защита от файловых угроз

1. В строке меню выберите **Защита** > **Отчеты**.

   Откроется окно **Отчеты**.

2. Откройте вкладку **Защита от файловых угроз**.

Защита от веб-угроз

Когда вы используете интернет, ваш компьютер подвергается риску заражения вредоносным ПО и другим угрозам компьютерной безопасности. Такие угрозы могут попадать на ваш компьютер при загрузке бесплатных программ или посещении сайтов, которые подверглись хакерским атакам. Кроме того, сетевые черви могут атаковать ваш компьютер, как только вы подключаетесь к интернету, даже до того, как вы откроете сайт или загрузите файл.

Kaspersky Endpoint Security защищает информацию, которую ваш компьютер отправляет и получает по протоколам HTTP и HTTPS через браузеры Safari, Chrome и Firefox.

Примечание. Kaspersky Endpoint Security контролирует веб-трафик на портах, которые наиболее часто используются для передачи данных по протоколам HTTP и HTTPS. Kaspersky Endpoint Security проверяет защищенные соединения (HTTPS), только если установлен флажок **Проверять защищенные соединения (HTTPS)** в блоке **Основное**.

Включение и выключение Защиты от веб-угроз

1. В строке меню нажмите на значок приложения и выберите пункт **Настройки**.

   Откроется окно настройки приложения.

2. На вкладке **Базовая** в блоке **Защита от веб-угроз** установите/снимите флажок **Включить Защиту от веб-угроз**.

Вы также можете включить Защиту от веб-угроз в Центре защиты. Выключение защиты или компонентов защиты значительно повышает риск заражения компьютера, поэтому информация о выключении защиты отображается в Центре защиты.

Важно! Если вы выключили Защиту от веб-угроз, то после перезапуска Kaspersky Endpoint Security или перезагрузки операционной системы она не включится автоматически. Вам потребуется включить ее вручную.

Защита от веб-угроз проверяет веб-трафик с учетом параметров, рекомендуемых "Лабораторией Касперского". При распознавании вредоносных объектов используются сигнатурный анализ, эвристический анализ и данные из Kaspersky Security Network.

Проверка ссылок на сайтах на фишинг и на принадлежность к вредоносным веб-адресам позволяет избежать *фишинг-атак*. *Фишинг-атаки*, как правило, представляют собой сообщения электронной почты, отправленные злоумышленниками от имени финансовых организаций (например, банков) со ссылками на поддельные сайты. В этих сообщениях электронной почты злоумышленники пытаются обманным путем заставить пользователя посетить фишинговый сайт и предоставить конфиденциальные данные (например, номер банковской карты или имя пользователя и пароль от учетной записи интернет-банка). Фишинг-атака может быть замаскирована, например, под сообщение из вашего банка со ссылкой на его официальный сайт, но на самом деле ссылка ведет вас на точную копию официального сайта банка, созданную злоумышленниками.

Защита от веб-угроз отслеживает попытки перейти на фишинговый сайт на уровне проверки веб-трафика и блокирует доступ к таким сайтам. Kaspersky Endpoint Security проверяет ссылки на сайтах на фишинг и на принадлежность к вредоносным веб-адресам, используя базы приложения, эвристический анализ и данные из Kaspersky Security Network.

Алгоритм проверки веб-трафика

Защита от веб-угроз перехватывает каждый сайт или файл, к которому вы или какая-либо программа обращаетесь по протоколу HTTP или HTTPS, и проверяет его на наличие вредоносного кода:

- Если сайт или файл содержит вредоносный код, Kaspersky Endpoint Security блокирует такой файл или сайт и выводит уведомление о том, что запрошенный файл или сайт заражены.

- Если сайт или файл не содержит вредоносного кода, он сразу же становится доступным для пользователя.

Выбор действия, которое Защита от веб-угроз выполняет при обнаружении опасного объекта веб-трафика

1. В строке меню нажмите на значок приложения и выберите пункт **Настройки**.

   Откроется окно настройки приложения.

2. На вкладке **Базовая** в блоке **Защита от веб-угроз** выберите действие, которое будет выполнять компонент при обнаружении опасного объекта веб-трафика.

Информация о работе Защиты от веб-угроз и обо всех обнаруженных опасных объектах веб-трафика записывается в отчет.

Примечание. Если компонент Защита от веб-угроз завершает работу с ошибкой, просмотрите отчет о его работе и попробуйте перезапустить его. Если вам не удается решить проблему, обратитесь в Службу технической поддержки.

Просмотр отчета о работе Защиты от веб-угроз

1. В строке меню выберите **Защита** > **Отчеты**.

   Откроется окно **Отчеты**.

2. Откройте вкладку **Защита от веб-угроз**.

Защита от почтовых угроз

Компонент Защита от почтовых угроз проверяет вложения входящих и исходящих сообщений электронной почты на наличие в них вредоносного ПО и других угроз. Компонент обеспечивает защиту компьютера с помощью баз вредоносного ПО, облачной службы Kaspersky Security Network и эвристического анализа.

Приложение поддерживает следующие почтовые клиенты: Apple Mail, Microsoft Outlook, Mozilla Thunderbird, Canary Mail, Spark, Mimestream, Airmail, Post Box, Boxy Suite 2, Twobird, Shift, Clean Email, eM Client, Superhuman, Polymail, HEY, Mail+ для Gmail, Spike mail.

По умолчанию Защита от почтовых угроз включена. При необходимости вы можете отключить Защиту от почтовых угроз.

Включение/выключение Защиты от почтовых угроз с помощью Web Console

1. В главном окне Web Console выберите **Активы (Устройства)** → **Политики и профили политик**.
2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры программы**.
4. Перейдите в раздел **Базовая защита** > **Защита от почтовых угроз**.
5. Включите/выключите переключатель **Защита от почтовых угроз**.
6. Если Защита от почтовых угроз включена, выберите действие, которое приложение будет выполнять при обнаружении вредоносного ПО:
   - **Удалять**
   - **Блокировать**
7. При необходимости в разделе **Дополнительные параметры** настройте ограничение по времени проверки архивов или максимальный размер архива для проверки.
8. Сохраните внесенные изменения.

Включение/выключение Защиты от почтовых угроз с помощью Консоли администрирования

1. Запустите Консоль администрирования.
2. Разверните узел **Сервер администрирования <Имя сервера>**.
3. В дереве консоли выберите папку **Управляемые устройства**.
4. В рабочей области выберите вкладку **Политики**.

5. По правой клавише мыши откройте контекстное меню политики, параметры которой вы хотите настроить, и выберите **Свойства**.

6. В окне **Свойства** выберите **Базовая защита** > **Защита от почтовых угроз**.

7. Установите или снимите флажок **Включить Защиту от почтовых угроз**.

8. В блоке **Действие при обнаружении угрозы** выберите действие, которое будет выполняться при обнаружении угрозы Kaspersky Endpoint Security.

9. При необходимости в разделе **Параметры Защиты от почтовых угроз** настройте ограничение по времени проверки архивов или максимальный размер архива для проверки.

10. Нажмите **OK**, чтобы сохранить изменения.

11. Чтобы применить изменения к политике, выполните одно из следующих действий:

    - Нажмите на кнопку **Применить**, чтобы остаться в окне **Свойства: <Название политики>** после сохранения внесенных изменений.

    - Нажмите на кнопку **OK**, чтобы закрыть окно **Свойства: <Название политики>** после сохранения внесенных изменений.

Включение/выключение Защиты от почтовых угроз с помощью приложения Kaspersky Endpoint Security

1. В строке меню нажмите на значок приложения и выберите пункт **Настройки**.

   Откроется окно настройки приложения.

2. На вкладке **Базовая** в блоке **Защита от почтовых угроз** установите или снимите флажок **Включить Защиту от почтовых угроз**.

3. Если флажок **Включить Защиту от почтовых угроз** установлен, выберите действие, которое будет выполняться при обнаружении угрозы Kaspersky Endpoint Security.

4. При необходимости настройте ограничение по времени проверки архивов или максимальный размер архива для проверки.

Просмотр отчета о работе Защиты от почтовых угроз

1. В строке меню выберите **Защита** > **Отчеты**.

   Откроется окно **Отчеты**.

2. Откройте вкладку **Защита от почтовых угроз**.

Защита от сетевых угроз

Kaspersky Endpoint Security защищает ваш компьютер от сетевых атак.

Сетевая атака – это вторжение в операционную систему удаленного компьютера. Злоумышленники предпринимают сетевые атаки, чтобы захватить управление над операционной системой, привести ее к отказу в обслуживании или получить доступ к защищенной информации. Для этого злоумышленники выполняют прямые атаки, такие как сканирование портов или подбор паролей, или используют вредоносные программы, установленные на атакуемом компьютере.

Сетевые атаки можно условно разделить на следующие типы:

- *Сканирование портов*. Этот вид сетевых атак обычно является подготовительным этапом более опасной сетевой атаки. Злоумышленник сканирует UDP- и TCP-порты, используемые сетевыми службами на атакуемом компьютере, и определяет степень уязвимости атакуемого компьютера перед более опасными видами сетевых атак. Сканирование портов также позволяет злоумышленнику определить операционную систему на атакуемом компьютере и выбрать подходящие для нее сетевые атаки.

- *DoS-атаки*, или сетевые атаки, вызывающие отказ в обслуживании. Это сетевые атаки, в результате которых атакуемая операционная система становится нестабильной или полностью неработоспособной.

  Основные типы DoS-атак:

  - Отправка специально сформированных сетевых пакетов, не ожидаемых этим компьютером, которые вызывают сбои в работе операционной системы или ее остановку.

  - Отправка на удаленный компьютер большого количества сетевых пакетов за короткий период времени. Все ресурсы атакуемого компьютера используются для обработки сетевых пакетов, отправленных злоумышленником. В результате, компьютер перестает выполнять свои функции.

- *Сетевые атаки-вторжения*. Эти сетевые атаки направлены на перехват операционной системы атакуемого компьютера. Это самый опасный вид сетевых атак, поскольку в случае ее успешного завершения операционная система полностью переходит под контроль злоумышленника.

Этот вид сетевых атак применяется в случаях, когда злоумышленнику нужно получить конфиденциальные данные с удаленного компьютера (например, номера банковских карт или пароли), либо использовать удаленный компьютер в своих целях (например, атаковать с этого компьютера другие компьютеры) без ведома пользователя.

Включение и выключение Защиты от сетевых угроз

1. В строке меню нажмите на значок приложения и выберите пункт **Настройки**.

   Откроется окно настройки приложения.

2. На вкладке **Базовая** в блоке **Защита от сетевых угроз** установите/снимите флажок **Включить Защиту от сетевых угроз**.

Вы также можете включить Защиту от сетевых угроз в Центре защиты. Выключение защиты или компонентов защиты значительно повышает риск заражения компьютера, поэтому информация о выключении защиты отображается в Центре защиты.

Важно! Если вы выключили Защиту от сетевых угроз, то после перезапуска Kaspersky Endpoint Security или перезагрузки операционной системы она не включится автоматически. Вам потребуется включить Защиту от сетевых угроз вручную.

При обнаружении опасной сетевой активности Kaspersky Endpoint Security автоматически добавляет IP-адрес атакующего компьютера в список заблокированных компьютеров, если этот компьютер не добавлен в список доверенных компьютеров.

Изменение списка заблокированных компьютеров

1. В строке меню нажмите на значок приложения и выберите пункт **Настройки**.

   Откроется окно настройки приложения.

2. На вкладке **Базовая** в блоке **Защита от сетевых угроз** установите флажок **Включить Защиту от сетевых угроз**.

3. Нажмите на кнопку **Настройки**.

   Откроется окно со списком доверенных компьютеров и списком заблокированных компьютеров.

4. Откройте вкладку **Заблокированные компьютеры**.

5. Если вы уверены, что заблокированный компьютер не представляет угрозы, выберите его IP-адрес в списке и нажмите на кнопку **Разблокировать**.

   Откроется окно подтверждения.

6. В окне подтверждения выполните одно из следующих действий:

   - Если вы хотите разблокировать компьютер, нажмите на кнопку **Разблокировать**.

     Kaspersky Endpoint Security разблокирует IP-адрес.

   - Если вы хотите, чтобы Kaspersky Endpoint Security больше никогда не блокировал выбранный IP-адрес, нажмите на кнопку **Разблокировать и добавить к исключениям**.

     Kaspersky Endpoint Security разблокирует IP-адрес и добавит его в список доверенных компьютеров.

7. Нажмите на кнопку **Сохранить**.

Вы можете создать и изменить список доверенных компьютеров. Приложение Kaspersky Endpoint Security не блокирует IP-адреса этих компьютеров автоматически при обнаружении исходящей с них опасной сетевой активности.

Изменение списка доверенных компьютеров

1. В строке меню нажмите на значок приложения и выберите пункт **Настройки**.

   Откроется окно настройки приложения.

2. На вкладке **Базовая** в блоке **Защита от сетевых угроз** установите флажок **Включить Защиту от сетевых угроз**.

3. Нажмите на кнопку **Настройки**.

   Откроется окно со списком доверенных компьютеров и списком заблокированных компьютеров.

4. Откройте вкладку **Доверенные компьютеры**.

5. Отредактируйте список доверенных компьютеров:

   - Чтобы добавить IP-адрес в список доверенных компьютеров:

     a. Нажмите на кнопку +.

b. В появившемся поле введите IP-адрес компьютера, в безопасности которого вы уверены.

- Чтобы удалить IP-адрес из списка доверенных компьютеров:

  a. Выберите IP-адрес в списке.

  b. Нажмите на кнопку —.

- Чтобы изменить IP-адрес в списке доверенных компьютеров:

  a. Выберите IP-адрес в списке.

  b. Нажмите на кнопку **Изменить**.

  c. Измените IP-адрес.

6. Нажмите на кнопку **Сохранить**.

При обнаружении сетевой атаки Kaspersky Endpoint Security сохраняет информацию о ней в отчете.

Примечание. Если компонент Защита от сетевых угроз завершил работу с ошибкой, вы можете просмотреть отчет и попробовать перезапустить компонент. Если вам не удается решить проблему, обратитесь в Службу технической поддержки.

Просмотр отчета о работе Защиты от сетевых угроз

1. В строке меню выберите **Защита** > **Отчеты**.

   Откроется окно **Отчеты**.

2. Откройте вкладку **Защита от сетевых угроз**.

Проверка

Компоненты Защита от файловых угроз и Защита от веб-угроз обеспечивают постоянную защиту компьютера. Также мы рекомендуем регулярно проверять компьютер на вредоносные программы и другие угрозы компьютерной безопасности. Проверка компьютера необходима для того, чтобы предотвратить распространение вредоносных программ, которые не были обнаружены компонентами защиты.

Kaspersky Endpoint Security содержит следующие встроенные задачи проверки:

- **Полная проверка**.

  Поиск вредоносного ПО в памяти компьютера, объектах автозапуска и всех внутренних дисках.

- **Быстрая проверка**.

  Поиск вредоносного ПО в важных областях компьютера: памяти, объектах автозапуска и системных папках.

- **Выборочная проверка**.

  Поиск вредоносного ПО в отдельном объекте (файле, папке, внутреннем или съемном диске).

- **Проверка внешних дисков**

  Поиск вредоносного ПО на внешних дисках, который выполняется после подключения внешнего диска к компьютеру.

Когда приложение выполняет задачи проверки, для распознавания вредоносных объектов используется сигнатурный анализ, а также эвристический анализ и другие технологии проверки.

В окне **Проверка** отображается информация о ходе выполнения каждой запущенной задачи сканирования (процент выполнения и оставшееся время), а также история сканирования (100 последних задач проверки).

Запуск задач полной проверки и быстрой проверки

1. На боковой панели главного окна приложения нажмите **Проверка**.

   Откроется окно **Проверка**.

2. В окне **Проверка** нажмите на кнопку **Полная проверка** или **Быстрая проверка**.

Запустится задача проверки.

Запуск задачи выборочной проверки

1. На боковой панели главного окна приложения нажмите **Проверка**.

Откроется окно **Проверка**.

2. Чтобы запустить задачу **Выборочная проверка**, выполните одно из следующих действий:

   - Перетащите файл или папку в окно.
   - Нажмите на кнопку **Выбрать**, чтобы указать файл или папку.

Запустится задача проверки.

Остановка задачи проверки

1. На боковой панели главного окна приложения нажмите **Проверка**.

   Откроется окно **Проверка**.

2. В окне **Проверка** нажмите на кнопку остановки ( ) рядом с задачей проверки, которую вы хотите остановить.

   Откроется окно подтверждения.

3. В окне подтверждения нажмите на кнопку **Остановить**.

Задача проверки остановится.

Вы можете настроить расписание запуска полной и быстрой проверки компьютера.

Настройка расписания запуска задачи проверки из окна Проверка

1. На боковой панели главного окна приложения нажмите **Проверка**.

   Откроется окно **Проверка**.

2. Нажмите на кнопку **Расписание проверки**.

   Откроется окно, в котором вы можете настроить параметры расписания.

3. Установите флажок **Полная проверка** или **Быстрая проверка**.
4. Укажите частоту запуска проверки и время запуска.
5. Нажмите **OK**.

Настройка расписания запуска задачи проверки из окна настройки приложения

1. В строке меню нажмите на значок приложения и выберите пункт **Настройки**.

   Откроется окно настройки приложения.

2. На вкладке **Проверка** нажмите на кнопку **Расписание**.

3. В открывшемся окне установите флажки рядом с названием задач, которые вы хотите запускать по расписанию.

4. Настройте частоту и время запуска задачи проверки.

5. Нажмите на кнопку **OK**, чтобы сохранить изменения в расписании запуска задачи проверки.

Когда вы подключаете внешний диск к компьютеру, приложение Kaspersky Endpoint Security может автоматически запустить проверку диска, запросить проверку или не выполнять никаких действий. Вы можете выбрать действие, которое выполнит приложение, в настройках задачи Проверка внешнего диска.

Выбор действия, которое выполнит приложение Kaspersky Endpoint Security при подключении внешнего диска к компьютеру

1. В строке меню нажмите на значок приложения и выберите пункт **Настройки**.

   Откроется окно настройки приложения.

2. На вкладке **Проверка** в списке слева выберите **Проверка внешних дисков**.

3. В блоке **Если подключен внешний диск** выберите действие, которое приложение Kaspersky Endpoint Security выполнит при подключении внешнего диска.

Задачи полной проверки и быстрой проверки имеют сформированные области проверки. При выполнении задачи полной проверки приложение Kaspersky Endpoint Security проверяет память, объекты автозапуска и все внутренние диски компьютера. При выполнении задачи быстрой проверки приложение проверяет память, объекты автозапуска и системные папки. Вы можете изменить область проверки задачи быстрой проверки.

Примечание. Чтобы значительно уменьшить время выполнения проверки, вы можете пропустить проверку системного тома "только для чтения". По умолчанию Kaspersky Endpoint Security не проверяет системный том "только для чтения" при быстрой проверке и проверяет его при полной проверке.

Примечание. Kaspersky Endpoint Security не проверяет файлы, расположенные в хранилищах OneDrive, iCloud и других облачных хранилищах. Исключите эти файлы из области проверки. В противном случае задача проверки может завершиться с ошибкой *Зараженный файл не удален*.

Включение и выключение проверки системного тома "только для чтения"

1. В строке меню нажмите на значок приложения и выберите пункт **Настройки**.

   Откроется окно настройки приложения.

2. На вкладке **Проверка** в списке слева выберите задачу **Полная проверка** или **Быстрая проверка**.

3. В блоке **Оптимизация** снимите/установите флажок **Пропускать проверку системного тома «только для чтения»**.

   Важно! В целях безопасности оптимизация может быть выключена.

Добавление файла или папки в область проверки задачи быстрой проверки и удаление из нее

1. В строке меню нажмите на значок приложения и выберите пункт **Настройки**.

   Откроется окно настройки приложения.

2. На вкладке **Проверка** в списке слева выберите задачу **Быстрая проверка**.

3. В блоке **Область проверки** нажмите на кнопку **Изменить**.

   Откроется окно со списком объектов, проверяемых в ходе выполнения задачи Быстрой проверки.

4. Отредактируйте список объектов, входящих в область проверки:

- Чтобы добавить файл или папку в область проверки:

  a. Нажмите на кнопку +.

  Откроется всплывающее меню, в котором вы можете выбрать объекты для добавления в область проверки.

  b. Выберите **Файлы и папки**.

  Откроется окно, в котором вы можете выбрать файл или папку.

  c. Выберите файл или папку, которую вы хотите добавить в область проверки.

  d. Нажмите на кнопку **Открыть**.

- Чтобы удалить файл или папку из области проверки:

  a. Выберите объект, который вы хотите удалить.

  b. Перетащите выбранный объект из окна или нажмите на кнопку −.

5. Нажмите на кнопку **Сохранить**.

Добавление в область проверки задачи быстрой проверки объекта из списка стандартных объектов

1. В строке меню нажмите на значок приложения и выберите пункт **Настройки**.

   Откроется окно настройки приложения.

2. На вкладке **Проверка** в списке слева выберите задачу **Быстрая проверка**.

3. В блоке **Область проверки** нажмите на кнопку **Изменить**.

   Откроется окно со списком объектов, входящих в область проверки.

4. Нажмите на кнопку +.

   Откроется всплывающее меню, в котором вы можете выбрать объекты для добавления в область проверки.

5. Во всплывающем меню выберите объект, который вы хотите добавить в область проверки (например, **Память**).

6. Нажмите **ОК**.

Удаление объекта из области проверки задачи быстрой проверки

1. В строке меню нажмите на значок приложения и выберите пункт **Настройки**.

   Откроется окно настройки приложения.

2. На вкладке **Проверка** в списке слева выберите задачу **Быстрая проверка**.

3. В блоке **Область проверки** нажмите на кнопку **Изменить**.

   Откроется окно со списком объектов, входящих в область проверки.

4. Снимите флажок рядом с объектом в списке объектов, включенных в область проверки.

5. Нажмите **ОК**.

При обнаружении угрозы в файле приложение отображает уведомление и выполняет над объектом выбранное действие. Вы можете изменить действие, выполняемое приложением при обнаружении объекта.

Выбор действия, которое Kaspersky Endpoint Security выполнит при обнаружении зараженного файла

1. В строке меню нажмите на значок приложения и выберите пункт **Настройки**.

   Откроется окно настройки приложения.

2. На вкладке **Проверка** выберите задачу в списке.

3. В блоке **Действие** выберите действие, которое приложение выполнит при обнаружении зараженного файла.

Перед лечением или удалением зараженного файла Kaspersky Endpoint Security сохраняет его копию в резервном хранилище, чтобы вы могли восстановить исходный файл, если потребуется.

Результаты выполнения задач проверки и сведения обо всех обнаруженных объектах записываются в отчет.

Примечание. Если при выполнении задачи поиска вредоносного ПО возникли ошибки, запустите ее еще раз. Если повторная попытка выполнения проверки также завершилась с ошибкой, обратитесь в Службу технической поддержки "Лаборатории Касперского".

Просмотр отчета о выполнении задач проверки

1. В строке меню выберите **Защита** > **Отчеты**.

   Откроется окно **Отчеты**.

2. Откройте вкладку **Проверка**.

Задачи обновления

Своевременное обновление антивирусных баз приложения – залог безопасности вашего компьютера. Защита от файловых угроз, Защита от веб-угроз и задачи проверки используют базы приложения для обнаружения и устранения вредоносных программ на вашем компьютере. Базы приложения регулярно пополняются записями о различных видах угроз и способах борьбы с ними, поэтому настоятельно рекомендуется их регулярно обновлять.

Kaspersky Endpoint Security загружает базы приложения и новые модули приложения с серверов обновлений "Лаборатории Касперского" и устанавливает их на ваш компьютер. Kaspersky Endpoint Security также может использовать точки распространения, локальные папки или другие веб-серверы.

Примечание. Для подключения к серверам обновлений и загрузки обновлений требуется доступ в интернет. Если подключение к интернету осуществляется через прокси-сервер, может потребоваться настройка параметров сети.

Обновления баз приложения можно загружать в одном из следующих режимов:

- **Автоматически**. Kaspersky Endpoint Security периодически проверяет наличие обновлений на серверах обновлений "Лаборатории Касперского". Если обновление доступно на сервере обновлений, Kaspersky Endpoint Security загружает его в фоновом режиме и устанавливает на компьютер. Этот режим включен по умолчанию.

- **Вручную**. Вы можете в любое время проверить наличие обновлений Kaspersky Endpoint Security вручную.

Включение и выключение автоматической загрузки обновлений баз Kaspersky Endpoint Security

1. В строке меню нажмите на значок приложения и выберите пункт **Настройки**.

   Откроется окно настройки приложения.

2. На вкладке **Обновление** в блоке **Базы** установите/снимите флажок **Загружать обновления автоматически**.

Проверка наличия обновлений баз Kaspersky Endpoint Security

1. На боковой панели главного окна приложения, нажмите **Обновление**.

   Откроется окно **Обновление**.

2. Нажмите на кнопку **Обновить**.

Запустится обновление баз приложения.

Также вы можете запустить задачу обновления одним из следующих способов:

- Нажмите на значок приложения и выберите **Обновление**.
- В строке меню выберите **Защита** > **Обновление**.

Во время обновления базы и модули приложения на вашем компьютере сравниваются с доступными на серверах обновлений. Если на вашем компьютере установлена последняя версия баз, в окне **Обновление** отображается сообщение о том, что базы приложения актуальны. Если версия и базы приложения отличаются от доступных на серверах обновлений, на компьютер загружаются и устанавливаются только недостающие обновления. Инкрементное обновление баз приложения занимает меньше времени и требует меньше веб-трафика.

Если подключение к интернету осуществляется через прокси-сервер, вы можете настроить параметры подключения к прокси-серверу. Kaspersky Endpoint Security использует эти параметры для обновления баз приложения и загрузки обновлений модулей приложения.

Настройка параметров подключения к прокси-серверу

1. В строке меню нажмите на значок приложения и выберите пункт **Настройки**.

   Откроется окно настройки приложения.

2. Выберите вкладку **Обновление**.

3. В блоке **Прокси** установите флажок **Использовать прокси-сервер** и нажмите на кнопку **Настройки**.

   Откроется окно, в котором вы можете настроить параметры подключения к прокси серверу.

4. Настройте параметры подключения к прокси-серверу.

5. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения параметров подключения к прокси-серверу.

Перед обновлением баз приложения Kaspersky Endpoint Security создает их резервную копию на случай, если возникнет необходимость вернуться к использованию предыдущей версии баз. Вам может понадобиться откат обновления, если новая версия баз приложения содержит неправильную сигнатуру, из-за которой Kaspersky Endpoint Security блокирует безопасную программу.

Примечание. При повреждении баз Kaspersky Endpoint Security рекомендуется запустить обновление, чтобы загрузить и установить последнюю версию баз приложения.

Откат последнего обновления

1. В строке меню нажмите на значок приложения и выберите пункт **Настройки**.

   Откроется окно настройки приложения.

2. Выберите вкладку **Обновление**.

3. В блоке **Откат обновления** нажмите на кнопку **Откатить обновление**.

Kaspersky Endpoint Security предоставляет подробный отчет о выполнении задач обновления в окне **Отчеты**.

Просмотр отчета о выполнении задачи обновления

1. В строке меню выберите **Защита** > **Отчеты**.
2. Откроется окно **Отчеты**.
3. Выберите вкладку **Обновление баз**.

Примечание. Функциональность обновлений (включая обновления сигнатур вредоносного ПО и обновления кодовой базы), а также функциональность KSN могут быть недоступны в ПО на территории США.

Локальные задачи

Задача проверки внешних дисков

Kaspersky Endpoint Security может проверять все файлы, которые вы запускаете или копируете, даже если файлы расположены на внешнем диске. Для предотвращения распространения вредоносного ПО, вы можете настроить автоматическую проверку внешних дисков при их подключении к устройству.

Можно настроить следующие параметры проверки внешних дисков:

- **Действие, которое Kaspersky Endpoint Security выполняет при подключении внешнего диска.**

  Проверить

  Если выбран этот вариант, Kaspersky Endpoint Security выполнит поиск вредоносного ПО на подключенном внешнем диске.

  Этот вариант выбран по умолчанию.

  Не предпринимать никаких действий

  Если выбран этот вариант, Kaspersky Endpoint Security не будет проверять подключенный внешний диск.

- **Действие, которое Kaspersky Endpoint Security выполняет при обнаружении зараженного объекта.**

  Лечить. Удалять, если лечение невозможно

  Если выбран этот вариант, Kaspersky Endpoint Security блокирует доступ к зараженному объекту и пытается его лечить, не запрашивая подтверждения пользователя.

  Если объект вылечен, Kaspersky Endpoint Security восстанавливает его в исходном месте под исходным именем. Если лечение невозможно, Kaspersky Endpoint Security удаляет зараженные объекты, которые не удалось вылечить.

  Этот вариант выбран по умолчанию.

  Запрашивать действие

  Если выбран этот вариант, Kaspersky Endpoint Security отображает окно уведомления с информацией о вредоносном объекте и предлагает пользователю выбрать действие, которое требуется выполнить. В зависимости от статуса объекта действия могут отличаться.

Вы можете настроить проверку внешних дисков в Консоли администрирования, в Web Console или в приложении Kaspersky Endpoint Security.

Как настроить запуск проверки внешних дисков в Консоли администрирования (MMC)

1. Запустите Консоль администрирования Kaspersky Security Center.
2. Разверните узел **Сервер администрирования <Имя сервера>**.
3. В дереве консоли выберите папку **Управляемые устройства**.
4. В рабочей области выберите вкладку **Политики**.
5. По правой клавише мыши откройте контекстное меню политики, параметры которой вы хотите настроить, и выберите **Свойства**.
6. В окне **Свойства** выберите **Локальные задачи** → **Проверка внешних дисков**.
7. Настройте параметры задачи.

8. Нажмите **OK**, чтобы сохранить изменения.

[Как настроить запуск проверки внешних дисков в Web Console и Cloud Console]

1. В главном окне Web Console выберите **Устройства** → **Политики и профили политик**.
2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры программы**.
4. Выберите **Локальные задачи** → **Проверка внешних дисков**.
5. Настройте параметры задачи.
6. Нажмите OK, чтобы сохранить изменения.

[Как настроить запуск проверки внешних дисков в интерфейсе приложения]

1. В строке меню нажмите на значок приложения и выберите пункт **Настройки**.

   Откроется окно настройки приложения.
2. На вкладке **Проверка** в списке слева выберите **Проверка внешних дисков**.
3. В блоке **Если подключен внешний диск** выберите действие, которое приложение Kaspersky Endpoint Security выполнит при подключении внешнего диска.

Резервное хранилище

Во время лечения зараженных файлов не всегда удается сохранить их целостность. Если вылеченный файл содержал важную информацию, которая в результате лечения стала полностью или частично недоступной, вы можете восстановить исходный файл из резервного хранилища.

Резервная копия – копия опасного файла, которая создается при первом лечении или удалении этого файла. Резервная копия хранится в резервном хранилище.

Резервное хранилище – это специальное хранилище, содержащее резервные копии файлов, которые были удалены или изменены в процессе лечения. Основная функция резервного хранилища – обеспечить возможность в любой момент восстановить исходный файл. Файлы в резервном хранилище хранятся в специальном формате и не представляют опасности для компьютера.

Просмотр содержимого резервного хранилища

1. В строке меню выберите **Защита** > **Обнаруженные объекты**.

   Откроется окно **Обнаруженные объекты**.

2. В блоке **Резервное хранилище** просмотрите список файлов, резервные копии которых сохранены.

Вы можете восстанавливать и удалять резервные копии файлов из резервного хранилища.

Восстановление резервной копии файла из резервного хранилища

1. В строке меню выберите **Защита** > **Обнаруженные объекты**.

   Откроется окно **Обнаруженные объекты**.

2. В блоке **Резервное хранилище** нажмите на кнопку ••• рядом с файлом, который вы хотите восстановить.

   Откроется всплывающее меню.

3. Выберите **Восстановить файл**.

   Откроется окно, в котором вам нужно указать имя файла, тег и папку, в которую он будет восстановлен. По умолчанию уже указаны исходное имя файла и исходное местоположение.

4. Укажите имя файла и папку, в которую нужно его восстановить.

5. Нажмите на кнопку **Сохранить**.

Приложение восстановит файл в указанное местоположение с указанным именем.

Сразу после восстановления вам нужно проверить файл на вредоносное ПО. Возможно, с обновленными антивирусными базами его удастся вылечить без потери целостности.

Важно! Не рекомендуется восстанавливать резервные копии файлов без крайней необходимости, так как это может привести к заражению вашего компьютера.

Удаление резервной копии файла из резервного хранилища

1. В строке меню выберите **Защита** > **Обнаруженные объекты**.

   Откроется окно **Обнаруженные объекты**.

2. В блоке **Резервное хранилище** выполните следующие действия:

   - Если вы хотите удалить все резервные копии файлов, нажмите на кнопку **Удалить все**.
   - Чтобы удалить выбранную резервную копию файла, нажмите на кнопку ••• рядом с названием файла и выберите **Удалить копию**.

По умолчанию срок хранения файлов в резервном хранилище составляет 30 дней. По истечении этого срока файлы удаляются. Вы можете изменить максимальный срок хранения файлов в резервном хранилище или отменить ограничение срока хранения.

Настройка срока хранения файлов в резервном хранилище

1. В строке меню нажмите на значок приложения и выберите пункт **Настройки**.

   Откроется окно настройки приложения.

2. На вкладке **Угрозы** в блоке **Резервное хранилище** установите флажок **Удалять объекты из резервного хранилища через <значение> дней** и укажите время, по истечении которого файлы, находящиеся в резервном хранилище, автоматически удаляются.

Отчеты

Вы можете просмотреть отчет Kaspersky Endpoint Security со списком всех обнаруженных объектов на вкладке **Обработанные объекты**. Системные события отображаются на вкладке **Системные события**. Дополнительно, подробный отчет формируется для каждого компонента приложения: Защиты от файловых угроз, Защиты от веб-угроз, Защиты от сетевых угроз, Анализа поведения, задач проверки и обновления.

Открытие окна Отчеты

В строке меню выберите **Защита** > **Отчеты**.

Kaspersky Endpoint Security позволяет сохранить отчет о своей работе в текстовом формате. Эта возможность может понадобиться, если в работе компонентов приложения или при выполнении задач возникает ошибка, которую вы не можете устранить самостоятельно, и вам требуется помощь Службы технической поддержки "Лаборатории Касперского". В этом случае отправьте отчет в текстовом формате в Службу технической поддержки "Лаборатории Касперского", чтобы наши специалисты могли изучить проблему и максимально быстро решить ее.

Экспорт отчета о работе компонентов или задач Kaspersky Endpoint Security в текстовый файл

1. В строке меню выберите **Защита** > **Отчеты**.

   Откроется окно **Отчеты**.

2. В левой части окна выберите вкладку с названием нужного отчета.

3. В верхнем правом углу окна нажмите на кнопку  .

4. В открывшемся окне укажите имя файла, теги и папку, в которой нужно сохранить отчет.

5. Нажмите на кнопку **Сохранить**.

По умолчанию Kaspersky Endpoint Security не сохраняет в отчете информационные события. Вы можете разрешить запись информационных событий в отчеты.

Включение записи информационных событий в отчеты

1. В строке меню нажмите на значок приложения и выберите пункт **Настройки**.

   Откроется окно настройки приложения.

2. На вкладке **Интерфейс**, в блоке **Отчеты** установите флажок **Записывать некритические события**, чтобы получать уведомления об информационных событиях Kaspersky Endpoint Security.

Managed Detection and Response

Компонент Managed Detection and Response был добавлен в Kaspersky Endpoint Security в версии 11.2. Компонент обеспечивает взаимодействие с решением Kaspersky Managed Detection and Response. *Kaspersky Managed Detection and Response (MDR)* обеспечивает непрерывный поиск, обнаружение и устранение угроз, направленных на вашу организацию. Подробную информацию о работе решения см. в *справке Kaspersky Managed Detection and Response* .

При взаимодействии с Kaspersky Managed Detection and Response приложение позволяет выполнять следующие функции:

- Активация Managed Detection and Response с помощью конфигурационного файла BLOB.
- Выполнение команд от Kaspersky Managed Detection and Response.
- Отправка данных телеметрии для обнаружения угроз в Kaspersky Managed Detection and Response.

Компонент Managed Detection and Response имеет следующие дополнительные требования:

- операционная система macOS 12 или более поздней версии;
- компьютер Mac на базе процессора Intel или Apple;
- активная лицензия для Kaspersky Endpoint Security.

Интеграция с Kaspersky Managed Detection and Response

Интеграция с Kaspersky Managed Detection and Response состоит из следующих этапов:

1. **Настройка прокси-сервера Kaspersky Security Network.**

   Прокси-сервер Kaspersky Security Network обеспечивает обмен данными между компьютерами и инфраструктурой облачных служб Kaspersky Security Network через Сервер администрирования, а не напрямую.

Загрузите конфигурационный файл Kaspersky Security Network в свойствах Сервера администрирования. Конфигурационный файл Kaspersky Security Network находится в ZIP-архиве конфигурационного файла MDR. Вы можете получить ZIP-архив в Консоли Kaspersky Managed Detection and Response. Подробнее о настройке прокси-сервера Kaspersky Security Network см. в *справке Kaspersky Security Center*.

В результате Kaspersky Endpoint Security будет использовать Локальный KSN для определения репутации файлов, программ и веб-сайтов. Статус *"Инфраструктура: Kaspersky Private Security Network"* будет отображаться в параметрах политики в разделе Kaspersky Security Network.

Использование Локального KSN с Kaspersky Managed Detection and Response гарантирует отправку телеметрии на выделенные серверы, соответствующие требованиям Общего регламента по защите данных (GDPR). Если вы не настроите Локальный KSN, телеметрия будет отправляться в Глобальный KSN. Это может являться нарушением законов вашей страны.

Важно! Для работы Managed Detection and Response необходимо включить расширенный режим работы KSN.

2 **Активация Managed Detection and Response**

Загрузите конфигурационный файл BLOB в политике Kaspersky Endpoint Security (см. инструкцию ниже). BLOB-файл содержит идентификатор клиента и информацию о лицензии Kaspersky Managed Detection and Response. BLOB-файл находится в ZIP-архиве конфигурационного файла MDR. Вы можете получить ZIP-архив в Консоли Kaspersky Managed Detection and Response. Подробную информацию о BLOB-файле см. в *справке Kaspersky Managed Detection and Response*.

Активация Managed Detection and Response в Консоли администрирования (MMC)

1. Запустите Консоль администрирования Kaspersky Security Center.
2. Разверните узел **Сервер администрирования <Имя сервера>**.
3. В дереве консоли выберите папку **Управляемые устройства**.
4. В рабочей области выберите вкладку **Политики**.
5. По правой клавише мыши откройте контекстное меню политики, параметры которой вы хотите настроить, и выберите **Свойства**.
6. В окне **Свойства** выберите **Detection and Response** > **Managed Detection and Response**.

7. Установите флажок **Managed Detection and Response**.

8. В блоке **Конфигурационный файл MDR** нажмите на кнопку **Импортировать** и выберите BLOB-файл, полученный в Консоли Kaspersky Managed Detection and Response. Файл имеет расширение P7.

9. Нажмите **OK**, чтобы сохранить изменения.

[Активация Managed Detection and Response в Web Console и Cloud Console]

1. В главном окне Web Console выберите **Устройства** > **Политики и профили политик**.

2. Нажмите на название политики Kaspersky Endpoint Security для Mac.

3. Откроется окно свойств политики.

4. Выберите вкладку **Параметры программы**.

5. Выберите **Detection and Response** > **Managed Detection and Response**.

6. Включите переключатель **Managed Detection and Response**.

7. Нажмите на кнопку **Импортировать** и выберите BLOB-файл, полученный в Консоли Kaspersky Managed Detection and Response. Файл имеет расширение P7.

8. Сохраните внесенные изменения.

В результате Kaspersky Endpoint Security проверит BLOB-файл. Проверка BLOB-файла включает в себя проверку цифровой подписи и срока действия лицензии. Если BLOB-файл прошел проверку, Kaspersky Endpoint Security загрузит файл и отправит файл на компьютер при следующей синхронизации с Kaspersky Security Center.

Endpoint Detection and Response (KATA)

Kaspersky Endpoint Security поддерживает интеграцию с компонентом Kaspersky Endpoint Detection and Response в составе решения Kaspersky Anti Targeted Attack Platform. Это решение предназначено для оперативного обнаружения продвинутых угроз, таких как целевые атаки, сложные постоянные угрозы, атаки "нулевого дня" и другие. Подробную информацию о работе решения см. в *справке Kaspersky Anti Targeted Attack Platform*.

Когда настроена интеграция с Endpoint Detection and Response (KATA), сервер KATA получает информацию о событиях, происходящих в работе Kaspersky Endpoint Security, угрозах, обнаруженных приложением, а также информацию об обработке этих угроз. Kaspersky Endpoint Security может выполнять задачи, запущенные в веб-интерфейсе Kaspersky Anti Targeted Attack Platform, чтобы отреагировать на обнаруженные угрозы.

Компонент Endpoint Detection and Response (KATA) имеет следующие дополнительные требования:

- Kaspersky Anti Targeted Attack Platform 6.0 или более поздней версии.
- Kaspersky Security Center 14.2 или более поздней версии.
- Интеграцию с Endpoint Detection and Response (KATA) можно настроить в Консоли администрирования Kaspersky Security Center (MMC), Web Console или Cloud Console.

Интеграция с Kaspersky Endpoint Detection and Response (KATA)

Интеграция с Kaspersky Endpoint Detection and Response (KATA) состоит из следующих этапов:

1. **Установка компонента Endpoint Detection and Response.**

   Вы можете выбрать компонент Endpoint Detection and Response во время установки Kaspersky Endpoint Security.

2. **Активация Endpoint Detection and Response**

   Если компонент Endpoint Detection and Response не поддерживается вашей текущей лицензией, вам необходимо активировать Kaspersky Endpoint Detection and Response отдельно.

   Вы можете проверить, поддерживается ли функциональность Endpoint Detection and Response текущей лицензией в окне **Лицензия**.

3. **Подключение к серверу KATA.**

   Kaspersky Anti Targeted Attack Platform требует установки доверенного соединения между Kaspersky Endpoint Security и сервером KATA. Чтобы настроить доверенное соединение, вам необходимо использовать TLS-сертификат. Вы можете загрузить TLS-сертификат в веб-интерфейсе Kaspersky Anti Targeted Attack Platform. Подробную информацию о загрузке сертификата см. в *справке Kaspersky Anti Targeted Attack Platform* .

По умолчанию Kaspersky Endpoint Security проверяет TLS-сертификат только сервера KATA. Чтобы сделать соединение более безопасным, вы можете включить двустороннюю аутентификацию. Чтобы включить двустороннюю аутентификацию, вам необходимо использовать криптоконтейнер, защищенный паролем. Подробную информацию о загрузке криптоконтейнера см. в *справке Kaspersky Anti Targeted Attack Platform*.

Подключение компьютеров с Kaspersky Endpoint Security к серверу KATA с помощью Консоли администрирования

1. Запустите Консоль администрирования.
2. Разверните узел **Сервер администрирования <Имя сервера>**.
3. В дереве консоли выберите папку **Управляемые устройства**.
4. В рабочей области выберите вкладку **Политики**.
5. По правой клавише мыши откройте контекстное меню политики, параметры которой вы хотите настроить, и выберите **Свойства**.
6. В окне **Свойства** выберите **Detection and Response** > **Endpoint Detection and Response (KATA)**.
7. Установите флажок **Endpoint Detection and Response (KATA)**.
8. Нажмите на кнопку **Параметры подключения к серверам**.
9. В открывшемся окне **Параметры подключения к серверам** настройте следующие параметры:
   - Нажмите на кнопку **Добавить TLS-сертификат**, чтобы выбрать сертификат TLS, который будет использоваться для установки доверенного соединения с сервером KATA.
   - Если вы хотите изменить время ожидания ответа сервера KATA, укажите время ожидания в поле **Время ожидания (сек.)**. По истечении времени ожидания ответа Kaspersky Endpoint Security пытается подключиться к другому серверу KATA.
   - Если вы хотите использовать двустороннюю аутентификацию, установите флажок **Использовать двустороннюю аутентификацию**. Нажмите на кнопку **Загрузить криптоконтейнер**, чтобы выбрать файл криптоконтейнера и введите пароль в поле **Пароль от криптоконтейнера**.

10. Нажмите на кнопку **Сохранить**.
11. Чтобы добавить сервер KATA, нажмите на кнопку **Добавить**.
12. В открывшемся окне **Сервер KATA** укажите адрес и порт сервера и нажмите на кнопку **Сохранить**.
13. Нажмите **OK**, чтобы сохранить изменения.

[Подключение компьютеров с Kaspersky Endpoint Security к серверу KATA с помощью Web Console]

1. В главном окне Web Console выберите **Устройства** > **Политики и профили политик**.
2. Нажмите на название политики Kaspersky Endpoint Security для Mac.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры программы**.
4. Выберите **Detection and Response** > **Endpoint Detection and Response (KATA)**.
5. Включите переключатель **Endpoint Detection and Response (KATA)**.
6. Нажмите на кнопку **Параметры подключения к серверам**.
7. В открывшемся окне **Параметры подключения к серверам** настройте следующие параметры:

   - Нажмите на кнопку **Добавить TLS-сертификат**, чтобы выбрать сертификат TLS, который будет использоваться для установки доверенного соединения с сервером KATA.
   - Если вы хотите изменить время ожидания ответа сервера KATA, укажите время ожидания в поле **Время ожидания (сек.)**. По истечении времени ожидания ответа Kaspersky Endpoint Security пытается подключиться к другому серверу KATA.
   - Если вы хотите использовать двустороннюю аутентификацию, установите флажок **Использовать двустороннюю аутентификацию**. Нажмите на кнопку **Загрузить криптоконтейнер**, чтобы выбрать файл криптоконтейнера и введите пароль в поле **Пароль от криптоконтейнера**.

8. Нажмите **OK**.

9. Чтобы добавить сервер KATA, нажмите на кнопку **Добавить**.

10. В открывшемся окне укажите адрес и порт сервера и нажмите на кнопку **OK**.

11. Сохраните внесенные изменения.

В результате компьютеры появятся в веб-интерфейсе Kaspersky Anti Targeted Attack Platform.

Endpoint Detection and Response Optimum

Начиная с версии Kaspersky Endpoint Security для Mac 12.1 в приложение добавлен встроенный агент для работы решения Kaspersky Endpoint Detection and Response Optimum (далее также "EDR Optimum"). Это решение предназначено для защиты корпоративной ИТ-инфраструктуры от сложных киберугроз. Функционал решения сочетают автоматическое обнаружение угроз с возможностью реагирования на эти угрозы для противодействия сложным атакам, в том числе новым эксплойтам (exploits), программам-вымогателям (ransomware), бесфайловым атакам (fileless attacks), а также методам, использующим законные системные инструменты. Подробнее о решении см. в справке Kaspersky Endpoint Detection and Response Optimum.

Kaspersky Endpoint Detection and Response выполняет обзор и анализ развития угрозы и предоставляет *Сотруднику службы безопасности* или *Администратору* информацию о потенциальной атаке, необходимую для принятия своевременных действий по реагированию. Kaspersky Endpoint Detection and Response показывает детали алерта в отдельном окне. *Детали алерта* – инструмент для просмотра всей собранной информации об обнаруженной угрозе. Детали алерта содержат, например, историю появления файлов на компьютере. Подробнее о работе с деталями алерта см. в справке Kaspersky Endpoint Detection and Response Optimum.

Примечание. Вы можете настроить компонент EDR Optimum в Web Console.

Параметры Endpoint Detection and Response

Параметр	Описание
Сетевая изоляция	Автоматическая изоляция компьютера от сети в результате реагирования на обнаруженные угрозы. После включения Сетевой изоляции приложение разрывает все активные соединения и блокирует все новые соединения TCP/IP на компьютере. Приложение оставляет активными только следующие соединения:

	• соединения, указанные в исключениях из Сетевой изоляции; • соединения, инициированные службами Kaspersky Endpoint Security; • соединения, инициированные Агентом администрирования Kaspersky Security Center.
Разблокировать автоматически изолированный компьютер через N часов	Сетевая изоляция может быть выключена автоматически по истечении заданного периода времени или вручную. По умолчанию, Kaspersky Endpoint Security выключает Сетевую изоляцию через 8 часов после начала изоляции.
Исключения из сетевой изоляции	Список правил исключений из Сетевой изоляции. Сетевые соединения, подпадающие под заданные правила, не будут заблокированы на компьютерах после включения Сетевой изоляции. Для настройки исключений из Сетевой изоляции в приложении доступен список стандартных сетевых профилей. По умолчанию исключения входят сетевые профили, состоящие из правил, обеспечивающих бесперебойную работу устройств с ролями DNS/DHCP-сервер и DNS/DHCP-клиент. Также вы можете изменить параметры стандартных сетевых профилей или задать исключения вручную. **Важно!** Исключения, заданные в свойствах политики,

Интеграция с Endpoint Detection and Response Optimum

Для интеграции с Kaspersky Endpoint Detection and Response вам нужно добавить компонент Endpoint Detection and Response Optimum (EDR Optimum) и настроить параметры Kaspersky Endpoint Security.

Примечание. Компоненты EDR Optimum и Endpoint Detection and Response (KATA) несовместимы между собой.

Для работы Endpoint Detection and Response должны быть выполнены следующие условия:

- Kaspersky Security Center 13.2 или более поздней версии. В более ранних версиях Kaspersky Security Center невозможно активировать функциональность Endpoint Detection and Response.

- Установлен плагин управления Kaspersky Endpoint Detection and Response. Это единый плагин для работы с агентами в операционных системах Windows, Mac и Linux. При работе

с Endpoint Detection and Response Optimum вам потребуется плагин управления Kaspersky Endpoint Security для создания задач реагирования на угрозы и плагин управления EDR для просмотра деталей обнаружения.

- Компонент EDR Optimum в составе Kaspersky Endpoint Security поддерживает работу с решением Kaspersky Endpoint Detection and Response Optimum версии 3.0. Взаимодействие с более ранними версиями Kaspersky Endpoint Detection and Response Optimum не поддерживается.
- Управление EDR Optimum доступно в Web Console.
- Приложение активировано и функциональность входит в лицензию.
- Компонент Endpoint Detection and Response включен.

Интеграция с Kaspersky Endpoint Detection and Response Optimum

Интеграция с Kaspersky Endpoint Detection and Response Optimum состоит из следующих этапов:

1. **Установка компонента Endpoint Detection and Response Optimum**

   Вы можете выбрать компонент Endpoint Detection and Response во время установки Kaspersky Endpoint Security.

2. **Активация Endpoint Detection and Response**

   Если компонент Endpoint Detection and Response не поддерживается вашей текущей лицензией, вам необходимо активировать Kaspersky Endpoint Detection and Response отдельно.

   Вы можете проверить, поддерживается ли функциональность Endpoint Detection and Response текущей лицензией в окне **Лицензия**.

3. **Включение компонента Endpoint Detection and Response**

   Вы можете включить или выключить компонент в настройках политики Kaspersky Endpoint Security для Mac.

   Как включить или выключить компонент Endpoint Detection and Response в Web Console

   1. В главном окне Web Console выберите **Активы (Устройства)** → **Политики и профили политик**.
   2. Нажмите на название политики Kaspersky Endpoint Security.

Откроется окно свойств политики.

3. Выберите вкладку **Параметры программы**.
4. Перейдите в раздел **Detection and Response → Endpoint Detection and Response**.
5. Включите переключатель **Endpoint Detection and Response**.
6. Сохраните внесенные изменения.

Проверка индикаторов компрометации

Индикатор компрометации (Indicator of Compromise, IOC) – набор данных об объекте или активности, который указывает на несанкционированный доступ к компьютеру (компрометация данных). Например, индикатором компрометации может быть большое количество неудачных попыток входа в систему. Задача **Поиск IOC** позволяет обнаруживать индикаторы компрометации на компьютере и выполнять действия по реагированию на угрозы.

Для поиска индикаторов компрометации Kaspersky Endpoint Security использует IOC-файлы. IOC-файлы – файлы, содержащие набор индикаторов, при совпадении с которыми приложение считает событие обнаружением. IOC-файлы должны соответствовать требованиям к IOC-файлам.

Режим запуска задачи Поиск IOC

Kaspersky Endpoint Detection and Response позволяет создавать стандартные задачи Поиска IOC для обнаружения компрометации данных. Стандартная задача Поиска IOC – групповая или локальная задача, которые создаются и настраиваются вручную в Web Console. Для запуска задач используются IOC-файлы, подготовленные пользователем. Если вы хотите добавить индикатор компрометации вручную, ознакомьтесь с требованиями к IOC-файлам.

Создание задачи Поиск IOC

Вы можете создавать задачи Поиск IOC вручную следующими способами:

- В деталях алерта (только для EDR Optimum).

  Детали алерта – инструмент для просмотра всей собранной информации об обнаруженной угрозе. Детали алерта содержат, например, историю появления файлов на компьютере. Подробнее о работе с деталями алерта см. в справке Kaspersky Endpoint Detection and Response Optimum.

- С помощью мастера создания задач.

Чтобы создать задачу Поиск IOC, выполните следующие действия:

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

   Откроется список задач.

2. Нажмите на кнопку **Добавить**.

   Запустится **мастер создания задачи**.

3. Настройте параметры задачи:

   a. В раскрывающемся списке **Программа** выберите Kaspersky Endpoint Security для Mac (12.2).

   b. В раскрывающемся списке **Тип задачи** выберите **Поиск IOC**.

   c. В поле **Название задачи** введите короткое описание задачи.

   d. В блоке **Выбор устройств, которым будет назначена задача** выберите область действия задачи.

4. Выберите устройства в соответствии с выбранным вариантом области действия задачи.

5. В разделе **Настройки поиска IOC** загрузите IOC-файлы для поиска индикаторов компрометации. Вы можете добавить IOC-файл или сгенерировать его из файла, содержащего хэши файлов или IP-адреса.

   После загрузки IOC-файлов вы можете просмотреть и отредактировать список индикаторов из IOC-файлов.

   > **Примечание.** Не рекомендуется добавлять или удалять IOC-файлы после запуска задачи. Это может привести к некорректному отображению результатов поиска IOC для предыдущих запусков задачи. Для поиска индикаторов компрометации по новым IOC-файлам рекомендуется добавлять новые задачи.

6. Настройте действия при обнаружении индикатора компрометации:

   - **Изолировать компьютер от сети**. Если выбран этот вариант действия, то Kaspersky Endpoint Security изолирует компьютер от сети для предотвращения распространения угрозы. Вы можете настроить время изоляции в параметрах компонента Endpoint Detection and Response.

   - **Копию поместить на Карантин, объект удалить**. Если выбран этот вариант действия, то Kaspersky Endpoint Security удаляет вредоносный объект, обнаруженный на компьютере. Перед удалением объекта Kaspersky Endpoint Security формирует его

резервную копию на тот случай, если впоследствии понадобится восстановить объект. Kaspersky Endpoint Security помещает резервную копию на карантин.

- **Запускать проверку важных областей**. Если выбран этот вариант действия, то Kaspersky Endpoint Security запускает задачу Быстрая проверка. По умолчанию Kaspersky Endpoint Security проверяет память, объекты автозапуска и системные папки.

7. Перейдите в раздел **Дополнительно**.
8. Выберите типы данных (IOC-документы), которые необходимо анализировать во время выполнения задачи.

> **Примечание.** Kaspersky Endpoint Security автоматически выбирает типы данных (IOC-документы) для задачи Поиск IOC в соответствии с содержанием загруженных IOC-файлов. Не рекомендуется самостоятельно отменять выбор типов данных.

Дополнительно вы можете настроить области поиска для следующих типов данных:

- **Процессы - ProcessItem**
- **Файлы - FileItem**
- **Сетевые порты - PortItem**
- **Учетные записи пользователей - UserItem**
- **ARP-таблицы – ArpEntryItem**
- **Системные объекты - SystemInfoItem**
- **История браузера - UrlHistoryItem**
- **Таблицы маршрутизации – RouteEntryItem**

9. Нажмите **OK**.
10. Выберите учетную запись пользователя, права которого требуется использовать для запуска задачи. Нажмите **Далее**.

> **Примечание.** По умолчанию Kaspersky Endpoint Security запускает задачу под системной учетной записью (root).

11. На шаге **Завершение создания задачи** нажмите на кнопку **Готово**, чтобы создать задачу и закрыть мастер.

    Если включен параметр **Открыть окно свойств задачи после ее создания**, откроется окно параметров задачи. В этом окне можно проверить параметры задачи, изменить их или при необходимости настроить расписание запуска задачи.

12. Нажмите на новую задачу.

    Откроется окно свойств задачи.

13. Выберите вкладку **Расписание**.

14. Настройте расписание запуска задачи.

    > **Примечание.** Убедитесь, что компьютер включен для выполнения задачи.

15. Нажмите на кнопку **Сохранить**.

16. Чтобы запустить задачу немедленно, независимо от настроенного расписания, выполните следующие действия:

    a. Установите флажок напротив задачи.

17. Нажмите на кнопку **Выполнить**.

    В результате Kaspersky Endpoint Security запустит поиск индикаторов компрометации на компьютере. Вы можете просмотреть результаты выполнения задачи в свойствах задачи в разделе **Результаты**. Информацию об обнаруженных индикаторах компрометации вы можете посмотреть в свойствах задачи **Параметры программы** → **Результаты поиска IOC**.

> **Примечание.** Срок хранения результатов поиска IOC составляет 30 дней. По истечении этого времени Kaspersky Endpoint Security автоматически удаляет старые записи.

Помещение файла на карантин

Развернуть всё | Свернуть всё

При реагировании на угрозы Kaspersky Endpoint Detection and Response может создавать задачи *Помещение файла на карантин*. Это нужно, чтобы минимизировать последствия угрозы. *Карантин* – это специальное локальное хранилище на компьютере. Пользователь может поместить на карантин файлы, которые считает опасными для компьютера. Файлы на карантине хранятся в зашифрованном виде и не угрожают безопасности устройства. Kaspersky Endpoint Security использует Резервное хранилище в качестве файлового хранилища. Подробнее о работе с карантином в составе решений см. в справке Kaspersky Endpoint Detection and Response Optimum.

Вы можете создавать задачи *Помещение файла на карантин* следующими способами:

- В деталях алерта (только для EDR Optimum).

  Детали алерта – инструмент для просмотра всей собранной информации об обнаруженной угрозе. Детали алерта содержат, например, историю появления файлов на компьютере. Подробнее о работе с деталями алерта см. в справке Kaspersky Endpoint Detection and Response Optimum.

- С помощью мастера создания задач.

  Вам нужно ввести путь к файлу или хеш файла (SHA256 или MD5), или путь к файлу и хеш файла.

Задача *Помещение файла на карантин* имеет следующие ограничения:

- Размер файла не должен превышать 100 МБ.
- Вы можете настроить параметры задачи для EDR Optimum в Web Console.
- Емкость Резервного хранилища ограничена свободным дисковым пространством.

Чтобы создать задачу Помещение файла на карантин, выполните следующие действия:

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

   Откроется список задач.

2. Нажмите на кнопку **Добавить**.

   Запустится **мастер создания задачи**.

3. Настройте параметры задачи:

   a. В раскрывающемся списке **Программа** выберите Kaspersky Endpoint Security для Mac (12.2).

   b. В раскрывающемся списке **Тип задачи** выберите **Помещение файла на карантин**.

   c. В поле **Название задачи** введите короткое описание задачи.

d. Выберите один из следующих вариантов:

- **Назначить задачу группе администрирования**

  Задача назначается устройствам, входящим в ранее созданную группу администрирования. Можно указать одну из существующих групп или создать новую группу.

  Например, вы можете использовать этот параметр, чтобы запустить задачу отправки сообщения пользователям, если сообщение предназначено для устройств из определенной группы администрирования.

  Если задача назначена группе администрирования, вкладка **Безопасность** не отображается в окне свойств задачи, поскольку групповые задачи подчиняются параметрам безопасности групп, к которым они относятся.

- **Задать адреса устройств вручную или импортировать из списка**

  Вы можете задавать NetBIOS-имена, DNS-имена, IP-адреса, а также диапазоны IP-адресов устройств, которым нужно назначить задачу.

  Вы можете использовать этот параметр для выполнения задачи для заданной подсети. Например, вы можете установить определенное приложение на устройства бухгалтеров или проверять устройства в подсети, которое, вероятно, заражено.

- **Назначить задачу выборке устройств**

  Задача назначается устройствам, входящим в выборку устройств. Можно указать одну из существующих выборок.

  Например, вы можете использовать этот параметр, чтобы запустить задачу на устройствах с определенной версией операционной системы.

4. Выберите устройства в соответствии с выбранным вариантом области действия задачи.

5. На шаге **Область действия задачи** укажите группу администрирования, устройства с определенными адресами или выборку устройств.

   Доступные параметры зависят от параметра, выбранного на предыдущем шаге.

6. В списке файлов нажмите на кнопку **Добавить**.

   Запустится мастер добавления файла.

7. В раскрывающемся списке **Укажите файл, который нужно поместить на Карантин**, выберите один из вариантов и заполните необходимые поля. Для добавления файла вам нужно ввести полный путь к файлу или хеш файла и путь к файлу.

8. Если вы хотите, чтобы задача была применима к критическим объектам системы, установите флажок **Применить к критическим объектам системы**.

9. Выберите учетную запись пользователя, права которого требуется использовать для запуска задачи. Нажмите **Далее**.

   > **Примечание.** По умолчанию Kaspersky Endpoint Security запускает задачу под системной учетной записью (root).

10. На шаге **Завершение создания задачи** нажмите на кнопку **Готово**, чтобы создать задачу и закрыть мастер.

    Если включен параметр **Открыть окно свойств задачи после ее создания**, откроется окно параметров задачи. В этом окне можно проверить параметры задачи, изменить их или при необходимости настроить расписание запуска задачи.

11. Нажмите на новую задачу.

    Откроется окно свойств задачи.

12. Выберите вкладку **Расписание**.

13. Настройте расписание запуска задачи.

    > **Примечание.** Убедитесь, что компьютер включен для выполнения задачи.

14. Нажмите на кнопку **Сохранить**.

15. Чтобы запустить задачу немедленно, независимо от настроенного расписания, выполните следующие действия:

    a. Установите флажок напротив задачи.

16. Нажмите на кнопку **Выполнить**.

В результате Kaspersky Endpoint Security переместит файл в карантин.

Задача *Поместить файл на карантин* может завершиться со статусом *Доступ запрещен*, если вы пытаетесь поместить запущенный исполняемый файл на карантин. Создайте задачу завершения процесса для этого файла, а затем повторите попытку.

Задача *Помещение файла на карантин* может быть завершена с ошибкой *Недостаточно места в хранилище карантина*, если вы пытаетесь поместить на карантин большой файл. Освободите место на диске и попробуйте еще раз.

Получение файла

Вы можете получать файлы с компьютеров пользователей. Например, вы можете настроить получение файла журнала событий, который создает стороннее приложение. Для получения файла вам нужно создать специальную задачу. В результате выполнения задачи файл будет сохранен в Резервном хранилище. Вы можете загрузить этот файл на компьютер из Резервного хранилища в Web Console. При этом на компьютере пользователя файл остается в исходной папке.

Важно! Размер файла не должен превышать 100 МБ. Емкость Резервного хранилища ограничена свободным дисковым пространством.

Чтобы создать задачу Получение файла, выполните следующие действия:

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

   Откроется список задач.

2. Нажмите на кнопку **Добавить**.

   Запустится **мастер создания задачи**.

3. Настройте параметры задачи:

   a. В раскрывающемся списке **Программа** выберите Kaspersky Endpoint Security для Mac (12.2).

   b. В раскрывающемся списке **Тип задачи** выберите **Получить файл**.

   c. В поле **Название задачи** введите короткое описание задачи.

   d. Выберите один из следующих вариантов:

   - Назначить задачу группе администрирования

     Задача назначается устройствам, входящим в ранее созданную группу администрирования. Можно указать одну из существующих групп или создать новую группу.

     Например, вы можете использовать этот параметр, чтобы запустить задачу отправки сообщения пользователям, если сообщение предназначено для устройств из определенной группы администрирования.

Если задача назначена группе администрирования, вкладка **Безопасность** не отображается в окне свойств задачи, поскольку групповые задачи подчиняются параметрам безопасности групп, к которым они относятся.

- **Задать адреса устройств вручную или импортировать из списка**

  Вы можете задавать NetBIOS-имена, DNS-имена, IP-адреса, а также диапазоны IP-адресов устройств, которым нужно назначить задачу.

  Вы можете использовать этот параметр для выполнения задачи для заданной подсети. Например, вы можете установить определенное приложение на устройства бухгалтеров или проверять устройства в подсети, которое, вероятно, заражено.

- **Назначить задачу выборке устройств**

  Задача назначается устройствам, входящим в выборку устройств. Можно указать одну из существующих выборок.

  Например, вы можете использовать этот параметр, чтобы запустить задачу на устройствах с определенной версией операционной системы.

4. Выберите устройства в соответствии с выбранным вариантом области действия задачи. В окне **Получение файла** нажмите на кнопку **Добавить**.

   Откроется окно **Получение файла**.

5. В раскрывающемся списке **Укажите файл, который требуется получить**, выберите один из вариантов и заполните необходимые поля.

   Для добавления файла вам нужно ввести полный путь к файлу или хеш файла и путь к файлу.

6. Нажмите **ОК**.

   Настройки добавляемого файла отобразятся в списке файлов.

7. Нажмите **Далее**.

8. Выберите учетную запись пользователя, права которого требуется использовать для запуска задачи. Нажмите **Далее**.

Примечание. По умолчанию Kaspersky Endpoint Security запускает задачу под системной учетной записью (root).

9. На шаге **Завершение создания задачи** нажмите на кнопку **Готово**, чтобы создать задачу и закрыть мастер.

   Если включен параметр **Открыть окно свойств задачи после ее создания**, откроется окно параметров задачи. В этом окне можно проверить параметры задачи, изменить их или при необходимости настроить расписание запуска задачи.

10. Нажмите на новую задачу.

    Откроется окно свойств задачи.

11. Выберите вкладку **Расписание**.

12. Настройте расписание запуска задачи.

    > **Примечание.** Убедитесь, что компьютер включен для выполнения задачи.

13. Нажмите на кнопку **Сохранить**.

14. Чтобы запустить задачу немедленно, независимо от настроенного расписания, выполните следующие действия:

    a. Установите флажок напротив задачи.

15. Нажмите на кнопку **Выполнить**.

    В результате Kaspersky Endpoint Security создает копию файла и помещает ее в Резервное хранилище. Вы можете скачать файл из Резервного хранилища в Web Console.

Удаление файла

Развернуть всё | Свернуть всё

Вы можете удалять файлы удаленно с помощью задачи *Удаление файла*. Например, вы можете удалить файл удаленно при реагировании на угрозы.

Чтобы создать задачу Удаления файла, выполните следующие действия:

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

   Откроется список задач.

2. Нажмите на кнопку **Добавить**.

   Запустится **мастер создания задачи**.

3. Настройте параметры задачи:

a. В раскрывающемся списке **Программа** выберите Kaspersky Endpoint Security для Mac (12.2).

b. В раскрывающемся списке **Тип задачи** выберите **Удаление файла**.

c. В поле **Название задачи** введите короткое описание задачи.

d. Выберите один из следующих вариантов:

- Назначить задачу группе администрирования

  Задача назначается устройствам, входящим в ранее созданную группу администрирования. Можно указать одну из существующих групп или создать новую группу.

  Например, вы можете использовать этот параметр, чтобы запустить задачу отправки сообщения пользователям, если сообщение предназначено для устройств из определенной группы администрирования.

  Если задача назначена группе администрирования, вкладка **Безопасность** не отображается в окне свойств задачи, поскольку групповые задачи подчиняются параметрам безопасности групп, к которым они относятся.

- Задать адреса устройств вручную или импортировать из списка

  Вы можете задавать NetBIOS-имена, DNS-имена, IP-адреса, а также диапазоны IP-адресов устройств, которым нужно назначить задачу.

  Вы можете использовать этот параметр для выполнения задачи для заданной подсети. Например, вы можете установить определенное приложение на устройства бухгалтеров или проверять устройства в подсети, которое, вероятно, заражено.

- Назначить задачу выборке устройств

  Задача назначается устройствам, входящим в выборку устройств. Можно указать одну из существующих выборок.

  Например, вы можете использовать этот параметр, чтобы запустить задачу на устройствах с определенной версией операционной системы.

4. Выберите устройства в соответствии с выбранным вариантом области действия задачи.

5. В раскрывающемся списке **Укажите файл, который требуется удалить**, выберите один из вариантов и заполните необходимые поля. Для добавления файла вам нужно ввести полный

путь к файлу или хеш файла и путь к файлу.

6. Если вы хотите, чтобы задача была применима к критическим объектам системы, установите флажок **Применить к критическим объектам системы**.

7. Выберите учетную запись пользователя, права которого требуется использовать для запуска задачи. Нажмите **Далее**.

   Примечание. По умолчанию Kaspersky Endpoint Security запускает задачу под системной учетной записью (root).

8. На шаге **Завершение создания задачи** нажмите на кнопку **Готово**, чтобы создать задачу и закрыть мастер.

   Если включен параметр **Открыть окно свойств задачи после ее создания**, откроется окно параметров задачи. В этом окне можно проверить параметры задачи, изменить их или при необходимости настроить расписание запуска задачи.

9. Нажмите на новую задачу.

   Откроется окно свойств задачи.

10. Выберите вкладку **Расписание**.

11. Настройте расписание запуска задачи.

    Примечание. Убедитесь, что компьютер включен для выполнения задачи.

12. Нажмите на кнопку **Сохранить**.

13. Чтобы запустить задачу немедленно, независимо от настроенного расписания, выполните следующие действия:

    a. Установите флажок напротив задачи.

14. Нажмите на кнопку **Запустить**.

В результате Kaspersky Endpoint Security удалит файл с компьютера. Если файл заблокирован другим процессом, то задача будет отображаться со статусом *Выполнено*, но сам файл будет удален только после перезагрузки компьютера. После перезагрузки компьютера убедитесь, что файл удален.

Задача *Удаление файла* может быть завершена с ошибкой *Доступ запрещен*, если вы пытаетесь удалить запущенный исполняемый файл. Создайте задачу завершения процесса для этого файла, а затем повторите попытку.

Запуск процесса

Развернуть всё | Свернуть всё

Вы можете удаленно запускать файлы с помощью задачи *Запуск процесса*.

Важно! Вы можете настроить параметры задачи для EDR Optimum в Web Console.

Чтобы создать задачу Запуск процесса, выполните следующие действия:

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

   Откроется список задач.

2. Нажмите на кнопку **Добавить**.

   Запустится **мастер создания задачи**.

3. Настройте параметры задачи:

   a. В раскрывающемся списке **Программа** выберите Kaspersky Endpoint Security для Mac (12.2).

   b. В раскрывающемся списке **Тип задачи** выберите **Запуск процесса**.

   c. В поле **Название задачи** введите короткое описание задачи.

   d. Выберите один из следующих вариантов:

   - Назначить задачу группе администрирования

     Задача назначается устройствам, входящим в ранее созданную группу администрирования. Можно указать одну из существующих групп или создать новую группу.

     Например, вы можете использовать этот параметр, чтобы запустить задачу отправки сообщения пользователям, если сообщение предназначено для устройств из определенной группы администрирования.

     Если задача назначена группе администрирования, вкладка **Безопасность** не отображается в окне свойств задачи, поскольку групповые задачи подчиняются параметрам безопасности групп, к которым они относятся.

- **Задать адреса устройств вручную или импортировать из списка**

  Вы можете задавать NetBIOS-имена, DNS-имена, IP-адреса, а также диапазоны IP-адресов устройств, которым нужно назначить задачу.

  Вы можете использовать этот параметр для выполнения задачи для заданной подсети. Например, вы можете установить определенное приложение на устройства бухгалтеров или проверять устройства в подсети, которое, вероятно, заражено.

- **Назначить задачу выборке устройств**

  Задача назначается устройствам, входящим в выборку устройств. Можно указать одну из существующих выборок.

  Например, вы можете использовать этот параметр, чтобы запустить задачу на устройствах с определенной версией операционной системы.

4. Выберите устройства в соответствии с выбранным вариантом области действия задачи.

5. На шаге **Область действия задачи** укажите группу администрирования, устройства с определенными адресами или выборку устройств.

   Доступные параметры зависят от параметра, выбранного на предыдущем шаге.

6. Настройте параметры задачи:

   a. В поле **Исполняемая команда** укажите команду, которая будет выполняться на локальном устройстве.

   b. При необходимости укажите аргументы командной строки в поле **Аргументы командной строки (необязательно)**.

   c. При необходимости укажите путь к исполняемому файлу в поле **Путь к рабочей папке (необязательно)**.

7. На шаге **Завершение создания задачи** нажмите на кнопку **Готово**, чтобы создать задачу и закрыть мастер.

   Если включен параметр **Открыть окно свойств задачи после ее создания**, откроется окно параметров задачи. В этом окне можно проверить параметры задачи, изменить их или при необходимости настроить расписание запуска задачи.

8. Нажмите на новую задачу.

   Откроется окно свойств задачи.

9. Выберите вкладку **Расписание**.
10. Настройте расписание запуска задачи.

> **Примечание.** Убедитесь, что компьютер включен для выполнения задачи.

11. Нажмите на кнопку **Сохранить**.
12. Чтобы запустить задачу немедленно, независимо от настроенного расписания, выполните следующие действия:

    a. Установите флажок напротив задачи.
13. Нажмите на кнопку **Выполнить**.

    В результате Kaspersky Endpoint Security выполнит команду в тихом режиме и запустит процесс. Вы можете просмотреть результаты выполнения задачи в свойствах задачи в разделе **Результаты выполнения**.

Завершение процесса

Развернуть всё | Свернуть всё

Вы можете удаленно завершать процессы с помощью задачи *Завершение процесса*. Например, вы можете удаленно завершить работу утилиты проверки скорости интернета, которая была запущена с помощью задачи Запуск процесса.

Если вы хотите запретить запуск файла, вы можете настроить компонент Запрет запуска. Вы можете запретить запуск исполняемых файлов, скриптов, файлов офисного формата.

Задача *Завершение процесса* имеет следующие ограничения:

- Вы можете настроить параметры задачи только для EDR Optimum в Web Console.

Чтобы создать задачу Завершение процесса, выполните следующие действия:

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

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

   Запустится **мастер создания задачи**.
3. Настройте параметры задачи:

a. В раскрывающемся списке **Программа** выберите Kaspersky Endpoint Security для Mac (12.2).

b. В раскрывающемся списке **Тип задачи** выберите **Завершение процесса**.

c. В поле **Название задачи** введите короткое описание задачи.

d. Выберите один из следующих вариантов:

- Назначить задачу группе администрирования

  Задача назначается устройствам, входящим в ранее созданную группу администрирования. Можно указать одну из существующих групп или создать новую группу.

  Например, вы можете использовать этот параметр, чтобы запустить задачу отправки сообщения пользователям, если сообщение предназначено для устройств из определенной группы администрирования.

  Если задача назначена группе администрирования, вкладка **Безопасность** не отображается в окне свойств задачи, поскольку групповые задачи подчиняются параметрам безопасности групп, к которым они относятся.

- Задать адреса устройств вручную или импортировать из списка

  Вы можете задавать NetBIOS-имена, DNS-имена, IP-адреса, а также диапазоны IP-адресов устройств, которым нужно назначить задачу.

  Вы можете использовать этот параметр для выполнения задачи для заданной подсети. Например, вы можете установить определенное приложение на устройства бухгалтеров или проверять устройства в подсети, которое, вероятно, заражено.

- Назначить задачу выборке устройств

  Задача назначается устройствам, входящим в выборку устройств. Можно указать одну из существующих выборок.

  Например, вы можете использовать этот параметр, чтобы запустить задачу на устройствах с определенной версией операционной системы.

4. Выберите устройства в соответствии с выбранным вариантом области действия задачи.

5. На шаге **Область действия задачи** укажите группу администрирования, устройства с определенными адресами или выборку устройств.

Доступные параметры зависят от параметра, выбранного на предыдущем шаге.

6. На этом шаге мастера в раскрывающемся списке **Укажите файл, процессы которого требуется завершить**, выберите один из вариантов и заполните необходимые поля. Для указания файла вам нужно ввести полный путь к файлу или хеш файла и путь к файлу.

   > **Примечание.** При создании задачи для локального устройства, вы можете указать процесс по PID.

7. Если вы хотите, чтобы задача была применима к критическим объектам системы, установите флажок **Применить к критическим объектам системы**.

8. Выберите учетную запись пользователя, права которого требуется использовать для запуска задачи. Нажмите **Далее**.

   > **Примечание.** По умолчанию Kaspersky Endpoint Security запускает задачу под системной учетной записью (root).

9. На шаге **Завершение создания задачи** нажмите на кнопку **Готово**, чтобы создать задачу и закрыть мастер.

   Если включен параметр **Открыть окно свойств задачи после ее создания**, откроется окно параметров задачи. В этом окне можно проверить параметры задачи, изменить их или при необходимости настроить расписание запуска задачи.

10. Нажмите на новую задачу.

    Откроется окно свойств задачи.

11. Выберите вкладку **Расписание**.

12. Настройте расписание запуска задачи.

    > **Примечание.** Убедитесь, что компьютер включен для выполнения задачи.

13. Нажмите на кнопку **Сохранить**.

14. Чтобы запустить задачу немедленно, независимо от настроенного расписания, выполните следующие действия:

    a. Установите флажок напротив задачи.

15. Нажмите на кнопку **Выполнить**.

    В результате Kaspersky Endpoint Security завершит процесс на компьютере. Например, если на компьютере запущено приложение *Game* и вы завершили процесс *Game*, приложение будет закрыто без сохранения данных. Вы можете просмотреть результаты выполнения задачи в свойствах задачи в разделе **Результаты**.

Запрет запуска

Запрет запуска позволяет управлять запуском исполняемых файлов и скриптов, а также открытием файлов офисного формата. Таким образом, вы можете, например, предотвратить выполнение программ, которые вы считаете небезопасными. В результате распространение угрозы может быть остановлено. Запрет запуска поддерживает определенный набор интерпретаторов скриптов.

Правило запрета запуска

Запрет запуска управляет доступом пользователей к файлам с помощью правил запрета запуска. Правило запрета запуска – это набор критериев, которые приложение учитывает при реагировании на запуск объекта, например, при блокировании запуска объекта. Приложение идентифицирует файлы по их пути или контрольной сумме с помощью алгоритмов хеширования MD5 и SHA256.

Вы можете создавать правила Запрета запуска следующими способами:

- В деталях алерта (только для EDR Optimum).

  Детали алерта – инструмент для просмотра всей собранной информации об обнаруженной угрозе. Детали алерта содержат, например, историю появления файлов на компьютере. Подробнее о работе с деталями алерта см. в справке Kaspersky Endpoint Detection and Response Optimum.

- С помощью групповой политики или локальных параметров приложения. Вам нужно ввести путь к файлу или хеш файла (SHA256 или MD5), или путь к файлу и хеш файла.

Вы также можете управлять Запретом запуска локально из командной строки.

Примечание. Невозможно запретить запуск критически важных системных объектов (англ. System Critical Object, SCO). К SCO относятся файлы, необходимые для работы операционной системы и приложения Kaspersky Endpoint Security для Mac.

Режимы применения правил запрета запуска

Компонент Запрет запуска может работать в двух режимах:

- **Только статистика.**

  В этом режиме Kaspersky Endpoint Security публикует в журнал событий Kaspersky Security Center и в единую систему логирования событие о попытках запуска исполняемых объектов или открытия документов, соответствующих критериям правил запрета, но не блокирует их запуск или открытие. Этот режим выбран по умолчанию.

- **Активный.**

  В этом режиме приложение блокирует запуск объектов или открытие документов, соответствующих критериям правил запрета. Также приложение публикует в журнал событий Kaspersky Security Center и в единую систему логирования событие о попытках запуска объектов или открытия документов.

Управление Запретом запуска

Важно! Вы можете настроить параметры компонента только в Web Console.

Чтобы запретить запуск объектов, выполните следующие действия:

1. В главном окне Web Console выберите **Устройства** → **Политики и профили политик**.
2. Нажмите на название политики Kaspersky Endpoint Security для Mac.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры программы**.
4. Перейдите в раздел **Detection and Response** → **Endpoint Detection and Response**.
5. Включите переключатель **Запрет запуска**.
6. В блоке **Действие при запуске или открытии объекта** выберите режим работы компонента:

   - **Блокировать и записывать в отчет**. В этом режиме приложение блокирует запуск объектов или открытие документов, соответствующих критериям правил запрета. Также приложение публикует в журнал событий Kaspersky Security Center и в единую систему логирования событие о попытках запуска объектов или открытия документов.

   - **Только записывать в отчет**. В этом режиме Kaspersky Endpoint Security публикует в журнал событий Kaspersky Security Center и в единую систему логирования событие о попытках запуска исполняемых объектов или открытия документов, соответствующих

критериям правил запрета, но не блокирует их запуск или открытие. Этот режим выбран по умолчанию.

7. Сформируйте список правил запрета запуска:

   a. Нажмите на кнопку **Добавить**.

   b. В открывшемся окне введите имя правила запрета запуска (например, Приложение "A").

   c. В раскрывающемся списке **Тип** выберите объект, который вы хотите заблокировать: **Приложение**, **Скрипт**, **Документ**.

   Если вы выберите неверный тип объекта, Kaspersky Endpoint Security не заблокирует файл или скрипт.

   d. Для добавления файла вам нужно ввести хеш файла (SHA256 или MD5) или полный путь к файлу, или хеш файла и путь к файлу.

> **Примечание.** Если файл находится на сетевом диске, введите путь к файлу следующим образом: /Volumes/shared_folder_name/filename. Если путь к файлу содержит букву сетевого диска, Kaspersky Endpoint Security не заблокирует файл или скрипт.

   a. Нажмите **OK**.

8. Сохраните внесенные изменения.

В результате Kaspersky Endpoint Security будет блокировать запуск объектов: запуск исполняемых файлов, скриптов и открытие файлов офисного формата. При этом вы можете, например, открыть файл скрипта в текстовом редакторе, даже если запуск скрипта запрещен. При блокировании запуска объекта Kaspersky Endpoint Security покажет пользователю стандартное уведомление приложения, если уведомления включены в настройках приложения.

Сетевая изоляция компьютера

Развернуть всё | Свернуть всё

Сетевая изоляция позволяет автоматически изолировать компьютеры от сети, в результате реагирования на обнаружение индикатора компрометации (IOC) – автоматический режим. Также вы можете включить Сетевую изоляцию вручную на время исследования обнаруженной угрозы – ручной режим.

После включения Сетевой изоляции приложение разрывает все активные и блокирует все новые сетевые соединения TCP/IP на компьютере, кроме следующих соединений:

- соединения, указанные в исключениях из Сетевой изоляции;
- соединения, инициированные службами Kaspersky Endpoint Security;
- соединения, инициированные Агентом администрирования Kaspersky Security Center.

Важно! Вы можете настроить параметры компонента только в Web Console.

Автоматический режим Сетевой изоляции

Вы можете настроить автоматическое включение Сетевой изоляции, в результате реагирования на обнаружение IOC. Для настройки автоматического режима Сетевой изоляции предназначена групповая политика.

Как настроить автоматическое включение Сетевой изоляции компьютера при обнаружении IOC

1. В главном окне Web Console выберите **Устройства** → **Задачи**.
2. Откроется список задач.
3. Нажмите на задачу Kaspersky Endpoint Security **Поиск IOC**.

   Откроется окно свойств задачи.

   Если требуется, создайте задачу Поиск IOC.
4. Выберите вкладку **Параметры программы**.
5. В блоке **Действие при обнаружении IOC** установите флажки **Предупреждать и применять действия по реагированию при обнаружении IOC** и **Изолировать компьютер от сети (на 8 часов)**.
6. Сохраните внесенные изменения.
7. В результате при обнаружении IOC приложение изолирует компьютер от сети, чтобы предотвратить распространение угрозы.

Вы можете настроить автоматическое выключение Сетевой изоляции по истечении заданного периода времени. По умолчанию приложение выключает Сетевую изоляцию через 8 часов с момента включения. Также вы можете выключить Сетевую изоляцию вручную (см. инструкцию ниже). После выключения Сетевой изоляции компьютер может работать в сети без ограничений.

Как задать период выключения Сетевой изоляции компьютера в автоматическом режиме

1. В главном окне Web Console выберите **Устройства** → **Политики и профили политик**.
2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры программы**.
4. Перейдите в раздел **Detection and Response** → **Endpoint Detection and Response**.
5. В блоке **Сетевая изоляция** нажмите **Настроить разблокировку компьютера**.
6. В открывшемся окне установите флажок **Разблокировать автоматически изолированный компьютер через** и задайте период времени, по истечении которого Сетевая изоляция должна быть выключена.
7. Сохраните внесенные изменения.

Ручной режим Сетевой изоляции

Вы можете включать или выключать Сетевую изоляцию вручную. Для настройки ручного режима Сетевой изоляции предназначены свойства компьютера в консоли Kaspersky Security Center.

Вы можете включить Сетевую изоляцию следующими способами:

- В деталях алерта (только для EDR Optimum).

  Детали алерта – инструмент для просмотра всей собранной информации об обнаруженной угрозе. Детали алерта содержат, например, историю появления файлов на компьютере. Подробнее о работе с деталями алерта см. в справке Kaspersky Endpoint Detection and Response Optimum.

- С помощью локальных параметров приложения.

Как вручную включить Сетевую изоляцию компьютера

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

   Откроются свойства компьютера.
3. Выберите вкладку **Программы**.
4. Нажмите на **Kaspersky Endpoint Security для Mac**.

   Откроются локальные параметры приложения.
5. Выберите вкладку **Параметры программы**.
6. Перейдите в раздел **Detection and Response** → **Endpoint Detection and Response**.
7. В блоке параметров **Сетевая изоляция** нажмите на кнопку **Изолировать компьютер от сети**.

Вы можете настроить автоматическое выключение Сетевой изоляции по истечении заданного периода времени. По умолчанию приложение выключает Сетевую изоляцию через 8 часов с момента включения. После выключения Сетевой изоляции компьютер может работать в сети без ограничений.

Как задать период выключения Сетевой изоляции компьютера в ручном режиме

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

   Откроются свойства компьютера.
3. Выберите вкладку **Задачи**.

   Откроется список задач, доступных на компьютере.
4. Выберите задачу **Сетевая изоляция**.
5. Выберите вкладку **Параметры программы**.
6. В открывшемся окне задайте период времени, по истечении которого Сетевая изоляция должна быть выключена.

7. Сохраните внесенные изменения.

Как вручную выключить Сетевую изоляцию компьютера

1. В главном окне Web Console выберите **Устройства** → **Управляемые устройства**.
2. Нажмите на имя компьютера, на котором вы хотите настроить локальные параметры приложения.
3. Откроются свойства компьютера.
4. Выберите вкладку **Программы**.
5. Нажмите на Kaspersky Endpoint Security для Mac.
6. Откроются локальные параметры приложения.
7. Выберите вкладку **Параметры программы**.
8. Перейдите в раздел **Detection and Response** → **Endpoint Detection and Response**.
9. В блоке параметров **Сетевая изоляция** нажмите на кнопку **Разблокировать изолированный от сети компьютер**.

Вы также можете выключить Сетевую изоляцию локально с помощью командной строки.

Исключения из Сетевой изоляции

Вы можете задать исключения из Сетевой изоляции. Сетевые соединения, подпадающие под заданные правила, не будут заблокированы на компьютере после включения Сетевой изоляции.

Для настройки исключений из Сетевой изоляции в приложении доступен список стандартных сетевых профилей. По умолчанию в исключения входят сетевые профили, состоящие из правил, обеспечивающих бесперебойную работу устройств с ролями DNS/DHCP-сервер и DNS/DHCP-клиент. Также вы можете изменить параметры стандартных сетевых профилей или задать исключения вручную (см. инструкцию ниже).

Важно! Исключения, заданные в свойствах политики, применяются, только если Сетевая изоляция включена приложением автоматически, в результате реагирования на обнаружение угрозы. Исключения, заданные в свойствах компьютера, применяются, только если Сетевая изоляция включена вручную в свойствах компьютера в консоли Kaspersky Security Center.

Примечание. Активная политика не блокирует применение исключений из Сетевой изоляции, заданных в свойствах компьютера, так как сценарии применения этих параметров разные.

Как добавить исключение из Сетевой изоляции в автоматическом режиме

1. В главном окне Web Console выберите **Устройства** → **Политики и профили политик**.
2. Нажмите на название политики Kaspersky Endpoint Security.
3. Откроется окно свойств политики.
4. Выберите вкладку **Параметры программы**.
5. Перейдите в раздел **Detection and Response** → **Endpoint Detection and Response**.
6. В блоке **Исключения из сетевой изоляции** нажмите **Исключения**.
7. В открывшемся окне нажмите на кнопку **Добавить из профиля** и выберите стандартные сетевые профили для настройки исключений.
8. Сетевые соединения из профиля будут добавлены в список исключений из Сетевой изоляции. Вы можете просмотреть свойства сетевых соединений. При необходимости, вы можете изменить параметры сетевого соединения.
9. Если требуется, добавьте исключение из Сетевой изоляции вручную. Для этого в окне со списком исключений нажмите на кнопку **Добавить** и задайте параметры сетевого соединения вручную.
10. Сохраните внесенные изменения.

Как добавить исключение из Сетевой изоляции в ручном режиме

1. В главном окне Web Console выберите **Устройства** → **Управляемые устройства**.
2. Нажмите на имя компьютера, на котором вы хотите настроить локальные параметры приложения.
3. Откроются свойства компьютера.
4. Выберите вкладку **Задачи**.
5. Откроется список задач, доступных на компьютере.
6. Выберите задачу **Сетевая изоляция**.
7. Выберите вкладку **Параметры программы**.
8. В открывшемся окне нажмите **Исключения**.
9. В открывшемся окне нажмите на кнопку **Добавить из профиля** и выберите стандартные сетевые профили для настройки исключений.
10. Сетевые соединения из профиля будут добавлены в список исключений из Сетевой изоляции. Вы можете просмотреть свойства сетевых соединений. При необходимости, вы можете изменить параметры сетевого соединения.
11. Если требуется, добавьте исключение из Сетевой изоляции вручную. Для этого в окне со списком исключений нажмите на кнопку **Добавить** и задайте параметры сетевого соединения вручную.
12. Сохраните внесенные изменения.

Вы также можете просмотреть список исключений из Сетевой изоляции локально из командной строки. При этом компьютер должен быть изолирован.

Cloud Sandbox

Cloud Sandbox – технология, которая позволяет обнаруживать сложные угрозы на компьютере. Kaspersky Endpoint Security автоматически отправляет обнаруженные файлы в Cloud Sandbox для анализа. Cloud Sandbox запускает эти файлы в изолированной среде для выявления вредоносной активности и принимает решение о репутации этих файлов. Далее данные об этих файлах попадают в Kaspersky Security Network. Таким образом, если Cloud Sandbox обнаруживает вредоносный файл, Kaspersky Endpoint Security выполнит действие для устранения угрозы на всех компьютерах, на которых обнаружит этот файл.

Важно! Для работы Cloud Sandbox необходимо включить использование Kaspersky Security Network.

Примечание. Если вы используете Kaspersky Private Security Network, технология Cloud Sandbox недоступна.

Чтобы включить Cloud Sandbox:

1. В главном окне Web Console выберите **Устройства** > **Политики и профили политик**.
2. Нажмите на название политики Kaspersky Endpoint Security для Mac.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры программы**.
4. Перейдите в раздел **Detection and Response** → **Endpoint Detection and Response**.
5. Включите переключатель **Cloud Sandbox**.
6. Сохраните внесенные изменения.

При обнаружении угрозы Kaspersky Endpoint Security активирует счетчик угроз, обнаруженных с помощью Cloud Sandbox, в главном окне приложения в разделе **Обнаружение угроз**. Kaspersky Endpoint Security также будет указывать технологию обнаружения угроз Cloud Sandbox в Отчете об угрозах в консоли Kaspersky Security Center.

Шифрование дисков с помощью FileVault

Примечание. Функция Шифрование дисков с помощью FileVault доступна в Kaspersky Security Center 10 SP3 и более поздних версиях. За дополнительной информацией обратитесь в Службу технической поддержки "Лаборатории Касперского".

Kaspersky Endpoint Security позволяет удаленно управлять шифрованием диска FileVault. Шифрование загрузочного диска на компьютере пользователя предотвращает доступ других пользователей к важной информации, которая хранится на диске.

Когда администратор запускает шифрование диска FileVault из Kaspersky Security Center, Kaspersky Endpoint Security запрашивает у пользователя компьютера его учетные данные. Шифрование диска запускается только после того, как пользователь предоставит учетные данные, перезагрузит компьютер и по прошествии 30 минут с момента получения параметров политики на компьютер. Минимальный интервал между запросами учетных данных также составляет 30 минут.

Чтобы пользователь не мог расшифровать загрузочный диск своего Mac при включенном шифровании FileVault, администратору необходимо с помощью JAMF развернуть MDM-профиль, запрещающий расшифровку диска. Чтобы расшифровать загрузочный диск компьютера Mac с MDM-профилем, запрещающим расшифровку диска, администратору сначала необходимо удалить профиль.

Примечание. Если управление шифрованием диска FileVault не включено в Kaspersky Security Center, пользователи с правами администратора могут зашифровать и расшифровать загрузочный диск Mac из Системных настроек. Вы можете найти дополнительную информацию о FileVault в документации Apple.

Если на компьютере пользователя создано несколько учетных записей, шифрование диска FileVault сделает недоступной информацию на диске для всех пользователей компьютера, кроме пользователя, который вел свои учетные данные.

Разрешение на разблокировку диска для других пользователей компьютера

1. Выберите **меню Apple** > **Системные настройки** > **Конфиденциальность и безопасность**.
2. Нажмите на кнопку **FileVault**.

   Откроется окно **FileVault**.
3. Нажмите на кнопку **Вкл. пользователей**.
4. В открывшемся окне выберите пользователя, которому вы хотите разрешить разблокировку компьютера.
5. Введите пароль учетной записи компьютера пользователя и нажмите **OK**.
6. Нажмите на кнопку **Продолжить**.

Пользователь может получить доступ к зашифрованному диску.

Примечание. Чтобы разрешить другим пользователям разблокировать диск, нужны права администратора компьютера.

Если системный администратор управляет Kaspersky Endpoint Security через Консоль администрирования Kaspersky Security Center, Kaspersky Security Center Web Console или Cloud Console и пользователь компьютера забыл или потерял учетные данные и не может получить доступ к зашифрованному диску, администратор может получить ключ восстановления.

Как получить ключ восстановления с помощью Консоли администрирования Kaspersky Security Center

Как получить ключ восстановления с помощью Kaspersky Security Center Web Console и Cloud Console

Защита паролем

Kaspersky Endpoint Security позволяет ограничить нежелательные действия на устройствах пользователей, установив пароль администратора.

Если защита паролем включена, Kaspersky Endpoint Security запрашивает пароль при попытке выполнения любых следующих действий:

- Настройке параметров приложения;
- Выходе из приложения;
- Удалении лицензионного ключа;
- Удалении приложения;

  Примечание. Защита паролем ограничивает удаление Kaspersky Endpoint Security только при использовании программы удаления.

- Восстановлении файлов, помещенных на карантин, из Резервного хранилища;
- Просмотре отчетов.

Отключение Защиты паролем не приводит к отключению параметров политики. Если изменение параметра запрещено в политике, его нельзя изменить, даже если Защита паролем отключена.

Включение Защиты паролем с помощью Консоли администрирования

1. Запустите Консоль администрирования.
2. Разверните узел **Сервер администрирования <Имя сервера>**.
3. В дереве консоли выберите папку **Управляемые устройства**.
4. В рабочей области выберите вкладку **Политики**.
5. По правой клавише мыши откройте контекстное меню политики, параметры которой вы хотите настроить, и выберите **Свойства**.
6. В окне **Свойства** выберите **Дополнительные параметры > Взаимодействие с пользователем**.
7. В разделе **Защита паролем** установите флажок **Включить Защиту паролем**.
8. В открывшемся окне **Параметры Защиты паролем** настройте следующие параметры:
   - Введите пароль в поле **Пароль** и введите его повторно в поле **Подтвердите пароль**.
   - В разделе **Требовать пароль, чтобы** установите флажки для защиты соответствующих действий на устройстве пользователя.
9. Нажмите **ОК**, чтобы сохранить изменения.
10. Чтобы применить изменения к политике, выполните одно из следующих действий:
    - Нажмите на кнопку **Применить**, чтобы остаться в окне **Свойства: <Название политики>** после сохранения внесенных изменений.
    - Нажмите на кнопку **ОК**, чтобы закрыть окно **Свойства: <Название политики>** после сохранения внесенных изменений.

Настройка параметров Защиты паролем с помощью Консоли администрирования

1. Запустите Консоль администрирования.
2. Разверните узел **Сервер администрирования <Имя сервера>**.

3. В дереве консоли выберите папку **Управляемые устройства**.

4. В рабочей области выберите вкладку **Политики**.

5. По правой клавише мыши откройте контекстное меню политики, параметры которой вы хотите настроить, и выберите **Свойства**.

6. В окне **Свойства** выберите **Дополнительные параметры > Взаимодействие с пользователем**.

7. В разделе **Защита паролем** нажмите на кнопку **Параметры**.

8. В открывшемся окне **Параметры Защиты паролем** отредактируйте параметры, которые вы хотите изменить.

9. Нажмите **OK**, чтобы сохранить изменения.

Включение Защиты паролем с помощью Web Console

1. В главном окне Web Console выберите **Устройства** > **Политики и профили политик**.

2. Нажмите на название политики Kaspersky Endpoint Security для Mac.

3. Откроется окно свойств политики.

4. Выберите вкладку **Параметры программы**.

5. Выберите **Дополнительные параметры** → **Взаимодействие с пользователем**.

6. Включите переключатель **Защита паролем**.

7. В открывшемся окне **Параметры Защиты паролем** настройте следующие параметры:

   - Введите пароль в поле **Пароль** и введите его повторно в поле **Подтвердите пароль**. По умолчанию символы пароля скрыты в целях безопасности. Чтобы увидеть введенный пароль, нажмите на кнопку **Показать**.

   - В разделе **Требовать пароль, чтобы** установите флажки для защиты соответствующих действий на устройстве пользователя.

8. Нажмите кнопку **OK**, чтобы закрыть окно **Параметры Защиты паролем**.

9. Нажмите кнопку **OK**, чтобы закрыть раздел **Взаимодействие с пользователем**.

10. Нажмите кнопку **Сохранить**, чтобы сохранить изменения в политике.

Изменение защиты паролем с помощью Web Console

1. В главном окне Web Console выберите **Устройства** > **Политики и профили политик**.
2. Нажмите на название политики Kaspersky Endpoint Security для Mac.
3. Откроется окно свойств политики.
4. Выберите вкладку **Параметры программы**.
5. Выберите **Дополнительные параметры** → **Взаимодействие с пользователем**.
6. В разделе **Защита паролем** нажмите на кнопку **Параметры**.
7. В открывшемся окне **Параметры Защиты паролем** настройте параметры, которые вы хотите изменить.
8. Нажмите кнопку **ОК**, чтобы закрыть окно **Параметры Защиты паролем**.
9. Нажмите кнопку **ОК**, чтобы закрыть раздел **Взаимодействие с пользователем**.
10. Нажмите кнопку **Сохранить**, чтобы сохранить изменения в политике.

Включение Защиты паролем с помощью приложения Kaspersky Endpoint Security

1. В строке меню нажмите на значок приложения и выберите пункт **Настройки**.

   Откроется окно настройки приложения.
2. На вкладке **Интерфейс** в блоке **Защита паролем** установите флажок **Включить Защиту паролем**.
3. В открывшемся окне настройте следующие параметры:

   - Введите пароль в поле **Пароль** и введите его повторно в поле **Подтвердите пароль**.
   - В разделе **Требовать пароль, чтобы** установите флажки для защиты соответствующих действий на устройстве пользователя.

4. Нажмите **OK**.

> **Примечание.** Если в качестве действия, защищенного паролем, вы выбрали **Изменить параметры приложения**, вам потребуется ввести пароль дважды, чтобы изменить настройки Защиты паролем.

Изменение параметров Защиты паролем с помощью приложения Kaspersky Endpoint Security

1. В строке меню нажмите на значок приложения и выберите пункт **Настройки**.

   Откроется окно настройки приложения.

2. На вкладке **Интерфейс** в разделе **Защита паролем** нажмите **Настройки**.

3. В открывшемся окне отредактируйте параметры, которые вы хотите изменить.

4. Нажмите **OK**.

Анализ поведения

Компонент Анализ поведения получает данные о действиях приложений на вашем компьютере и предоставляет эту информацию другим компонентам защиты для повышения эффективности их работы. Компонент Анализ поведения использует шаблоны опасного поведения приложений (BSS). Если активность приложения совпадает с одним из шаблонов опасного поведения, Kaspersky Endpoint Security выполняет выбранное ответное действие. Функциональность Kaspersky Endpoint Security, основанная на шаблонах опасного поведения, обеспечивает проактивную защиту компьютера.

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

Включение/выключение Анализа поведения с помощью Web Console

1. В главном окне Web Console выберите **Активы (Устройства)** → **Политики и профили политик**.

2. Нажмите на название политики Kaspersky Endpoint Security.

Откроется окно свойств политики.

3. Выберите вкладку **Параметры программы**.

4. Перейдите в раздел **Продвинутая защита** > **Анализ поведения**.

5. Включите/выключите переключатель **Behavior Detection**.

6. Если Анализ поведения включен, выберите одно из следующих действий, которые будут выполняться при обнаружении активности вредоносного ПО:

   - **Блокировать**

     Если выбран этот вариант, приложение Kaspersky Endpoint Security завершает работу приложения при обнаружении вредоносной активности.

   - **Удалять**

     Если выбран этот вариант, при обнаружении вредоносной активности приложение Kaspersky Endpoint Security удаляет исполняемый файл вредоносного приложения и создает резервную копию файла в Резервном хранилище.

   - **Запрашивать действие**

     Если выбран этот вариант, при обнаружении вредоносной активности приложение Kaspersky Endpoint Security отображает окно уведомления с информацией о вредоносном объекте и предлагает пользователю выбрать действие, которое выполнит приложение Kaspersky Endpoint Security. В зависимости от статуса объекта действия могут отличаться.

7. Если Анализ поведения и Защита папок общего доступа от внешнего шифрования включены, выберите одно из следующих действий, которое будут выполняться при обнаружении внешнего шифрования:

   - **Информировать**

     Если выбран этот вариант, при обнаружении попытки изменить файлы в папках общего доступа, приложение Kaspersky Endpoint Security добавляет информацию об этой попытке в список активных угроз, вносит запись в отчеты локального приложения и отправляет информацию о выявленной вредоносной активности в Kaspersky Security Center.

- **Блокировать атакующее устройство на**

  Если выбран этот вариант, при обнаружении попытки изменить файлы в папках общего доступа, приложение Kaspersky Endpoint Security блокирует доступ к изменению файлов (только для чтения) для сеанса, инициировавшего вредоносную активность, и создает резервные копии измененных файлов.

8. Сохраните внесенные изменения.

Включение/выключение Анализа поведения с помощью Консоли администрирования

1. Запустите Консоль администрирования.
2. Разверните узел **Сервер администрирования <Имя сервера>**.
3. В дереве консоли выберите папку **Управляемые устройства**.
4. В рабочей области выберите вкладку **Политики**.
5. По правой клавише мыши откройте контекстное меню политики, параметры которой вы хотите настроить, и выберите **Свойства**.
6. В окне **Свойства** выберите **Продвинутая защита** > **Анализ поведения**.
7. Установите или снимите флажок **Анализ поведения**.
8. При необходимости в разделе **Действие при обнаружении вредоносной активности** выберите действие, которое будет выполнено при обнаружении активности вредоносных программ.
9. Нажмите **OK**, чтобы сохранить изменения.
10. Чтобы применить изменения к политике, выполните одно из следующих действий:

    - Нажмите на кнопку **Применить**, чтобы остаться в окне **Свойства: <Название политики>** после сохранения внесенных изменений.
    - Нажмите на кнопку **OK**, чтобы закрыть окно **Свойства: <Название политики>** после сохранения внесенных изменений.

Включение/выключение Анализа поведения с помощью приложения Kaspersky Endpoint Security

1. В строке меню нажмите на значок приложения и выберите пункт **Настройки**.

   Откроется окно настройки приложения.

2. На вкладке **Дополнительно** в разделе **Анализ поведения** установите или снимите флажок **Включить Анализ поведения**.

3. Если флажок **Включить Анализ поведения** установлен, выберите одно из следующих действий, которое будет выполняться при обнаружении активности вредоносного ПО:

   - **Блокировать**

     Если выбран этот вариант, приложение Kaspersky Endpoint Security завершает работу приложения при обнаружении вредоносной активности.

   - **Удалять**

     Если выбран этот вариант, при обнаружении вредоносной активности приложение Kaspersky Endpoint Security удаляет исполняемый файл вредоносного приложения и создает резервную копию файла в Резервном хранилище.

   - **Запрашивать действие**

     Если выбран этот вариант, при обнаружении вредоносной активности приложение Kaspersky Endpoint Security отображает окно уведомления с информацией о вредоносном объекте и предлагает пользователю выбрать действие, которое выполнит приложение Kaspersky Endpoint Security. В зависимости от статуса объекта действия могут отличаться.

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

Важно! Мы не рекомендуем отключать Анализ поведения без крайней необходимости, так как это снизит эффективность компонентов защиты. Для обнаружения угроз компоненты защиты могут запрашивать данные, собранные компонентом Анализ поведения.

Защита от эксплойтов

Компонент Защита от эксплойтов отслеживает программный код, который использует уязвимости на компьютере для получения эксплойтом прав администратора или выполнения вредоносных действий. Эксплойты, например, используют атаку на переполнение буфера обмена. Для этого эксплойт отправляет большой объем данных в уязвимое приложение. При обработке этих данных уязвимое приложение выполняет вредоносный код. В результате этой атаки эксплойт может запустить несанкционированную установку вредоносного ПО. Если попытка запустить исполняемый файл из уязвимого приложения не была произведена пользователем, то Kaspersky Endpoint Security блокирует запуск этого файла или информирует пользователя.

По умолчанию Защита от эксплойтов включена. При необходимости вы можете отключить Защиту от эксплойтов.

Включение/выключение Защиты от эксплойтов с помощью Web Console

1. В главном окне Web Console выберите **Активы (Устройства)** → **Политики и профили политик**.
2. Нажмите на название политики Kaspersky Endpoint Security.

   Откроется окно свойств политики.
3. Выберите вкладку **Параметры программы**.
4. Перейдите в раздел **Продвинутая защита** > **Защита от эксплойтов**.
5. Включите/выключите переключатель **Защита от эксплойтов**.
6. Если Защита от эксплойтов включена, выберите одно из следующих действий, которые будут выполняться при обнаружении эксплойта:

   - Блокировать

Если этот пункт выбран, при обнаружении эксплойта Kaspersky Endpoint Security блокирует его действия и добавляет запись с информацией об этом эксплойте в журнал.

- Информировать

  Если этот пункт выбран, при обнаружении эксплойта Kaspersky Endpoint Security записывает информацию о нем в журнал и добавляет сведения об этом эксплойте в список активных угроз.

7. Сохраните внесенные изменения.

Включение/выключение Защиты от эксплойтов с помощью Консоли администрирования

1. Запустите Консоль администрирования.
2. Разверните узел **Сервер администрирования <Имя сервера>**.
3. В дереве консоли выберите папку **Управляемые устройства**.
4. В рабочей области выберите вкладку **Политики**.
5. По правой клавише мыши откройте контекстное меню политики, параметры которой вы хотите настроить, и выберите **Свойства**.
6. В окне **Свойства** выберите **Продвинутая защита** > **Защита от эксплойтов**.
7. Установите или снимите флажок **Защита от эксплойтов**.
8. При необходимости в блоке **При обнаружении эксплойта** выберите действие, которое будет выполняться при обнаружении эксплойта Kaspersky Endpoint Security.
9. Нажмите **ОК**, чтобы сохранить изменения.
10. Чтобы применить изменения к политике, выполните одно из следующих действий:

    - Нажмите на кнопку **Применить**, чтобы остаться в окне **Свойства: <Название политики>** после сохранения внесенных изменений.
    - Нажмите на кнопку **ОК**, чтобы закрыть окно **Свойства: <Название политики>** после сохранения внесенных изменений.

Включение/выключение Защиты от эксплойтов с помощью приложения Kaspersky Endpoint Security

1. В строке меню нажмите на значок приложения и выберите пункт **Настройки**.

   Откроется окно настройки приложения.

2. На вкладке **Дополнительно** в разделе Защита от эксплойтов установите или снимите флажок **Включить Защиту от эксплойтов**.

3. Если флажок **Включить Анализ поведения** установлен, выберите одно из следующих действий, которые будут выполняться при обнаружении активности вредоносного ПО:

   - Блокировать опасную вредоносную активность автоматически

     Если этот пункт выбран, при обнаружении эксплойта Kaspersky Endpoint Security блокирует его действия и добавляет запись с информацией об этом эксплойте в журнал.

   - Информировать

     Если этот пункт выбран, при обнаружении эксплойта Kaspersky Endpoint Security записывает информацию о нем в журнал и добавляет сведения об этом эксплойте в список активных угроз.

Просмотр отчета о работе Защиты от эксплойтов

1. В строке меню выберите **Защита** > **Отчеты**.

   Откроется окно **Отчеты**.

2. Откройте вкладку **Защита от эксплойтов**.

Участие в Kaspersky Security Network

Если вы принимаете участие в Kaspersky Security Network, приложение Kaspersky Endpoint Security автоматически отправляет статистическую информацию в "Лабораторию Касперского", чтобы улучшить защиту вашего Mac.

Примечание. "Лаборатория Касперского" не осуществляет получение, обработку и хранение любых персональных данных без вашего явного согласия.

Участие в Kaspersky Security Network является добровольным. Решение об участии вы принимаете на этапе установки приложения. Вы можете изменить свое решение в любой момент.

Присоединение к Kaspersky Security Network

1. В строке меню нажмите на значок приложения и выберите пункт **Настройки**.

   Откроется окно настройки приложения.

2. На вкладке **Дополнительно** в блоке **KSN** нажмите на кнопку **Показать Положение о KSN**, чтобы ознакомиться с Положением о Kaspersky Security Network.

3. Если вы хотите, чтобы приложение Kaspersky Endpoint Security использовало информацию о репутации файлов, веб-ресурсов и программ, полученную из Kaspersky Security Network, и вы принимаете все условия Положения, установите флажок **Участвовать в Kaspersky Security Network**.

4. В открывшемся окне нажмите на кнопку **Подтвердить**.

   Будут установлены флажки **Участвовать в Kaspersky Security Network** и **Включить расширенный режим работы KSN**.

Примечание. По умолчанию Kaspersky Endpoint Security использует расширенный режим работы KSN. *Расширенный режим работы KSN* – режим работы приложения, при котором Kaspersky Endpoint Security передает в "Лабораторию Касперского" дополнительные данные. Если вы не хотите отправлять эти данные в "Лабораторию Касперского", снимите флажок **Включить расширенный режим работы KSN**.

Данные, предоставляемые в "Лабораторию Касперского" при использовании Kaspersky Security Network

Если флажок **Участвовать в Kaspersky Security Network** установлен, а флажок **Включить расширенный режим работы KSN** снят, Kaspersky Endpoint Security отправляет в "Лабораторию Касперского" следующие данные:

- Информация об используемой лицензии: тип лицензии и срок ее действия, количество дней до истечения срока действия лицензии, идентификатор партнера, у которого приобретена лицензия, идентификатор регионального центра активации, контрольная сумма кода активации, хеш-сумма тела тикета, рассчитанная по алгоритму SHA1, дата и время создания лицензионного тикета, идентификатор информации о лицензии, идентификатор лицензионного тикета, идентификатор последовательности лицензионного тикета, уникальный идентификатор компьютера пользователя, дата начала и окончания периода валидности лицензионного тикета, текущее состояние лицензионного тикета, версия заголовка тикета, версия лицензии, идентификатор сертификата подписи заголовка тикета, контрольная сумма файла ключа, серийный номер подписчика заголовка тикета, токен авторизации.

- Полная версия установленного ПО;

  тип установленного ПО; идентификатор обновления ПО; идентификатор службы репутации; идентификатор типа протокола; идентификатор регионального центра активации; версия списка отозванных заключений службы ПО; идентификатор сработавшей записи в антивирусных базах ПО; временная метка сработавшей записи в антивирусных базах ПО; тип сработавшей записи в антивирусных базах ПО; уникальный идентификатор установки ПО на компьютере; дата активации лицензии; дата окончания срока действия лицензии; идентификатор лицензии; статус лицензии, по которой используется ПО; тип контрольной суммы обрабатываемого объекта; название обнаруженной вредоносной программы или легальной программы, которая может быть использована для нанесения вреда устройству или данным пользователя; контрольная сумма обрабатываемого объекта; контрольная сумма кода активации ПО; полная версия ПО; уникальный идентификатор устройства; идентификатор ПО; контрольная сумма файла ключа, которым активировано ПО; идентификатор информационной модели, примененной при предоставлении лицензии на использование ПО; идентификатор сертификата, которым подписан заголовок лицензионного тикета ПО; дата и время создания лицензионного тикета ПО; контрольная сумма лицензионного тикета ПО; версия лицензионного тикета ПО; версия кода активации ПО; формат данных в запросе к инфраструктуре Правообладателя; идентификатор тикета текущей лицензии; идентификатор компонента ПО; результат действий, выполненных ПО; код ошибки; адрес веб-службы, на который осуществлялось обрабатываемое обращение (веб-адрес, IP); номер порта; веб-адрес источника запроса к веб-службе (referrer); публичный ключ сертификата; отпечаток цифрового сертификата проверяемого объекта и алгоритм хеширования.

Если флажки **Участвовать в Kaspersky Security Network** и **Включить расширенный режим работы KSN** установлены, Kaspersky Endpoint Security отправляет в "Лабораторию Касперского" следующие данные:

- Информация о версиях установленной на компьютере операционной системы (ОС) и установленных пакетов обновлений, версия и контрольные суммы (MD5, SHA2-256, SHA1) файла ядра ОС, параметры режима работы ОС; версия ОС, номер сборки ОС, номер обновления ОС, редакция ОС, расширенная информация о редакции ОС;

версия пакета обновления ОС; дата и время запуска ОС; время задержки обработки события о совершении действия в ОС в подсистеме поведенческого анализа; количество задержанных событий текущего типа, совершенных в ОС; время задержки обработки события о совершении действия в ОС в подсистеме проактивной защиты; количество обработанных событий, совершенных в ОС; количество обработанных синхронных событий, совершенных в ОС; суммарная задержка всех событий текущего типа, совершенных в ОС; время задержки обработки события о совершении действия в ОС в подсистеме постоянного хранения событий; суммарная задержка всех событий, совершенных в ОС; количество ожидающих синхронных событий, совершенных в ОС; дата и время получения события о совершении действия в ОС.

- Информация о последней неуспешной перезагрузке ОС: количество неуспешных перезагрузок.

- Информация об установленном ПО Правообладателя и состоянии антивирусной защиты компьютера: идентификатор установки ПО (PCID); версия записи в базе данных ПО; уникальный идентификатор установки программы на компьютере, тип программы, идентификатор типа программы, полная версия установленной программы, идентификатор версии настроек программы, идентификатор типа компьютера, уникальный идентификатор компьютера, на котором установлена программа, уникальный идентификатор пользователя в службах Правообладателя, язык локали и ее рабочее состояние, версия установленных компонентов ПО и их рабочее состояние, версия протокола, который используется для подключения к службам Правообладателя; полная версия установленного ПО; тип установленного ПО; идентификатор обновления ПО; идентификатор службы репутации; идентификатор типа протокола; идентификатор регионального центра активации; версия списка отозванных заключений службы ПО; идентификатор сработавшей записи в антивирусных базах ПО; временная метка сработавшей записи в антивирусных базах ПО; тип сработавшей записи в антивирусных базах ПО; уникальный идентификатор установки ПО на компьютере; дата активации лицензии; дата окончания срока действия лицензии; идентификатор лицензии; статус лицензии, по которой используется ПО; тип контрольной суммы обрабатываемого объекта; название обнаруженной вредоносной программы или легальной программы, которая может быть использована для нанесения вреда устройству или данным пользователя; контрольная сумма обрабатываемого объекта; контрольная сумма кода активации ПО; полная версия ПО; идентификатор ПО; контрольная сумма файла ключа, которым активировано ПО; идентификатор информационной модели, примененной при предоставлении лицензии на использование ПО; идентификатор сертификата, которым подписан заголовок лицензионного тикета ПО; дата и время создания лицензионного тикета ПО; контрольная сумма лицензионного тикета ПО; версия лицензионного тикета ПО; версия кода активации ПО; формат данных в запросе к инфраструктуре Правообладателя; идентификатор тикета текущей лицензии; идентификатор компонента ПО; результат действий, выполненных ПО; код ошибки; адрес веб-службы, на который осуществлялось обрабатываемое обращение (веб-адрес, IP); номер порта; веб-адрес источника запроса к веб-службе (referrer);

количество циклов обновления и применения антивирусных баз; дата и время последнего обновления и применения антивирусных баз; дата и время выпуска баз ПО; версия компонента ПО; идентификатор обновления ПО; тип установленного ПО; дата и время запуска компонента мониторинг активности; дата и время установки ПО; вероятность отправки статистики компонентом мониторинг активности; код события, обрабатываемого компонентом мониторинг активности дольше стандартного времени обработки; время обработки события в базах, обработка которого компонентом мониторинг активности длилась дольше стандартного времени; максимально допустимое время обработки события компонентом мониторинг активности; время обработки события, обработка которого компонентом мониторинг активности длилась дольше стандартного времени; общее количество событий, обработка которых компонентом мониторинг активности длилась дольше стандартного времени.

- Данные обо всех обрабатываемых объектах и действиях: заключение ПО по обрабатываемому объекту; код каталога файлов; размер обрабатываемого объекта; контрольная сумма (SHA256) обрабатываемого объекта; номер обнаруженного ПО в контексте компонента мониторинг активности; дата и время обнаружения стороннего ПО компонентом мониторинг активности; характеристики обнаружения; идентификатор сработавшей записи в антивирусных базах ПО; причина обнаружения стороннего ПО компонентом мониторинг активности; контрольная сумма (MD5) обрабатываемого объекта; результат проверки подписи модуля, целостность которого проверяется ПО; имя обрабатываемого объекта; тип сработавшей записи в антивирусных базах ПО; путь к обрабатываемому объекту; имя проверяемого объекта; дата и время проверки; URL-адрес и Referrer, по которому он был загружен; размер проверяемых файлов и пути к ним; признак нахождения в архиве; дата и время создания файла; имя, размер и контрольные суммы (MD5, SHA2-256) упаковщика (если файл был упакован); энтропия файла; тип файла; код типа файла; признак исполняемого файла, идентификатор исполняемого файла и формат исполняемого файла; контрольная сумма объекта (MD5, SHA2-256); тип и значение дополнительной контрольной суммы объекта; данные о ЭЦП (сертификате) объекта: данные об издателе сертификата, количество запусков объекта с момента последней отправки статистики, идентификатор задачи проверки, способ получения информации о репутации объекта, значение фильтра target, технические характеристики по применяемым технологиям обнаружения; путь к обрабатываемому объекту; код каталога файлов.

- Для исполняемых файлов: энтропия разделов файла, признак проверки репутации или подписи файла, название, тип, идентификатор типа, контрольная сумма (MD5) и размер приложения, загруженного проверяемым объектом, путь к приложению и пути к шаблонам, признак нахождения в списке автозапуска, дата записи, список атрибутов, название упаковщика, информация о цифровой подписи приложения: издатель сертификата, название отправляемого файла в формате MIME, дата и время сборки файла.

- Информация о запускаемых программах и их модулях: контрольные суммы запускаемых файлов (MD5, SHA2-256), размер, атрибуты, дата создания, имя упаковщика (если файл был упакован), имена файлов, данные о запущенных в системе процессах (идентификатор процесса в системе (PID), имя процесса, данные об учетной записи, от которой запущен процесс, приложении и команде, запустившей процесс, полный путь к файлам процесса и командная строка запуска, описание приложения, к которому относится процесс (название приложения и данные об издателе), а также данные об используемых цифровых сертификатах и информация, необходимая для проверки подлинности этих сертификатов, или данные об отсутствии цифровой подписи файла), также информация о загружаемых в процессы модулях: их имена, размер, типы, даты создания, атрибуты, контрольные суммы (MD5, SHA2-256, SHA1), пути к ним, информация заголовка PE-файлов, имена упаковщиков (если файл был упакован), информация о наличии и валидности данных этой статистики, идентификатор условия формирования передаваемой статистики.

- В случае обнаружения угрозы или уязвимости, дополнительно к информации об обнаруженном объекте предоставляется информация об идентификаторе, версии и типе записи в антивирусных базах, название угрозы согласно классификации Правообладателя, дата и время последнего обновления антивирусных баз, имя исполняемого файла, контрольная сумма (MD5) файла приложения, запросившего URL-адрес, в котором произошло обнаружение, IP-адрес (IPv4 или IPv6) обнаруженной угрозы, идентификатор уязвимости и класс ее опасности, URL-адрес и Referrer страницы обнаружения уязвимости.

- В случае обнаружения потенциально вредоносного объекта предоставляется информация о данных в памяти процессов.

- Информация о сетевой атаке: IP-адрес атакующего компьютера и номер порта компьютера пользователя, на который была направлена сетевая атака, идентификатор протокола, по которому выполнялась атака, название и тип атаки.

- Информация о сетевых соединениях: версия и контрольные суммы (MD5, SHA2-256, SHA1) файла процесса, открывшего порт, путь к файлу процесса и его цифровая подпись, локальный и удаленный IP-адреса, номера локального и удаленного портов соединения, состояние соединения, время открытия порта.

- URL и IP-адрес веб-страницы, на которой был обнаружен вредоносный или подозрительный контент, имя, размер и контрольная сумма файла, запросившего данный URL, идентификатор, вес и степень применимости правила, по которому был вынесен вердикт, цель атаки.

- Информация об обновлении установленной программы и антивирусных баз: статус завершения задачи обновления, тип ошибки, которая могла произойти при обновлении, число неуспешных завершений обновления, идентификатор компонента программы, который выполняет обновление.

- Информация об использовании Kaspersky Security Network (далее "KSN"): идентификатор KSN, идентификатор ПО, полная версия ПО, обезличенный IP-адрес устройства пользователя, показатели качества выполнения запросов к KSN, показатели качества обработки пакетов для KSN, показатели количества запросов в KSN и информация о типах запросов в KSN, дата и время начала передачи статистики, дата и время окончания передачи статистики, информация об обновлениях конфигурации KSN: идентификатор активной конфигурации, идентификатор полученной конфигурации, код ошибки при обновлении конфигурации.

- Информация о событиях в системных журналах: время события, название журнала, в котором обнаружено событие, тип и категория события, название источника события и его описание.

- Информация для определения репутации файлов, URL-адресов и сертификатов: URL-адрес, для которого запрашивается репутация и Referrer, тип протокола соединения, внутренний идентификатор типа программы, номер используемого порта, идентификатор пользователя, контрольная сумма проверяемого файла (MD5), тип обнаруженной угрозы, информация о записи, которая была использована для обнаружения угрозы (идентификатор записи в антивирусной базе, время создания и тип записи); публичный ключ сертификата; отпечаток цифрового сертификата проверяемого объекта и алгоритм хеширования.

- Данные о территориальной распространенности программы: дата установки и дата активации программы, идентификатор партнера, предоставившего лицензию для активации программы, идентификатор программы, идентификатор языковой локализации программы, серийный номер лицензии, по которой программа активирована, признак участия в KSN.

- Информация об используемой лицензии: тип лицензии и срок ее действия, количество дней до истечения срока действия лицензии, идентификатор партнера, у которого приобретена лицензия, идентификатор регионального центра активации, контрольная сумма кода активации, хеш-сумма тела тикета, рассчитанная по алгоритму SHA1, дата и время создания лицензионного тикета, идентификатор информации о лицензии, идентификатор лицензионного тикета, идентификатор последовательности лицензионного тикета, уникальный идентификатор компьютера пользователя, дата начала и окончания периода валидности лицензионного тикета, текущее состояние лицензионного тикета, версия заголовка тикета, версия лицензии, идентификатор сертификата подписи заголовка тикета, контрольная сумма файла ключа, серийный номер подписчика заголовка тикета, токен авторизации.

- Информация об установленном на компьютере аппаратном обеспечении: тип, название, модель, версия прошивки, характеристики встроенных и подключенных устройств.

- Информация об устройстве: идентификатор устройства.

- Информация о работе компонента "Веб-Контроль":

  версия компонента, причина категоризации, дополнительная информация о причине категоризации, категоризированный URL-адрес, IP-адрес хоста заблокированного/категоризированного объекта.

Примечание. В зависимости от настроек Kaspersky Security Center, вы можете участвовать в Kaspersky Private Security Network вместо Kaspersky Security Network. Kaspersky Endpoint Security уведомит вас о переключении с Kaspersky Private Security Network на Kaspersky Security Network и предложит принять условия Положения о Kaspersky Security Network. Подробную информацию об участии в Kaspersky Private Security Network вы можете найти в справке Kaspersky Security Center.

Инфраструктура Kaspersky Security Network

Kaspersky Endpoint Security поддерживает следующие инфраструктурные решения KSN:

- *Глобальный KSN* – это решение, которое используют большинство приложений "Лаборатории Касперского". Участники KSN получают информацию от Kaspersky Security Network, а также отправляют в "Лабораторию Касперского" данные об объектах, обнаруженных на компьютере пользователя, для дополнительной проверки аналитиками "Лаборатории Касперского" и пополнения репутационных и статистических баз Kaspersky Security Network.

- *Локальный KSN* – это решение, позволяющее пользователям компьютеров, на которые установлено приложение Kaspersky Endpoint Security или другие приложения "Лаборатории Касперского", получать доступ к репутационным базам Kaspersky Security Network, а также другим статистическим данным, не отправляя данные в KSN со своих компьютеров. Локальный KSN разработан для корпоративных клиентов, не имеющих возможности участвовать в Kaspersky Security Network, например, по следующим причинам:

  - отсутствие подключения локальных рабочих мест к интернету;

  - законодательный запрет или ограничение корпоративной безопасности на отправку любых данных за пределы страны или за пределы локальной сети организации.

По умолчанию Kaspersky Security Center использует Глобальный KSN. Вы можете настроить использование Локального KSN в Консоли администрирования (MMC) Kaspersky Security Center и в Kaspersky Security Center Web Console. Настроить использование Локального KSN в Kaspersky Security Center Cloud Console невозможно.

KSN Proxy

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

Служба KSN Proxy предоставляет следующие возможности:

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

Подробную информацию о службе KSN Proxy см. в справке Kaspersky Security Center.

Примечание. Функциональность обновлений (включая обновления сигнатур вредоносного ПО и обновления кодовой базы), а также функциональность KSN могут быть недоступны в ПО на территории США.

Проверка целостности компонентов приложения

Kaspersky Endpoint Security содержит различные бинарные модули в виде динамически подключаемых библиотек, исполняемых файлов, конфигурационных файлов и интерфейсных файлов. Злоумышленники могут заменить один или несколько исполняемых модулей или файлов приложения другими файлами, содержащими вредоносный код. Чтобы предотвратить это, Kaspersky Endpoint Security может проверить целостность компонентов приложения. Приложение проверяет модули и файлы на наличие несанкционированных изменений или повреждений. Если модуль или файл приложения имеет неправильную контрольную сумму, он считается поврежденным.

Целостность компонентов приложения проверяется с помощью утилиты integrity_checker, расположенной в каталоге /Library/Application Support/Kaspersky Lab/KAV/Binaries. Этот утилита проверяет целостность файла манифеста, содержащего список файлов приложения, целостность которых критична для корректной работы компонента приложения.

Файл манифеста целостности integrity_check.xml, защищенный криптографической подписью "Лаборатории Касперского", находится в той же директории, что и утилита проверки целостности (/Library/Application Support/Kaspersky Lab/KAV/Binaries).

Примечание. Для запуска утилиты проверки целостности требуются права учетной записи пользователя Root.

Проверка целостности может быть выполнена с помощью утилиты, установленной вместе с приложением, или с помощью утилиты на сертифицированном компакт-диске.

Чтобы проверить целостность компонентов приложения, выполните следующую команду:

```
sudo "/Library/Application Support/Kaspersky
Lab/KAV/Binaries/integrity_checker"
```

По умолчанию утилита использует файл integrity_check.xml, расположенный в каталоге /Library/Application Support/Kaspersky Lab/KAV/Binaries.

Чтобы вызвать справку по настройкам утилиты, выполните следующую команду:

```
--help
```

Результат проверки каждого файла манифеста отображается рядом с именем файла манифеста в следующем формате:

- `SUCCEEDED` – целостность файлов подтверждена (код возврата `0`)
- `FAILED` – целостность файлов не подтверждена (код возврата не равен `0`)

Управление приложением через Консоль администрирования Kaspersky Security Center

Программа Kaspersky Security Center предназначена для централизованного управления защитой сети организации. Подробную информацию о Kaspersky Security Center вы можете найти в справке Kaspersky Security Center .

Также вы можете управлять работой Kaspersky Endpoint Security с помощью графического пользовательского интерфейса приложения, через Kaspersky Security Center Web Console и Cloud Console и из командной строки.

Развертывание Kaspersky Endpoint Security в сети организации

1. Разверните в сети *Сервер администрирования*.

   Сервер администрирования – компонент программы Kaspersky Security Center, осуществляющий функции централизованного хранения информации об установленных в сети организации приложениях "Лаборатории Касперского" и управления ими.

2. Установите *Консоль администрирования* на рабочее место администратора Kaspersky Security Center.

Консоль администрирования – компонент программы Kaspersky Security Center, предоставляющий пользовательский интерфейс к административным сервисам Сервера администрирования и *Агента администрирования*. Агент администрирования обеспечивает взаимодействие Сервера администрирования и приложения Kaspersky Endpoint Security, установленного на компьютерах в сети организации.

3. Установите плагин управления Kaspersky Endpoint Security на рабочее место администратора Kaspersky Security Center.

   Плагин управления – специализированный компонент, предоставляющий интерфейс для управления работой программ "Лаборатории Касперского" через Консоль администрирования. Для каждого приложения существует свой плагин управления. Плагин управления входит в состав всех приложений "Лаборатории Касперского", управление которыми может осуществляться при помощи Kaspersky Security Center.

4. Установите Агент администрирования на удаленные компьютеры Mac одним из следующих способов:

   - Локально.
   - Удаленно с помощью Apple Remote Desktop.
   - Удаленно через Kaspersky Security Center.
   - Удаленно с помощью SSH-протокола.

   Примечание. Для управления Kaspersky Endpoint Security для Mac 12.2 через Kaspersky Security Center вам нужно установить Агент администрирования версии 15 на удаленные компьютеры.

5. Установите Kaspersky Endpoint Security на удаленные компьютеры Mac одним из следующих способов:

   - Локально.
   - Удаленно с помощью Apple Remote Desktop.
   - Удаленно с помощью SSH-протокола.
   - Удаленно через Kaspersky Security Center.

Важно! Если Kaspersky Internet Security для Mac или другие программы поиска вредоносного ПО уже установлены на удаленных компьютерах, вам нужно их удалить перед установкой Kaspersky Endpoint Security.

Подробную информацию о развертывании Сервера администрирования и установке Консоли администрирования вы можете найти в справке Kaspersky Security Center .

Обновление Kaspersky Endpoint Security версии 11.1 или более поздней до версии 12.2

Примечание. Для управления Kaspersky Endpoint Security для Mac 12.2 через Kaspersky Security Center вам нужно установить Агент администрирования версии 15 на удаленные компьютеры.

Вы можете обновить Kaspersky Endpoint Security версии 11.1 или более поздней под управлением Kaspersky Security Center до версии 12.2 одним из следующих способов:

- Одновременно обновить и Kaspersky Endpoint Security до версии 12.2, и Агент администрирования до версии 15 на удаленных компьютерах.
- Сначала обновить Агент администрирования до версии 15, а затем обновить Kaspersky Endpoint Security до версии 12.2.

При обновлении приложения до более новой версии учитывайте следующее:

- Для обновления Kaspersky Endpoint Security до версии 12.2 требуется macOS 12 или более поздняя версия.
- Необходимо загрузить архив KES_11.3_profile.zip с сайта Службы технической поддержки , чтобы применить новый конфигурационный профиль.
- После обновления Kaspersky Endpoint Security до версии 12.2 в настройках сети могут появиться два элемента Kaspersky Filter и два Kaspersky Monitor.
- Если у вас установлено приложение Kaspersky Endpoint Security версии 11.0.1 или более ранней, чтобы обновить приложение до версии 12.2, вам необходимо удалить приложение и обновить macOS до версии 12 или более поздней. Затем вы можете установить Kaspersky Endpoint Security версии 12.2.

Примечание. Функциональность обновлений (включая обновления сигнатур вредоносного ПО и обновления кодовой базы), а также функциональность KSN могут быть недоступны в ПО на территории США.

Подготовка к удаленной установке Kaspersky Endpoint Security

В этом разделе содержится информация об установке плагина управления Kaspersky Endpoint Security на рабочее место администратора Kaspersky Security Center и установке Агента администрирования на удаленный компьютер.

Установка плагина управления Kaspersky Endpoint Security и установка Агента администрирования являются этапами подготовки к установке Kaspersky Endpoint Security через Kaspersky Security Center.

Установка плагина управления Kaspersky Endpoint Security

Плагин управления Kaspersky Endpoint Security – специализированный компонент, предоставляющий интерфейс для управления работой приложения Kaspersky Endpoint Security через Консоль администрирования.

Установка плагина управления Kaspersky Endpoint Security

1. На рабочем месте администратора Kaspersky Security Center распакуйте архив с файлами дистрибутива Kaspersky Endpoint Security.
2. Откройте папку с файлами дистрибутива Kaspersky Endpoint Security.
3. Запустите файл klcfginst.exe двойным щелчком мыши.

Начнется установка плагина управления Kaspersky Endpoint Security.

Важно! Перед установкой плагина управления Kaspersky Endpoint Security нужно завершить работу Консоли администрирования на рабочем месте администратора Kaspersky Security Center.

Локальная установка Агента администрирования

Агент администрирования обеспечивает взаимодействие Сервера администрирования и приложения Kaspersky Endpoint Security, установленного на компьютерах в сети организации.

Локальная установка Агента администрирования

1. На удаленном компьютере откройте содержимое дистрибутива Агента администрирования.
2. Откройте DMG-файл дистрибутива Агента администрирования.

   Откроется окно с содержимым дистрибутива.
3. В окне с содержимым дистрибутива дважды щелкните по кнопке **Kaspersky Network Agent**.
4. Подтвердите, что вы хотите установить Агент администрирования, нажав на кнопку **Продолжить**.
5. В окне **Введение** нажмите на кнопку **Продолжить**.
6. В окне **Лицензия** прочитайте текст Лицензионного соглашения об использовании Агента администрирования, которое заключается между вами и АО "Лаборатория Касперского". Вы можете выполнить следующие действия:
   - Если вы согласны со всеми пунктами Лицензионного соглашения, нажмите на кнопку **Продолжить**, чтобы продолжить установку.
   - Чтобы распечатать текст соглашения, нажмите на кнопку **Напечатать**.
   - Чтобы сохранить соглашение в текстовом файле, нажмите на кнопку **Сохранить**.
7. В окне подтверждения выполните одно из следующих действий:
   - Чтобы продолжить установку Агента администрирования, нажмите на кнопку **Принимаю**.
   - Чтобы вернуться к тексту Лицензионного соглашения, нажмите на кнопку **Прочитать лицензию**.
   - Чтобы отменить установку, нажмите на кнопку **Не принимаю**.
8. В окне **Параметры** выполните следующие действия:
   a. В поле **Сервер** укажите IP-адрес или DNS-имя сервера, на котором установлен Kaspersky Security Center.
   b. В поле **Порт** укажите номер порта для незащищенного соединения с сервером.

c. В поле **SSL-порт** укажите номер порта для SSL-соединения с сервером.

d. Если вы хотите запустить Агента администрирования сразу после установки, установите флажок **Запустить после установки**.

Если вы не хотите использовать SSL для соединения с сервером, снимите флажок **Использовать SSL**. Для продолжения установки нажмите на кнопку **Продолжить**.

9. В окне **Тип установки** прочитайте информацию о диске, на который будет устанавливаться Агент администрирования.

   Чтобы установить Агента администрирования, используя рекомендованные настройки, нажмите на кнопку **Установить** и введите пароль администратора для подтверждения.

   Подождите, пока программа установки Агента администрирования установит компоненты приложения.

10. Нажмите на кнопку **Закрыть** для выхода из программы установки.

Установка Агента администрирования с помощью Apple Remote Desktop

1. На удаленном компьютере выберите **меню Apple** > **Системные настройки** > **Общие** > **Общий доступ**.

2. Установите флажок **Удаленное управление**.

3. На другом Mac, который вы хотите назначить сервером, установите Apple Remote Desktop. Вы можете найти дополнительную информацию об Apple Remote Desktop на сайте Службы поддержки Apple.

4. Откройте Apple Remote Desktop.

5. В левой части окна **Remote Desktop** нажмите **Scanner** и выберите устройства, на которые вы хотите установить Агент администрирования.

6. Нажмите на кнопку **Copy**.

7. Нажмите на кнопку + и выберите файлы для установки Агента администрирования: DMG-файл, KUD-файл и SH-файл.

8. Во всплывающем меню **Place items in** выберите **Top folder of the disk**.

9. Нажмите на кнопку **Copy**.

10. После того, как копирование файлов завершилось, нажмите на кнопку **Unix**.

11. Введите следующую команду:

```
cd /;
./install.sh --accept_eula -r <адрес Сервера администрирования>
```

где `<адрес Сервера администрирования>` – DNS-имя или IP-адрес Сервера администрирования Kaspersky Security Center.

> **Примечание.** Если вы вводите эту команду, вы принимаете условия Лицензионного соглашения.

12. Укажите, что вы хотите запускать команду как **User** и введите "root" в поле.

13. Нажмите на кнопку **Send**.

Установка Агента администрирования запустится на выбранных устройствах.

Установка Агента администрирования через Kaspersky Security Center

Kaspersky Security Center устанавливает Агент администрирования на клиентский компьютер с использованием SSH-соединения.

Перед установкой Агента администрирования на клиентский компьютер убедитесь, что соблюдены следующие условия:

- Сервер администрирования Kaspersky Security Center развернут в сети организации.
- Консоль администрирования установлена на рабочее место администратора Kaspersky Security Center.
- На удаленных компьютерах разрешен Удаленный вход.
- На удаленном компьютере создана выделенная учетная запись с правами администратора, которая будет использована для запуска задачи удаленной установки. Вы можете использовать доменную учетную запись для установки.
- Пароль sudo выключен для выделенной учетной записи.

Создание инсталляционного пакета Агента администрирования

1. Запустите Консоль администрирования Kaspersky Security Center.

2. Разверните узел **Сервер администрирования <Имя сервера>**.

3. В дереве консоли выберите папку **Дополнительно**, в ней подпапку **Удаленная установка**, а в ней подпапку **Инсталляционные пакеты**.

4. В рабочей области нажмите на кнопку **Создать инсталляционный пакет**.

5. В окне **Выбор типа инсталляционного пакета** нажмите на кнопку **Создать инсталляционный пакет для программы "Лаборатории Касперского"**.

6. В окне **Определение имени инсталляционного пакета** в поле ввода **Имя** укажите имя нового инсталляционного пакета и нажмите **Далее**.

7. В окне **Выбор дистрибутива программы для установки** нажмите на кнопку **Обзор**.

   Откроется окно выбора файла для создания инсталляционного пакета.

8. Откройте папку с содержимым дистрибутива Агента администрирования и выберите файл klnagent.kud.

   В окне **Выбор дистрибутива программы для установки** отобразится название и версия приложения для удаленной установки с помощью файла, который был добавлен.

9. Нажмите **Далее**.

   Инсталляционный пакет Kaspersky Endpoint Security с указанными параметрами будет создан.

10. В последнем окне мастера нажмите на кнопку **Готово**, чтобы выйти из мастера создания инсталляционного пакета.

Создание задачи удаленной установки Агента администрирования на клиентский компьютер

1. Запустите Консоль администрирования Kaspersky Security Center.

2. Разверните узел **Сервер администрирования <Имя сервера>**.

3. Выберите папку **Задачи**.

4. В рабочей области нажмите на кнопку **Новая задача**, чтобы запустить мастер создания задачи.

5. Следуйте шагам мастера создания задачи, чтобы создать задачу удаленной установки Kaspersky Endpoint Security на клиентский компьютер.

Чтобы перейти к следующему шагу мастера, нажмите на кнопку **Далее**. Чтобы вернуться к предыдущему шагу мастера, нажмите на кнопку . Чтобы завершить работу мастера на любом шаге, нажмите на кнопку **Отмена**.

Примечание. Вид кнопок может отличаться в зависимости от используемой версии Windows.

Шаг 1. Выбор типа задачи

1. В окне **Выбор типа задачи** разверните узел **Сервер администрирования Kaspersky Security Center**.
2. Выберите задачу **Удаленная установка программы**.

Шаг 2. Выбор инсталляционного пакета

В окне **Выбор инсталляционного пакета** выполните одно из следующих действий:

- Если инсталляционный пакет Агента администрирования с нужными параметрами уже был создан ранее, выберите его в списке инсталляционных пакетов в верхней части окна **Выбор инсталляционного пакета**.
- Если инсталляционный пакет с нужными параметрами еще не был создан, нажмите **Новый**, чтобы запустить мастер создания пакета.

Шаг 3. Настройка параметров установки

В окне **Параметры** выполните следующие действия:

1. Установите флажок **Средствами операционной системы с помощью Сервера администрирования**.
2. Снимите остальные флажки.

Шаг 4. Выбор группы администрирования для добавления компьютеров после установки

Если требуется, в окне **Перемещение в список управляемых устройств** выберите группу администрирования, в которую будут добавлены компьютеры после установки приложения.

Шаг 5. Определение способа выбора клиентских компьютеров, для которых будет создана задача

В окне **Выбор устройств, которым будет назначена задача** выберите способ, который хотите использовать для выборки клиентских компьютеров:

- Если вы хотите выбрать из компьютеров, обнаруженных в сети Сервером администрирования, выберите вариант **Выбрать устройства, обнаруженные в сети Сервером администрирования**.
- Если вы хотите указать IP-адреса компьютеров вручную или импортировать IP-адреса компьютеров из файла, выберите вариант **Задать адреса устройств вручную или импортировать из списка**.
- Если вы хотите создать задачу для выборки устройств по предопределенному критерию, выберите вариант **Назначить задачу выборке устройств**.
- Если вы хотите выбрать компьютеры из указанной группы администрирования, выберите вариант **Назначить задачу группе администрирования**.

Шаг 6. Выбор клиентских компьютеров

В открывшемся окне (**Выбор устройств**, **Выборка устройств** или **Выберите группу администрирования**, в зависимости от варианта, который вы выбрали на предыдущем шаге), выберите клиентские компьютеры, укажите IP-адреса компьютеров, укажите выборку компьютеров, или выберите группу администрирования, для которой будет создана задача.

Шаг 7. Выбор учетной записи для запуска задачи

1. В окне **Выбор учетной записи для запуска задачи** установите флажок **Учетная запись требуется (Агент администрирования не используется)**.
2. Нажмите на кнопку **Добавить** > **Учетная запись**.

   Откроется окно **Учетная запись**.

3. Введите логин и пароль выделенной учетной записи администратора на удаленном компьютере.

4. Нажмите **OK**.

Шаг 8. Настройка расписания запуска задачи

1. В окне **Настройка расписания запуска задачи** в раскрывающемся списке **Запуск по расписанию** выберите режим запуска задачи.

2. Если требуется, укажите дату и время запуска задачи, чтобы задача запустилась автоматически по установленному расписанию.

3. Если вы хотите запускать задачи, которые приложение не смогло запустить по расписанию (например, компьютер был выключен в установленное расписанием время), установите флажок **Запускать пропущенные задачи**.

   Kaspersky Endpoint Security запустит задачу, как только помеха, которая препятствует запуску задачи, будет устранена.

Шаг 9. Определение названия задачи

В окне **Определение названия задачи** в поле **Имя** введите название создаваемой задачи.

Шаг 10. Завершение создания задачи

В окне **Завершение создания задачи** выполните следующие действия:

1. Если вы хотите запустить задачу после завершения работы мастера, установите флажок **Запустить задачу после завершения работы мастера**.

2. Нажмите на кнопку **Готово** для завершения работы мастера.

Установка Агента администрирования с использованием SSH-протокола

Вы можете установить Агент администрирования на удаленный компьютер с использованием SSH-протокола.

Перед установкой приложения убедитесь, что вы выполнили следующие требования:

- Сервер администрирования Kaspersky Security Center развернут в сети организации.
- Консоль администрирования установлена на рабочее место администратора Kaspersky Security Center.
- Инсталляционный пакет Агента администрирования создан и хранится в папке общего доступа Сервера администрирования.
- На удаленном компьютере разрешен Удаленный вход.
- Учетная запись, с помощью которой устанавливается Агент администрирования, добавлена в файл sudoers.

Подробную информацию об инсталляционных пакетах вы можете найти в справке Kaspersky Security Center .

Установка Агента администрирования с использованием SSH-протокола

1. На рабочем месте администратора запустите SSH-клиент.
2. Соединитесь с удаленным компьютером.
3. Подключите папку общего доступа Сервера администрирования в качестве сетевого диска на удаленном компьютере. Для этого в SSH-клиенте введите следующие команды:

   ```
   mkdir /Volumes/KLSHARE
   mount_smbfs //<учетная запись администратора>:<пароль>@<IP-адрес Сервера администрирования>/KLSHARE /Volumes/KLSHARE
   ```

   Описание параметров:

   - `<учетная запись администратора>` – имя учетной записи администратора Сервера администрирования;
   - `<пароль>` – пароль учетной записи администратора Сервера администрирования;
   - `<IP-адрес Сервера администрирования>` – IP-адрес сервера, на котором установлен Kaspersky Security Center.
4. Запустите скрипт установки. Для этого в SSH-клиенте введите следующую команду:

   ```
   cd /Volumes/KLSHARE/<папка с инсталляционным пакетом>
   ```

где `<папка с инсталляционным пакетом>` – папка, в которой расположен инсталляционный пакет Агента администрирования.

```
sudo ./install.sh --accept_eula [-r <сервер>] [-p <номер порта>]
[-s use_ssl 0|1] [-l <номер SSL-порта>] [-x use_proxy 0|1] [-a
<прокси>] [-n <имя пользователя>] [-w <пароль>]
```

Описание параметров:

- `<сервер>` – IP-адрес или DNS-имя сервера, на котором установлен Kaspersky Security Center.
- `<номер порта>` – номер порта, по которому будет осуществляться незащищенное соединение с Сервером администрирования. По умолчанию используется 14000 порт.
- `use_ssl 0|1` – параметр, определяющий использование шифрования при соединении Агента администрирования с Сервером администрирования. Если указано значение "0", используется незащищенное соединение. Если указано значение "1", соединение осуществляется по SSL-протоколу (значение по умолчанию).
- `<номер SSL-порта>` – номер порта, по которому будет осуществляться защищенное соединение с Сервером администрирования по SSL-протоколу. По умолчанию используется 13000 порт.
- `use_proxy 0|1` – параметр, определяющий использование прокси-сервера при подключении к интернету. Если указано значение "0", прокси-сервер не используется. Если указано значение "1", соединение осуществляется через прокси-сервер (значение по умолчанию).
- `<прокси>` – IP-адрес или DNS-имя прокси-сервера.
- `<имя пользователя>` – имя пользователя для соединения с прокси-сервером.
- `<пароль>` – пароль для соединения с прокси-сервером.

Важно! Для выполнения команды требуются права администратора.

5. Отключите сетевой диск на удаленном компьютере. Для этого в SSH-клиенте введите следующую команду:
   ```
   umount /Volumes/KLSHARE
   ```
6. Проверьте правильность работы Агента администрирования на удаленном компьютере. Для этого в SSH-клиенте введите следующие команды:

```
cd /Library/Application\ Support/Kaspersky\
Lab/klnagent/Binaries/
sudo ./klnagchk
```

Если проверка прошла успешно, то Агент администрирования работает нормально.

Локальное удаление Агента администрирования

1. На удаленном компьютере откройте папку с дистрибутивом Агента администрирования.
2. Откройте DMG-файл дистрибутива Агента администрирования.

   Откроется окно с содержимым дистрибутива.
3. В окне с содержимым дистрибутива дважды щелкните по кнопке **Программа удаления Агента администрирования**.
4. В окне **Введение** нажмите на кнопку **Продолжить**.
5. В окне **Информация** нажмите на кнопку **Удалить**.
6. В окне запроса учетных данных администратора компьютера введите имя администратора и пароль и подтвердите, что вы хотите удалить Агента администрирования.

   Начнется удаление Агента администрирования.
7. Прочитайте информацию о завершении удаления и нажмите на кнопку **Готово**, чтобы закрыть программу удаления.

Агент администрирования удален с удаленного компьютера.

Управление Агентом администрирования из командной строки

Этот раздел содержит информацию об управлении Агентом администрирования с помощью командной строки на компьютере пользователя.

Вы можете завершить работу Агента администрирования и запустить его вновь из командной строки на компьютере пользователя.

Также вы можете подключить удаленный компьютер к Серверу администрирования вручную с помощью утилиты klmover и проверить соединение удаленного компьютера с Сервером администрирования посредством утилиты klnagchk.

Вы можете удалить Агент администрирования.

Запуск и остановка Агента администрирования на удаленном компьютере

Вы можете завершить работу Агента администрирования и запустить его вновь на удаленном компьютере из командной строки.

Завершение работы Агента администрирования

На удаленном компьютере из командной строки запустите утилиту launchctl с командой unload.

Синтаксис команды:

```
sudo launchctl unload
/Library/LaunchDaemons/com.kaspersky.klnagent.plist
```

Запуск Агента администрирования

На удаленном компьютере из командной строки запустите утилиту launchctl с командой load.

Синтаксис команды:

```
sudo launchctl load /Library/LaunchDaemons/com.kaspersky.klnagent.plist
```

Важно! Для завершения работы и запуска Агента администрирования требуются права администратора.

Проверка соединения клиентского компьютера и Сервера администрирования вручную Утилита klnagchk

Проверка соединения клиентского компьютера с Сервером администрирования

На удаленном компьютере из командной строки запустите утилиту klnagchk.

Утилита klnagchk входит в инсталляционный пакет Агента администрирования.

После установки Агента администрирования утилита klnagchk располагается в папке /Library/Application Support/Kaspersky Lab/klnagent/Binaries.

В зависимости от параметров, указанных при запуске из командной строки, утилита klnagchk выполняет следующие действия:

- выводит на экран или сохраняет в файл значения параметров соединения установленного на удаленном компьютере Агента администрирования с Сервером администрирования;
- сохраняет в файл или выводит на экран статистику работы Агента администрирования (с момента последнего запуска программы) и результаты выполнения операций;
- предпринимает попытку установить соединение Агента администрирования с Сервером администрирования;
- если соединение установить не удалось, утилита посылает ICMP-пакет для проверки статуса компьютера, на котором установлен Сервер администрирования.

Перед запуском утилиты в командной строке перейдите в папку /Library/Application Support/Kaspersky Lab/klnagent/Binaries.

Синтаксис команды:

```
sudo ./klnagchk [-logfile <имя файла>] [-sp] [-savecert <путь к файлу сертификата>] [-restart]
```

Важно! Для запуска утилиты требуются права администратора.

Описание параметров

`-logfile <имя файла>` – сохранять в указанный файл значения параметров соединения Агента администрирования с Сервером администрирования и результаты выполнения операций. Если параметр не указан, параметры соединения с сервером, результаты выполнения операций и сообщения об ошибках выводятся на экран.

`-sp` – сохранять в указанный файл или выводить на экран пароль для аутентификации на прокси-сервере. Параметр используется, если Агент администрирования соединяется с Сервером администрирования через прокси-сервер. По умолчанию не используется.

`-savecert <имя файла>` – сохранять сертификат для аутентификации на Сервере администрирования в указанном файле.

`-restart` – перезапустить Агент администрирования после завершения работы утилиты.

Пример:

sudo ./klnagchk -logfile klnagchk.log -sp

Подключение удаленного компьютера к Серверу администрирования вручную. Утилита klmover

Подключение удаленного компьютера к Серверу администрирования

На удаленном компьютере из командной строки запустите утилиту klmover.

Утилита klmover входит в инсталляционный пакет Агента администрирования.

После установки Агента администрирования утилита klmover располагается в папке /Library/Application Support/Kaspersky Lab/klnagent/Binaries.

В зависимости от параметров, указанных при запуске из командной строки, утилита klmover выполняет следующие действия:

- подключает Агента администрирования к Серверу администрирования с указанными параметрами;
- сохраняет результаты выполнения операции в файл или выводит их на экран.

Перед запуском утилиты в командной строке перейдите в папку /Library/Application Support/Kaspersky Lab/klnagent/Binaries.

Синтаксис командной строки:

```
sudo ./klmover [-logfile <имя файла>] [-address <адрес сервера>] [-pn <номер порта>] [-ps <номер SSL-порта>] [-nossl] [-cert <путь к файлу сертификата>] [-silent] [-dupfix]
```

Важно! Для запуска утилиты требуются права администратора.

Описание параметров

`-logfile <имя файла>` – сохранять результаты выполнения операции в указанный файл. Если параметр не указан, результаты выполнения операции и сообщения об ошибках выводятся на экран.

`-address <адрес сервера>` – адрес Сервера администрирования, который Агент администрирования использует для соединения. Вы можете указать IP-адрес или DNS-имя сервера.

Примечание. Вы также можете использовать команду с этим параметром, чтобы изменить адрес Сервера администрирования, с которым удаленные компьютеры устанавливают соединение.

`-pn <номер порта>` – номер порта, по которому будет осуществляться незащищенное соединение с Сервером администрирования. По умолчанию используется 14000 порт.

`-ps <номер SSL-порта>` – номер порта, по которому будет осуществляться защищенное соединение с Сервером администрирования по SSL-протоколу. По умолчанию используется 13000 порт.

`-nossl` – использовать незащищенное соединение с Сервером администрирования. Если параметр не указан, Агент администрирования устанавливает защищенное соединение с Сервером администрирования по SSL-протоколу.

`-cert <путь к файлу сертификата>` – использовать указанный файл сертификата для аутентификации на новом Сервере администрирования. Если параметр не указан, Агент администрирования получит сертификат при первом подключении к Серверу администрирования.

`-silent` – запустить утилиту на выполнение в неинтерактивном режиме.

`-dupfix` – этот параметр используется в случае, если установка Агента администрирования на компьютеры была выполнена не предложенными в этой справке способами, а, например, путем восстановления из образа диска с установленным Агентом администрирования. Если автоматическая самоидентификация Агента администрирования приводит к дублированию значков исходного компьютера и остальных компьютеров в Консоли администрирования, вы можете подключить дублирующиеся компьютеры заново.

Примечание. Рекомендуется запускать утилиту klmover с указанием значений всех параметров.

Пример:

```
sudo ./klmover -logfile klmover.log -address 192.0.2.12 -ps 13001
```

Удаленный компьютер, который подключен к Серверу администрирования через Агента администрирования, называется *клиентским компьютером*.

Удаление Агента администрирования

Синтаксис команды:

```
sudo '/Library/Application Support/Kaspersky
Lab/klnagent/Binaries/UninstallScript'
```

Установка и удаление Kaspersky Endpoint Security

В этом разделе содержится информация об удаленной установке Kaspersky Endpoint Security на клиентский компьютер и удалении с него.

Также вы можете установить и удалить Kaspersky Endpoint Security локально или через Kaspersky Security Center Web Console или Kaspersky Security Center Cloud Console.

Установка приложения с использованием SSH-протокола

Перед установкой Kaspersky Endpoint Security на удаленный компьютер убедитесь, что соблюдены следующие условия:

- Сервер администрирования Kaspersky Security Center развернут в сети организации.
- Консоль администрирования установлена на рабочее место администратора Kaspersky Security Center.
- Инсталляционный пакет для приложения Kaspersky Endpoint Security создан и хранится в папке общего доступа Сервера администрирования.
- Файл ключа для Kaspersky Endpoint Security хранится в папке общего доступа Сервера администрирования (по желанию).
- На удаленном компьютере разрешен Удаленный вход.
- Учетная запись, с помощью которой устанавливается приложение, добавлена в файл sudoers.

Установка Kaspersky Endpoint Security на клиентский компьютер с использованием SSH-протокола

1. На рабочем месте администратора Kaspersky Security Center запустите SSH-клиент.

2. Соединитесь с удаленным компьютером.

3. Подключите папку общего доступа Сервера администрирования в качестве сетевого диска на удаленном компьютере. Для этого в SSH-клиенте введите следующие команды:

   ```
   mkdir /Volumes/KLSHARE
   mount_smbfs //<учетная запись администратора>:<пароль>@<IP-адрес Сервера администрирования>/KLSHARE /Volumes/KLSHARE
   ```

   Описание параметров:

   - `<учетная запись администратора>` – имя учетной записи администратора Сервера администрирования;
   - `<пароль>` – пароль учетной записи администратора Сервера администрирования;
   - `<IP-адрес Сервера администрирования>` – IP-адрес сервера, на котором установлен Kaspersky Security Center.

4. Запустите скрипт установки. Для этого в SSH-клиенте введите следующие команды:

   ```
   cd /Volumes/KLSHARE/<папка KES с установочным файлом>
   ./install.sh --accept_eula
   ```

   где `<папка KES с установочным файлом>` – папка, в которой расположен инсталляционный пакет Kaspersky Endpoint Security.

   Важно! Для выполнения команды требуются права администратора.

5. Отключите сетевой диск на удаленном компьютере. Для этого в SSH-клиенте введите следующую команду:

   ```
   umount /Volumes/KLSHARE
   ```

Установка приложения через Kaspersky Security Center

Перед установкой Kaspersky Endpoint Security на клиентский компьютер убедитесь, что соблюдены следующие условия:

- Сервер администрирования Kaspersky Security Center развернут в сети организации.

- Консоль администрирования установлена на рабочее место администратора Kaspersky Security Center.
- Агент администрирования установлен на клиентском компьютере.
- Инсталляционный пакет для приложения Kaspersky Endpoint Security создан и хранится в папке общего доступа Сервера администрирования.
- Файл ключа для Kaspersky Endpoint Security хранится в папке общего доступа Сервера администрирования (по желанию).
- Клиентский компьютер добавлен в группу администрирования **Управляемые устройства** Сервера администрирования (по желанию).

Подробную информацию о группах администрирования Сервера администрирования вы можете найти в справке Kaspersky Security Center .

Чтобы установить Kaspersky Endpoint Security на клиентский компьютер через Kaspersky Security Center, вам нужно создать и запустить задачу **Удаленная установка программы**.

Создание задачи удаленной установки Kaspersky Endpoint Security на клиентский компьютер

1. Запустите Консоль администрирования Kaspersky Security Center.
2. Разверните узел **Сервер администрирования <Имя сервера>**.
3. Выберите папку **Задачи**.
4. В рабочей области нажмите на кнопку **Новая задача**, чтобы запустить мастер создания задачи.
5. Следуйте шагам мастера создания задачи, чтобы создать задачу удаленной установки Kaspersky Endpoint Security на клиентский компьютер.

Чтобы перейти к следующему шагу мастера, нажмите на кнопку **Далее**. Чтобы вернуться к предыдущему шагу мастера, нажмите на кнопку . Чтобы завершить работу мастера на любом шаге, нажмите на кнопку **Отмена**.

Примечание. Вид кнопок может отличаться в зависимости от используемой версии Windows.

Шаг 1. Выбор типа задачи

1. В окне **Выбор типа задачи** разверните узел **Сервер администрирования Kaspersky Security Center**.

2. Выберите задачу **Удаленная установка программы**.

Шаг 2. Выбор инсталляционного пакета

В окне **Выбор инсталляционного пакета** выполните одно из следующих действий:

- Если инсталляционный пакет Kaspersky Endpoint Security с нужными параметрами уже был создан ранее, выберите его в списке инсталляционных пакетов в верхней части окна **Выбор инсталляционного пакета**.

- Если инсталляционный пакет с нужными параметрами еще не был создан, нажмите **Новый**, чтобы запустить мастер создания пакета.

Шаг 3. Установка дополнительных программ

В окне **Дополнительно** установите флажки **Установить Агент администрирования совместно с данной программой** и **<Название инсталляционного пакета Агента администрирования>**, если вы хотите установить Агент администрирования на клиентский компьютер.

> **Примечание.** Инсталляционный пакет для Агента администрирования должен быть создан заранее. Если инсталляционный пакет отсутствует, нажмите на кнопку **Создать**, чтобы запустить мастер создания инсталляционного пакета.

Шаг 4. Настройка параметров установки

В окне **Параметры** настройте параметры удаленной установки приложения.

Шаг 5. Выбор группы администрирования для добавления компьютеров после установки

Если требуется, в окне **Перемещение в список управляемых устройств** выберите группу администрирования, в которую будут добавлены компьютеры после установки приложения.

Примечание. Окно **Перемещение в список управляемых устройств** появляется, если на шаге 3 вы выбрали установку Агента администрирования.

Шаг 6. Определение способа выбора клиентских компьютеров, для которых будет создана задача

В окне **Выбор устройств, которым будет назначена задача** выберите способ, который хотите использовать для выборки клиентских компьютеров:

- Если вы хотите выбрать из компьютеров, обнаруженных в сети Сервером администрирования, выберите вариант **Выбрать устройства, обнаруженные в сети Сервером администрирования**.
- Если вы хотите указать IP-адреса компьютеров вручную или импортировать IP-адреса компьютеров из файла, выберите вариант **Задать адреса устройств вручную или импортировать из списка**.
- Если вы хотите создать задачу для выборки устройств по предопределенному критерию, выберите вариант **Назначить задачу выборке устройств**.
- Если вы хотите выбрать компьютеры из указанной группы администрирования, выберите вариант **Назначить задачу группе администрирования**.

Шаг 7. Выбор клиентских компьютеров

В открывшемся окне (**Выбор устройств**, **Выборка устройств** или **Выберите группу администрирования**, в зависимости от варианта, который вы выбрали на предыдущем шаге), выберите клиентские компьютеры, укажите IP-адреса компьютеров, укажите выборку компьютеров, или выберите группу администрирования, для которой будет создана задача.

Шаг 8. Выбор учетной записи для запуска задачи

В окне **Выбор учетной записи для запуска задачи** установите флажок **Учетная запись не требуется (Агент администрирования уже установлен)**.

Это означает, что вы установили Агент администрирования до запуска мастера создания задачи.

Шаг 9. Настройка расписания запуска задачи

1. В окне **Настройка расписания запуска задачи** в раскрывающемся списке **Запуск по расписанию** выберите режим запуска задачи.
2. Если требуется, укажите дату и время запуска задачи, чтобы задача запустилась автоматически по установленному расписанию.
3. Если вы хотите запускать задачи, которые приложение не смогло запустить по расписанию (например, компьютер был выключен в установленное расписанием время), установите флажок **Запускать пропущенные задачи**.

   Kaspersky Endpoint Security запустит задачу, как только помеха, которая препятствует запуску задачи, будет устранена.

Шаг 10. Определение названия задачи

В окне **Определение названия задачи** в поле **Имя** введите название создаваемой задачи.

Шаг 11. Завершение создания задачи

В окне **Завершение создания задачи** выполните следующие действия:

1. Если вы хотите запустить задачу после завершения работы мастера, установите флажок **Запустить задачу после завершения работы мастера**.
2. Нажмите на кнопку **Готово** для завершения работы мастера.

Созданная задача отобразится в рабочей области папки **Задачи**.

Создание инсталляционного пакета

Если вы создаете задачу **Удаленная установка программы**, вы можете использовать как уже созданный инсталляционный пакет, так и создать новый. Если вы хотите просмотреть список созданных инсталляционных пакетов, выберите **Дополнительно** > **Удаленная установка** > **Инсталляционные пакеты**.

Создание инсталляционного пакета в Kaspersky Security Center

1. Запустите Консоль администрирования Kaspersky Security Center.
2. Разверните узел **Сервер администрирования <Имя сервера>**.
3. В дереве консоли выберите папку **Дополнительно**, в ней подпапку **Удаленная установка**, а в ней подпапку **Инсталляционные пакеты**.
4. В рабочей области нажмите на кнопку **Создать инсталляционный пакет**.
5. В окне **Выбор типа инсталляционного пакета** нажмите на кнопку **Создать инсталляционный пакет для программы "Лаборатории Касперского"**.
6. В окне **Определение имени инсталляционного пакета** в поле ввода **Имя** укажите имя нового инсталляционного пакета и нажмите **Далее**.
7. В окне **Выбор дистрибутива программы для установки** нажмите на кнопку **Обзор**.

   Откроется окно выбора файла для создания инсталляционного пакета.
8. Откройте папку с содержимым дистрибутива Kaspersky Endpoint Security и выберите файл kesmac.kud.

   В окне **Выбор дистрибутива программы для установки** отобразится название и версия приложения для удаленной установки с помощью файла, который был добавлен.
9. Если требуется, установите флажок **Скопировать обновления из хранилища в инсталляционный пакет**, чтобы скопировать обновления приложения из хранилища Kaspersky Security Center в инсталляционный пакет, и нажмите **Далее**.

   Начнется загрузка инсталляционного пакета на Сервер администрирования. По завершении загрузки откроется окно **Тип установки**.
10. В окне **Тип установки** в блоке **Выберите пакеты для установки** установите или снимите флажки рядом с названиями компонентов программы, которые вы хотите пропустить во время установки на клиентский компьютер и нажмите **Далее**.

    Инсталляционный пакет Kaspersky Endpoint Security с указанными параметрами будет создан.
11. В последнем окне мастера нажмите на кнопку **Готово**, чтобы завершить работу мастера создания инсталляционного пакета.

Удаление приложения через Kaspersky Security Center

Перед удалением Kaspersky Endpoint Security с клиентского компьютера через Kaspersky Security Center убедитесь, что соблюдены следующие условия:

- Сервер администрирования Kaspersky Security Center развернут в сети организации.
- Консоль администрирования установлена на рабочее место администратора Kaspersky Security Center.
- Агент администрирования установлен на клиентском компьютере.

Чтобы удалить Kaspersky Endpoint Security с клиентского компьютера через Kaspersky Security Center вам нужно создать и запустить задачу **Удаленная деинсталляция программы**.

Важно! Удаляя Kaspersky Endpoint Security с клиентского компьютера, вы подвергаете его серьезному риску заражения.

Создание задачи удаленной деинсталляции Kaspersky Endpoint Security с клиентского компьютера

1. Запустите Консоль администрирования Kaspersky Security Center.
2. Разверните узел **Сервер администрирования <Имя сервера>**.
3. Выберите папку **Задачи**.
4. В рабочей области нажмите на кнопку **Новая задача**, чтобы запустить мастер создания задачи.
5. Следуйте шагам мастера создания задачи, чтобы создать задачу удаленной деинсталляции Kaspersky Endpoint Security с клиентского компьютера.

Чтобы перейти к следующему шагу мастера, нажмите на кнопку **Далее**. Чтобы вернуться к предыдущему шагу мастера, нажмите на кнопку . Чтобы завершить работу мастера на любом шаге, нажмите на кнопку **Отмена**.

Примечание. Вид кнопок может отличаться в зависимости от используемой версии Windows.

Шаг 1. Выбор типа задачи

1. В окне **Выбор типа задачи** разверните узел **Сервер администрирования Kaspersky Security Center**.
2. Разверните узел **Дополнительно**.
3. Выберите задачу **Удаленная деинсталляция программы**.

Шаг 2. Выбор удаляемого приложения

В окне **Выбор удаляемой программы** выберите вариант **Удалить программу, поддерживаемую Kaspersky Security Center**.

Шаг 3. Настройка параметров удаления

В окне **Параметры** выполните следующие действия:

1. В раскрывающемся списке **Программа для удаления** выберите элемент **Kaspersky Endpoint Security для Mac 12.2**.
2. Нажмите **Далее**.
3. Настройте параметры удаления приложения.

Шаг 4. Выбор варианта перезагрузки операционной системы

В окне **Выбор действия при необходимости перезагрузки операционной системы** выберите вариант **Не перезагружать устройство**.

Шаг 5. Определение способа выбора клиентских компьютеров, для которых будет создана задача

В окне **Выбор устройств, которым будет назначена задача** выберите способ, который хотите использовать для выборки клиентских компьютеров:

- Если вы хотите выбрать из компьютеров, обнаруженных в сети Сервером администрирования, выберите вариант **Выбрать устройства, обнаруженные в сети Сервером администрирования**.

- Если вы хотите указать IP-адреса компьютеров вручную или импортировать IP-адреса компьютеров из файла, выберите вариант **Задать адреса устройств вручную или импортировать из списка**.
- Если вы хотите создать задачу для выборки устройств по предопределенному критерию, выберите вариант **Назначить задачу выборке устройств**.
- Если вы хотите выбрать компьютеры из указанной группы администрирования, выберите вариант **Назначить задачу группе администрирования**.

Шаг 6. Выбор клиентских компьютеров

В открывшемся окне (**Выбор устройств**, **Выборка устройств** или **Выберите группу администрирования**, в зависимости от варианта, который вы выбрали на предыдущем шаге), выберите клиентские компьютеры, укажите IP-адреса компьютеров, укажите выборку компьютеров, или выберите группу администрирования, для которой будет создана задача.

Шаг 7. Выбор учетной записи для запуска задачи

В окне **Выбор учетной записи для запуска задачи** установите флажок **Учетная запись не требуется (Агент администрирования уже установлен)**.

Это означает, что вы установили Агент администрирования до запуска мастера создания задачи.

Шаг 8. Настройка расписания запуска задачи

1. В окне **Настройка расписания запуска задачи** в раскрывающемся списке **Запуск по расписанию** выберите режим запуска задачи.
2. Если требуется, укажите дату и время запуска задачи, чтобы задача запустилась автоматически по установленному расписанию.
3. Если вы хотите запускать задачи, которые приложение не смогло запустить по расписанию (например, компьютер был выключен в установленное расписанием время), установите флажок **Запускать пропущенные задачи**.

   Kaspersky Endpoint Security запустит задачу, как только помеха, которая препятствует запуску задачи, будет устранена.

Шаг 9. Определение названия задачи

В окне **Определение названия задачи** в поле **Имя** введите название создаваемой задачи.

Шаг 10. Завершение создания задачи

В окне **Завершение создания задачи** выполните следующие действия:

1. Если вы хотите запустить задачу после завершения работы мастера, установите флажок **Запустить задачу после завершения работы мастера**.
2. Нажмите на кнопку **Готово** для завершения работы мастера.

Созданная задача отобразится в рабочей области папки **Задачи**.

Запуск и остановка приложения через Kaspersky Security Center

Вы можете запустить и остановить Kaspersky Endpoint Security на компьютере, выбранном в списке устройств, которыми можно управлять через Kaspersky Security Center.

Запуск и остановка Kaspersky Endpoint Security через Kaspersky Security Center

1. Запустите Консоль администрирования Kaspersky Security Center.
2. Разверните узел **Сервер администрирования <Имя сервера>**.
3. В дереве консоли выберите папку **Управляемые устройства**.
4. Выберите группу администрирования, в которую входит клиентский компьютер.
5. Выберите вкладку **Устройства**.
6. Выберите компьютер в списке клиентских компьютеров.
7. Откройте окно **Свойства: <Название компьютера>** одним из следующих способов:
   - дважды щелкните по имени клиентского компьютера;
   - по правой клавише мыши откройте контекстное меню клиентского компьютера и выберите пункт **Свойства**.

8. Выберите раздел **Программы**.

9. В списке **Программы "Лаборатории Касперского", установленные на устройстве** по правой клавише мыши откройте контекстное меню элемента **Kaspersky Endpoint Security для Mac 12.2** и выполните одно из следующих действий:

   - Если вы хотите запустить программу, выберите пункт **Запустить**.
   - Если вы хотите остановить программу, выберите пункт **Остановить**.

Важно! После остановки работы Kaspersky Endpoint Security, клиентский компьютер продолжит работать в незащищенном режиме и может быть подвергнут риску заражения.

Создание задач и управление ими

Этот раздел содержит информацию об использовании Kaspersky Security Center для создания и настройки задач Kaspersky Endpoint Security на клиентском компьютере или на группе клиентских компьютеров.

Задача – набор действий с настраиваемыми параметрами, который Kaspersky Endpoint Security выполняет на клиентском компьютере.

В Kaspersky Security Center вы можете создать следующие задачи:

- Добавление ключа
- Быстрая проверка
- Откат обновления
- Проверка
- Обновление

Над задачами вы можете выполнять следующие действия:

- запускать и останавливать задачи;
- настраивать параметры задачи;
- отслеживать выполнение задачи;

- копировать и переносить задачи из одной группы в другую;
- удалять задачи;
- импортировать и экспортировать задачи.

Подробную информацию о задачах вы можете найти в справке Kaspersky Security Center.

Создание задачи

При работе с Kaspersky Endpoint Security через Kaspersky Security Center вы можете создавать следующие типы задач:

- Локальные задачи. *Локальная задача* – это задача, которая запускается на отдельном клиентском компьютере.
- Групповые задачи. *Групповая задача* – это задача, которая запускается на компьютерах, входящих в группу администрирования.
- Задачи для произвольного набора компьютеров. Вы можете создать задачу, которая будет запускаться на любых компьютерах, вне зависимости от их принадлежности к группе администрирования или выборке компьютеров.

Создание локальной задачи для отдельного клиентского компьютера

1. Запустите Консоль администрирования Kaspersky Security Center.
2. Разверните узел **Сервер администрирования <Имя сервера>**.
3. В дереве консоли выберите папку **Управляемые устройства**.
4. Выберите группу администрирования, в которую входит клиентский компьютер.
5. В рабочей области выберите вкладку **Устройства**.
6. Выберите компьютер в списке клиентских компьютеров.
7. Откройте окно **Свойства: <Название компьютера>** одним из следующих способов:
   - дважды щелкните по имени клиентского компьютера;
   - по правой клавише мыши откройте контекстное меню клиентского компьютера и выберите пункт **Свойства**.
8. В окне **Свойства:<Название компьютера>** выберите раздел **Задачи**.

В рабочей области справа отобразится список системных и пользовательских задач, созданных для выбранного клиентского компьютера.

9. В нижней части рабочей области нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи.

10. Следуйте шагам мастера создания задачи, чтобы создать локальную задачу для отдельного клиентского компьютера.

Создание задачи для клиентских компьютеров, входящих в группу администрирования

1. Запустите Консоль администрирования Kaspersky Security Center.
2. Разверните узел **Сервер администрирования <Имя сервера>**.
3. В дереве консоли выберите папку **Управляемые устройства**.
4. Выберите группу администрирования, в которую входит клиентский компьютер.
5. В рабочей области выберите вкладку **Задачи**.
6. В рабочей области нажмите на кнопку **Новая задача**, чтобы запустить мастер создания задачи.
7. Следуйте шагам мастера создания задачи, чтобы создать задачу для клиентских компьютеров, входящих в группу администрирования.

Подробную информацию об особенностях создания групповых задач вы можете найти в справке Kaspersky Security Center.

Создание задачи для произвольного набора компьютеров

1. Запустите Консоль администрирования Kaspersky Security Center.
2. Разверните узел **Сервер администрирования <Имя сервера>**.
3. В дереве консоли выберите папку **Задачи**.
4. В рабочей области нажмите на кнопку **Новая задача**, чтобы запустить мастер создания задачи.

5. Следуйте шагам мастера создания задачи, чтобы создать задачу для произвольного набора клиентских компьютеров.

Чтобы перейти к следующему шагу мастера, нажмите на кнопку **Далее**. Чтобы вернуться к предыдущему шагу мастера, нажмите на кнопку . Чтобы завершить работу мастера на любом шаге, нажмите на кнопку **Отмена**.

Примечание. Вид кнопок может отличаться в зависимости от используемой версии Windows.

Шаг 1. Выбор приложения и типа задачи

1. В окне **Выбор типа задачи** разверните узел **Kaspersky Endpoint Security для Mac 12.2**.
2. Выберите тип задачи, которую вы хотите создать:
   - Если вы хотите создать задачу добавления ключа, выберите **Добавление ключа**.
   - Чтобы создать задачу проверки важных областей, выберите **Быстрая проверка**.
   - Если вы хотите создать задачу отката обновления, выберите **Откат обновления**.
   - Если вы хотите создать задачу поиска вредоносного ПО, выберите **Проверка**.
   - Если вы хотите создать задачу обновления, выберите **Обновление**.

Шаг 2. Настройка параметров выбранного типа задачи

В зависимости от выбранного на предыдущем шаге типа задачи содержимое окна настройки параметров задачи может различаться. Для задачи отката обновления это окно не отображается.

Активация приложения

В окне **Активация приложения** выполните следующие действия:

1. Выберите код активации или ключ из хранилища Kaspersky Security Center или добавьте файл ключа, который хранится на вашем компьютере.

2. Если вы хотите добавить указанный ключ в качестве резервного, установите флажок **Добавить в качестве резервного ключа**.

   Резервный ключ становится активным по окончании срока годности текущего активного ключа.

Информация об указанном ключе (ключ, тип ключа, а также дата окончания срока годности ключа) отобразится в окне **Активация приложения**.

Обновление

Основным источником обновлений Kaspersky Endpoint Security являются специальные серверы обновлений "Лаборатории Касперского". Kaspersky Endpoint Security также может использовать в качестве *источника обновлений* точки распространения, локальные папки или другие веб-серверы.

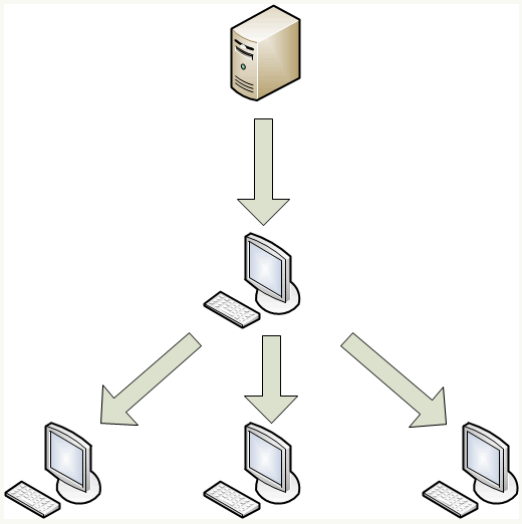
Вы можете поместить полученные обновления в локальную папку для обновления баз и модулей Kaspersky Endpoint Security на других компьютерах сети организации для уменьшения интернет-трафика.

Процедура получения обновлений будет организована следующим образом:

1. Один из компьютеров сети получает пакет обновлений Kaspersky Endpoint Security с серверов обновлений "Лаборатории Касперского" либо из другого источника обновлений. Вы помещаете полученные обновления в папку общего доступа.

   Примечание. Вы должны создать локальную папку с общим доступом заранее.

2. Другие компьютеры сети для получения обновлений обращаются к локальной папке с общим доступом, как к источнику обновлений.



Распространение обновлений через локальный компьютер

Если требуется, в окне **Обновление** измените параметры задачи обновления:

1. Если вы хотите отключить обновление модулей приложения, снимите флажок **Обновлять модули приложения**.
2. Если вы хотите изменить источники обновлений:
   a. Нажмите на кнопку **Параметры**.
      Откроется окно **Параметры: Обновление**.
   b. Установите флажки рядом с источниками обновлений, которые вы хотите использовать.
3. Если вы хотите указать другой источник обновлений, нажмите на кнопку **Добавить**.
   Откроется окно **Источник обновлений**.
   a. Укажите веб-адрес источника обновлений или путь к локальной или сетевой папке, которая является источником обновлений и нажмите **ОК**.
   b. Нажмите на кнопку **ОК**, чтобы сохранить изменения и закрыть окно **Параметры: Обновление**.

Проверка и быстрая проверка

По умолчанию Kaspersky Endpoint Security использует уровень безопасности **Рекомендованный**, запрашивает действие при обнаружении зараженного объекта по окончании проверки и проверяет следующие объекты:

- все съемные диски;
- все внутренние диски;
- все сетевые диски;
- память компьютера.

Примечание. Kaspersky Endpoint Security не проверяет файлы, расположенные в хранилищах OneDrive, iCloud и других облачных хранилищах. Исключите эти файлы из области проверки. В противном случае задача проверки может завершиться с ошибкой *Зараженный файл не удален*.

Если требуется, в окне **Проверка** измените параметры проверки:

1. Выберите один из предустановленных уровней безопасности или настройте параметры уровня безопасности вручную.
2. Укажите действие, которое Kaspersky Endpoint Security выполняет при обнаружении зараженного объекта.
3. Сформируйте область проверки.

Шаг 3. Определение способа выбора клиентских компьютеров, для которых будет создана задача

Примечание. Этот шаг не отображается для локальных или групповых задач.

В окне **Выбор устройств, которым будет назначена задача** выберите способ, который хотите использовать для выборки клиентских компьютеров:

- Если вы хотите выбрать из компьютеров, обнаруженных в сети Сервером администрирования, выберите вариант **Выбрать устройства, обнаруженные в сети Сервером администрирования**.
- Если вы хотите указать IP-адреса компьютеров вручную или импортировать IP-адреса компьютеров из файла, выберите вариант **Задать адреса устройств вручную или импортировать из списка**.
- Если вы хотите создать задачу для выборки устройств по предопределенному критерию, выберите вариант **Назначить задачу выборке устройств**.
- Если вы хотите выбрать компьютеры из указанной группы администрирования, выберите вариант **Назначить задачу группе администрирования**.

Шаг 4. Выбор клиентских компьютеров

Примечание. Этот шаг не отображается для локальных или групповых задач.

В открывшемся окне (**Выбор устройств**, **Выборка устройств** или **Выберите группу администрирования**, в зависимости от варианта, который вы выбрали на предыдущем шаге), выберите клиентские компьютеры, укажите IP-адреса компьютеров, укажите выборку компьютеров, или выберите группу администрирования, для которой будет создана задача.

Шаг 5. Настройка расписания запуска задачи

1. В окне **Настройка расписания запуска задачи** в раскрывающемся списке **Запуск по расписанию** выберите режим запуска задачи.
2. Если требуется, укажите дату и время запуска задачи, чтобы задача запустилась автоматически по установленному расписанию.
3. Если вы хотите запускать задачи, которые приложение не смогло запустить по расписанию (например, компьютер был выключен в установленное расписанием время), установите флажок **Запускать пропущенные задачи**.

   Kaspersky Endpoint Security запустит задачу, как только помеха, которая препятствует запуску задачи, будет устранена.
4. Если вы хотите, чтобы Kaspersky Security Center автоматически определял интервал между запусками задачи на разных компьютерах, установите флажок **Использовать автоматическое определение случайного интервала между запусками задачи**.

   Это позволяет снизить нагрузку на Сервер администрирования Kaspersky Security Center.
5. Если вы хотите установить интервал между запусками задачи на разных компьютерах вручную, установите флажок **Использовать случайную задержку запуска задачи в интервале (мин)** и укажите количество минут.

   Это позволяет снизить нагрузку на Сервер администрирования Kaspersky Security Center.

Шаг 6. Определение названия задачи

В окне **Определение названия задачи** в поле **Имя** введите название создаваемой задачи.

Шаг 7. Завершение создания задачи

В окне **Завершение создания задачи** выполните следующие действия:

1. Если вы хотите запустить задачу после завершения работы мастера, установите флажок **Запустить задачу после завершения работы мастера**.

2. Нажмите на кнопку **Готово** для завершения работы мастера.

Запуск и остановка задач вручную

Запуск и остановка задач по расписанию осуществляется автоматически в соответствии с расписанием. Тем не менее, вы можете запустить задачу вручную в любое время.

Примечание. Запуск задач на клиентском компьютере выполняется только в том случае, если запущен Агент администрирования. При остановке работы Агента администрирования выполнение всех запущенных задач прерывается.

Запуск и остановка задач вручную

1. Откройте список задач, в который входит нужная задача.

2. Выберите задачу, которую вы хотите запустить или остановить.

3. Запустите или остановите задачу одним из следующих способов:

   - По правой клавише мыши откройте контекстное меню задачи и выберите пункт **Запустить** или **Остановить**.

   - В рабочей области нажмите на кнопку **Запустить** или **Остановить**.

   - По правой клавише мыши откройте контекстное меню задачи и выберите пункт **Свойства**. В открывшемся окне нажмите на кнопку **Запустить** или **Остановить**.

Импорт и экспорт задач

Вы можете экспортировать параметры групповых задач и задач для произвольного набора компьютеров в файл.

Экспорт задачи

1. Выберите список задач, в который входит задача, которую вы хотите экспортировать:

- Выберите группу администрирования и откройте вкладку **Задачи**.
- В дереве консоли выберите папку **Задачи**.

2. По правой клавише мыши откройте контекстное меню задачи, которую вы хотите экспортировать, и выберите пункт **Все задачи** > **Экспорт**.
3. В окне **Сохранить как** укажите имя файла и папку, в которую он будет сохранен.
4. Нажмите на кнопку **Сохранить**.

Импорт задачи

1. Выберите список задач, в который вы хотите импортировать задачу:
   - Выберите группу администрирования и откройте вкладку **Задачи**.
   - В дереве консоли выберите папку **Задачи**.
2. Импортируйте задачу одним из следующих способов:
   - По правой клавише мыши откройте контекстное меню рабочей области и выберите пункт **Все задачи** > **Импортировать**.
   - Нажмите на кнопку **Импортировать задачу из файла**.
3. В окне **Открыть** укажите путь к файлу задачи, которую вы хотите импортировать.
4. Нажмите на кнопку **Открыть**.

Задача отобразится в списке задач.

Просмотр задач

Вы можете просматривать список задач, созданных для отдельного клиентского компьютера, компьютеров, входящих в группу администрирования, а также список всех нелокальных задач.

Просмотр списка задач для компьютеров, входящих в группу администрирования

1. Запустите Консоль администрирования Kaspersky Security Center.

2. Разверните узел **Сервер администрирования <Имя сервера>**.

3. В дереве консоли выберите папку **Управляемые устройства**.

4. Выберите группу администрирования, в которую входит клиентский компьютер.

5. В рабочей области выберите вкладку **Задачи**.

Отобразится список задач для компьютеров, входящих в выбранную группу администрирования.

Просмотр списка локальных задач

1. Запустите Консоль администрирования Kaspersky Security Center.

2. Разверните узел **Сервер администрирования <Имя сервера>**.

3. В дереве консоли выберите папку **Управляемые устройства**.

4. Выберите группу администрирования, в которую входит клиентский компьютер.

5. В рабочей области выберите вкладку **Устройства**.

6. Выберите компьютер в списке клиентских компьютеров.

7. Откройте окно **Свойства: <Название компьютера>** одним из следующих способов:

   - дважды щелкните по имени клиентского компьютера;
   - по правой клавише мыши откройте контекстное меню клиентского компьютера и выберите пункт **Свойства**.

8. В окне **Свойства:<Название компьютера>** выберите раздел **Задачи**.

В рабочей области справа отобразится список системных и пользовательских задач, созданных для выбранного клиентского компьютера.

Просмотр списка нелокальных задач

1. Запустите Консоль администрирования Kaspersky Security Center.

2. Разверните узел **Сервер администрирования <Имя сервера>**.

3. В дереве консоли выберите папку **Задачи**.

Отобразится список нелокальных задач, созданных для компьютеров, которые могут входить или не входить в группы администрирования.

Настройка параметров, зависящих от задачи

Просмотр параметров локальной задачи

1. Откройте список локальных задач.

2. Выберите задачу в списке и откройте параметры задачи одним из следующих способов:

   - дважды щелкните по названию задачи;

   - по правой кнопке мыши откройте контекстное меню задачи и выберите пункт **Свойства**.

Просмотр параметров групповой задачи

1. Откройте список групповых задач для группы администрирования.

2. Выберите задачу в списке и откройте параметры задачи одним из следующих способов:

   - дважды щелкните по названию задачи;

   - по правой кнопке мыши откройте контекстное меню задачи и выберите пункт **Свойства**;

   - в рабочей области нажмите на ссылку **Настроить параметры задачи**.

Просмотр параметров нелокальной задачи

1. Откройте список нелокальных задач.

2. Выберите задачу в списке и откройте параметры задачи одним из следующих способов:

   - дважды щелкните по названию задачи;
   - по правой кнопке мыши откройте контекстное меню задачи и выберите пункт **Свойства**;
   - в рабочей области нажмите на ссылку **Настроить параметры задачи**.

Подробную информацию о задачах вы можете найти в справке Kaspersky Security Center.

Для локальных задач, групповых задач и задач для произвольного набора компьютеров

Настройка параметров задачи Добавление ключа

1. Откройте окно с параметрами задачи **Добавление ключа**.
2. Выберите раздел **Активация приложения**.
3. Если требуется, добавьте другой ключ одним из следующих способов:

   - Если вы хотите выбрать ключ или код активации из списка кодов активации, добавленных в хранилище Kaspersky Security Center, выполните следующие действия:

     a. Выберите вариант **Ключ или код активации**.

     b. Нажмите на кнопку **Выбрать**.

     Откроется окно **Ключи и коды активации в хранилище Kaspersky Security Center**.

     c. Выберите ключ или код активации.

     d. Нажмите **OK**.

   - Если вы хотите добавить файл ключа, выполните следующие действия:

     a. Выберите вариант **Файл ключа**.

b. Нажмите на кнопку **Добавить**.

Откроется окно выбора файла.

c. Выберите файл ключа.

d. Нажмите на кнопку **Открыть**.

Примечание. Текущий ключ удаляется при добавлении другого ключа.

4. Если вы хотите добавить указанный ключ в качестве резервного, установите флажок **Добавить в качестве резервного ключа**.

   Резервный ключ становится активным по окончании срока годности текущего ключа.

   Примечание. Дата окончания срока годности резервного ключа должна быть позднее, чем дата окончания срока годности текущего ключа.

5. Сохраните внесенные изменения одним из следующих способов:

   - Нажмите на кнопку **Применить**, чтобы остаться в окне **Свойства: <Название задачи>** после сохранения внесенных изменений.
   - Нажмите на кнопку **ОК**, чтобы закрыть окно **Свойства: <Название задачи>** после сохранения внесенных изменений.

Настройка параметров задачи Быстрая проверка

1. Откройте окно с параметрами задачи **Быстрая проверка**.
2. Выберите раздел **Быстрая проверка**.
3. Если вы хотите изменить уровень безопасности, на котором Kaspersky Endpoint Security выполняет задачу Быстрая проверка, в блоке **Уровень безопасности**, выполните одно из следующих действий:

   - Выберите предустановленный уровень безопасности, перемещая ползунок по шкале.

     Вы можете выбрать один из следующих уровней безопасности:

- **Максимальная защита**. Kaspersky Endpoint Security осуществляет максимально полный контроль открываемых, сохраняемых и исполняемых файлов.

- **Рекомендованный**. Kaspersky Endpoint Security осуществляет контроль файлов с параметрами, рекомендованными специалистами "Лаборатории Касперского".

  Этот уровень безопасности установлен по умолчанию.

- **Максимальная скорость**. Kaspersky Endpoint Security осуществляет контроль минимального набора файлов. Вы можете выбрать этот уровень безопасности для работы с другими программами, требующими значительных ресурсов оперативной памяти.

- Настройте параметры безопасности вручную:

  a. Нажмите на кнопку **Параметры**.

  Откроется окно **Параметры: Проверка**.

  b. На вкладке **Основные** в блоке **Типы файлов** выберите типы файлов, которые Kaspersky Endpoint Security проверяет при выполнении задачи быстрой проверки.

  c. На вкладке **Основные** в блоке **Оптимизация** настройте параметры, которые определяют производительность проверки.

  d. На вкладке **Основные** в блоке **Составные файлы** выберите, какие составные файлы Kaspersky Endpoint Security анализирует на присутствие обнаруживаемых объектов.

  e. На вкладке **Дополнительно** в блоке **Дополнительные параметры** настройте использование технологии iSwift и запись информации об обнаруженных объектах в статистику приложения.

  f. На вкладке **Дополнительно** в блоке **Эвристический анализатор** настройте использование эвристического анализатора и выберите уровень защиты, который эвристический анализатор применяет при выполнении задач поиска вредоносного ПО.

  g. Нажмите на кнопку **ОК**, чтобы сохранить внесенные изменения и закрыть окно **Параметры: Проверка**.

  Уровень безопасности изменится на **Пользовательский**.

- Если вы хотите вернуть параметры по умолчанию, нажмите на кнопку **По умолчанию**.

Уровень безопасности изменится на **Рекомендованный**.

4. Если требуется, в блоке **Действие** выберите действие, которое Kaspersky Endpoint Security выполняет при обнаружении зараженного объекта.

5. Если вы хотите указать область проверки, в блоке **Область проверки** нажмите на кнопку **Параметры** и в открывшемся окне **Область проверки** выполните следующие действия:

   a. Если вы хотите, чтобы Kaspersky Endpoint Security проверял память компьютера, установите флажок **Память**.

   b. Если вы хотите, чтобы Kaspersky Endpoint Security проверял объекты автозапуска, установите флажок **Объекты входа**.

   c. Если вы хотите, чтобы Kaspersky Endpoint Security проверял другие дополнительные файлы или папки, нажмите на кнопку **Добавить** и укажите файл, папку или маску имени файла или папки.

   d. Нажмите на кнопку **ОК**, чтобы сохранить внесенные изменения и закрыть окно **Область проверки**.

6. Сохраните внесенные изменения одним из следующих способов:

   - Нажмите на кнопку **Применить**, чтобы остаться в окне **Свойства: <Название задачи>** после сохранения внесенных изменений.

   - Нажмите на кнопку **ОК**, чтобы закрыть окно **Свойства: <Название задачи>** после сохранения внесенных изменений.

Настройка параметров задачи Проверка

1. Откройте окно с параметрами задачи **Проверка**.

2. Выберите раздел **Проверка**.

3. Если вы хотите изменить уровень безопасности, на котором Kaspersky Endpoint Security выполняет задачу Проверка, в блоке **Уровень безопасности**, выполните одно из следующих действий:

   - Выберите предустановленный уровень безопасности, перемещая ползунок по шкале.

     Вы можете выбрать один из следующих уровней безопасности:

- **Максимальная защита**. Kaspersky Endpoint Security осуществляет максимально полный контроль открываемых, сохраняемых и исполняемых файлов.

- **Рекомендованный**. Kaspersky Endpoint Security осуществляет контроль файлов с параметрами, рекомендованными специалистами "Лаборатории Касперского".

  Этот уровень безопасности установлен по умолчанию.

- **Максимальная скорость**. Kaspersky Endpoint Security осуществляет контроль минимального набора файлов. Вы можете выбрать этот уровень безопасности для работы с другими программами, требующими значительных ресурсов оперативной памяти.

- Настройте параметры безопасности вручную:

  a. Нажмите на кнопку **Параметры**.

  Откроется окно **Параметры: Проверка**.

  b. На вкладке **Основные** в блоке **Типы файлов** выберите типы файлов, которые Kaspersky Endpoint Security проверяет при выполнении задачи проверки.

  c. На вкладке **Основные** в блоке **Оптимизация** настройте параметры, которые определяют производительность проверки.

  d. На вкладке **Основные** в блоке **Составные файлы** выберите, какие составные файлы Kaspersky Endpoint Security анализирует на присутствие обнаруживаемых объектов.

  e. На вкладке **Дополнительно** в блоке **Дополнительные параметры** настройте использование технологии iSwift и запись информации об обнаруженных объектах в статистику приложения.

  f. На вкладке **Дополнительно** в блоке **Эвристический анализатор** настройте использование эвристического анализатора и выберите уровень защиты, который эвристический анализатор применяет при выполнении задач поиска вредоносного ПО.

  g. Нажмите на кнопку **ОК**, чтобы сохранить внесенные изменения и закрыть окно **Параметры: Проверка**.

  Уровень безопасности изменится на **Пользовательский**.

- Если вы хотите вернуть параметры по умолчанию, нажмите на кнопку **По умолчанию**.

  Уровень безопасности изменится на **Рекомендованный**.

4. Если требуется, в блоке **Действие** выберите действие, которое Kaspersky Endpoint Security выполняет при обнаружении зараженного объекта.

5. Если вы хотите указать область проверки, в блоке **Область проверки** нажмите на кнопку **Параметры** и в открывшемся окне **Область проверки** выполните следующие действия:

    a. Если вы хотите, чтобы Kaspersky Endpoint Security проверял все съемные диски, установите флажок **Все съемные диски**.

    b. Если вы хотите, чтобы Kaspersky Endpoint Security проверял все внутренние диски, установите флажок **Все внутренние диски**.

    c. Если вы хотите, чтобы Kaspersky Endpoint Security проверял все сетевые диски, установите флажок **Все сетевые диски**.

    d. Если вы хотите, чтобы Kaspersky Endpoint Security проверял память компьютера, установите флажок **Память**.

    e. Если вы хотите, чтобы Kaspersky Endpoint Security проверял объекты автозапуска, установите флажок **Объекты входа**.

    f. Если вы хотите, чтобы Kaspersky Endpoint Security проверял другие файлы или папки, нажмите на кнопку **Добавить** и укажите файл, папку или маску имени файла или папки.

    g. Нажмите на кнопку **ОК**, чтобы сохранить внесенные изменения и закрыть окно **Область проверки**.

6. Сохраните внесенные изменения одним из следующих способов:

    - Нажмите на кнопку **Применить**, чтобы остаться в окне **Свойства: <Название задачи>** после сохранения внесенных изменений.

    - Нажмите на кнопку **ОК**, чтобы закрыть окно **Свойства: <Название задачи>** после сохранения внесенных изменений.

Настройка параметров задачи Обновление

1. Откройте окно с параметрами задачи **Обновление**.

2. Выберите раздел **Обновление**.

3. Если вы хотите, чтобы Kaspersky Endpoint Security обновлял модули приложения вместе с базами приложения, установите флажок **Обновлять модули приложения**.

4. Если вы хотите выбрать источник обновлений, выполните следующие действия:

   a. Нажмите на кнопку **Параметры**.

      Откроется окно **Параметры: Обновление**.

   b. Укажите источник обновлений одним из следующих способов:

      - Если вы хотите, чтобы приложение загружало обновления с Сервера администрирования, установите флажок **Kaspersky Security Center**.
      - Если вы хотите, чтобы приложение загружало обновления с серверов обновлений "Лаборатории Касперского", установите флажок **Серверы обновлений «Лаборатории Касперского»**.
      - Если вы хотите указать другой источник обновлений, нажмите на кнопку **Добавить** и в открывшемся окне введите путь к источнику обновлений.

        По умолчанию Kaspersky Endpoint Security загружает обновления с серверов обновлений "Лаборатории Касперского".

   c. Нажмите на кнопку **OK**, чтобы сохранить изменения и закрыть окно **Параметры: Обновление**.

5. Сохраните внесенные изменения одним из следующих способов:

   - Нажмите на кнопку **Применить**, чтобы остаться в окне **Свойства: <Название задачи>** после сохранения внесенных изменений.
   - Нажмите на кнопку **OK**, чтобы закрыть окно **Свойства: <Название задачи>** после сохранения внесенных изменений.

Только для локальных задач

Настройка параметров задачи Защита от файловых угроз

1. Откройте список локальных задач для клиентского компьютера.

2. В списке локальных задач выберите задачу Защита от файловых угроз и откройте ее свойства одним из следующих способов:

- дважды щелкните по названию задачи;
- по правой кнопке мыши откройте контекстное меню задачи и выберите пункт **Свойства**;
- нажмите на кнопку **Свойства**.

3. Выберите раздел **Защита от файловых угроз**.

4. Если требуется, настройте следующие параметры:

- Включите или выключите Защиту от файловых угроз на клиентском компьютере.
- Если вы хотите выбрать один из предустановленных уровней безопасности, в блоке **Уровень безопасности** переместите ползунок по шкале.
- Если вы хотите настроить параметры безопасности вручную, нажмите на кнопку **Параметры** и в открывшемся окне **Параметры: Защита от файловых угроз** выполните следующие действия:

  a. На вкладке **Основные** в блоке **Типы файлов** выберите типы файлов, которые Kaspersky Endpoint Security проверяет при открытии, исполнении и сохранении.

  b. На вкладке **Основные** в блоке **Оптимизация** настройте параметры, которые определяют производительность проверки, выберите технологию проверки и выберите, будет ли Kaspersky Endpoint Security пропускать проверку системного тома "только для чтения" на клиентских компьютерах.

  c. На вкладке **Основные** в блоке **Составные файлы** выберите, какие составные файлы нужно проверять на присутствие обнаруживаемых объектов и установите ограничение на проверку больших объектов.

  d. На вкладке **Область защиты** укажите файлы или папки, которые проверяет задача Защита от файловых угроз.

  По умолчанию включена проверка всех объектов, расположенных на съемных, внутренних и сетевых дисках, подключенных к клиентскому компьютеру. Вы можете добавить объект в область защиты, изменить объект списка, временно отключить проверку объекта списка или удалить объект из списка.

  e. На вкладке **Дополнительно** в блоке **Режим проверки** выберите режим работы Защиты от файловых угроз.

  f. На вкладке **Дополнительно** в блоке **Приостановка задачи** включите или выключите приостановку Защиты от файловых угроз по расписанию и

настройте параметры автоматической приостановки выполнения задач по расписанию.

g. На вкладке **Дополнительно** в блоке **Эвристический анализатор** настройте использование эвристического анализатора для Защиты от файловых угроз.

h. Нажмите на кнопку **ОК**, чтобы сохранить внесенные изменения и закрыть окно **Параметры: Защита от файловых угроз**.

- В блоке **Если обнаружен вредоносный объект** выберите действие, которое Защита от файловых угроз выполняет при обнаружении зараженного объекта.

5. Сохраните внесенные изменения одним из следующих способов:

- Нажмите на кнопку **Применить**, чтобы остаться в окне **Свойства: Защита от файловых угроз** после сохранения внесенных изменений.
- Нажмите на кнопку **ОК**, чтобы закрыть окно **Свойства: Защита от файловых угроз** после сохранения внесенных изменений.

Настройка параметров задачи Защита от веб-угроз

1. Откройте список локальных задач для клиентского компьютера.
2. В списке локальных задач выберите задачу Защита от веб-угроз и откройте ее свойства одним из следующих способов:
   - дважды щелкните по названию задачи;
   - по правой кнопке мыши откройте контекстное меню задачи и выберите пункт **Свойства**;
   - нажмите на кнопку **Свойства**.
3. Выберите раздел **Защита от веб-угроз**.
4. Если требуется, настройте следующие параметры:
   - Включите или выключите Защиту от веб-угроз на клиентском компьютере.
   - Если вы хотите выбрать один из предустановленных уровней безопасности, в блоке **Уровень безопасности** переместите ползунок по шкале.

- Если вы хотите настроить параметры безопасности вручную, нажмите на кнопку **Параметры** и в открывшемся окне **Параметры: Защита от веб-угроз** выполните следующие действия:

  a. На вкладке **Основные** в блоке **Режим проверки** включите или выключите проверку веб-адресов по базе вредоносных веб-адресов.

  b. На вкладке **Основные** в блоке **Параметры антифишинга** включите или выключите проверку веб-адресов по базе фишинговых веб-адресов.

  c. На вкладке **Основные** в блоке **Параметры антифишинга** включите или выключите использование эвристического анализатора для обнаружения фишинговых ссылок.

  d. На вкладке **Доверенные веб-адреса** включите или выключите проверку веб-трафика с доверенных веб-адресов и создайте или измените список доверенных веб-адресов.

  e. Нажмите на кнопку **OK**, чтобы сохранить внесенные изменения и закрыть окно **Параметры: Защита от веб-угроз**.

5. В блоке **Если обнаружен вредоносный объект** выберите действие, которое Защита от веб-угроз выполняет при обнаружении опасного объекта веб-трафика.

6. Сохраните внесенные изменения одним из следующих способов:

   - Нажмите на кнопку **Применить**, чтобы остаться в окне **Свойства: Защита от веб-угроз** после сохранения внесенных изменений.

   - Нажмите на кнопку **OK**, чтобы закрыть окно **Свойства: Защита от веб-угроз** после сохранения внесенных изменений.

Настройка параметров задачи Быстрая проверка

1. Откройте список локальных задач для клиентского компьютера.

2. В списке локальных задач выберите задачу Быстрая проверка и откройте ее свойства одним из следующих способов:

   - дважды щелкните по названию задачи;

   - по правой кнопке мыши откройте контекстное меню задачи и выберите пункт **Свойства**;

- нажмите на кнопку **Свойства**.

3. Выберите раздел **Проверка**.

4. Если требуется, настройте следующие параметры:

   - Если вы хотите выбрать один из предустановленных уровней безопасности, в блоке **Уровень безопасности** переместите ползунок по шкале.

   - Если вы хотите настроить параметры безопасности вручную, нажмите на кнопку **Параметры** и в открывшемся окне **Параметры: Проверка** выполните следующие действия:

     a. На вкладке **Основные** в блоке **Типы файлов** выберите типы файлов, которые Kaspersky Endpoint Security проверяет.

     b. На вкладке **Основные** в блоке **Оптимизация** настройте параметры, которые определяют производительность проверки.

     c. На вкладке **Основные** в блоке **Составные файлы** выберите, какие составные файлы Kaspersky Endpoint Security проверяет.

     d. На вкладке **Дополнительно** в блоке **Дополнительные параметры** настройте использование технологии iSwift и запись информации об обнаруженных объектах в статистику приложения.

     e. На вкладке **Дополнительно** в блоке **Эвристический анализатор** настройте использование эвристического анализатора и выберите уровень защиты, который применяет эвристический анализатор.

     f. Нажмите на кнопку **ОК**, чтобы сохранить внесенные изменения и закрыть окно **Параметры: Проверка**.

   - В блоке **Действие** выберите действие, которое Kaspersky Endpoint Security выполнит при обнаружении зараженного объекта.

   - Если вы хотите указать область проверки, в блоке **Область проверки** нажмите на кнопку **Параметры** и в открывшемся окне **Область проверки** выполните следующие действия:

     - Если вы хотите, чтобы Kaspersky Endpoint Security проверял объекты из списка по умолчанию, установите флажок рядом с нужным объектом.

     - Если вы хотите, чтобы Kaspersky Endpoint Security проверял другие файлы или папки, нажмите на кнопку **Добавить** и укажите файл, папку или маску имени файла или папки.

- Нажмите на кнопку **OK**, чтобы сохранить внесенные изменения и закрыть окно **Область проверки**.

5. Сохраните внесенные изменения одним из следующих способов:

   - Нажмите на кнопку **Применить**, чтобы остаться в окне **Свойства: Быстрая проверка** после сохранения внесенных изменений.

   - Нажмите на кнопку **OK**, чтобы закрыть окно **Свойства: Быстрая проверка** после сохранения внесенных изменений.

Настройка параметров задачи Полная проверка

1. Откройте список локальных задач для клиентского компьютера.

2. В списке локальных задач выберите задачу Полная проверка и откройте ее свойства одним из следующих способов:

   - дважды щелкните по названию задачи;

   - по правой кнопке мыши откройте контекстное меню задачи и выберите пункт **Свойства**;

   - нажмите на кнопку **Свойства**.

3. Выберите раздел **Проверка**.

4. Если требуется, настройте следующие параметры:

   - Если вы хотите выбрать один из предустановленных уровней безопасности, в блоке **Уровень безопасности** переместите ползунок по шкале.

   - Если вы хотите настроить параметры безопасности вручную, нажмите на кнопку **Параметры** и в открывшемся окне **Параметры: Проверка** выполните следующие действия:

     a. На вкладке **Основные** в блоке **Типы файлов** выберите типы файлов, которые Kaspersky Endpoint Security проверяет.

     b. На вкладке **Основные** в блоке **Оптимизация** настройте параметры, которые определяют производительность проверки.

     c. На вкладке **Основные** в блоке **Составные файлы** выберите, какие составные файлы Kaspersky Endpoint Security проверяет.

d. На вкладке **Дополнительно** в блоке **Дополнительные параметры** настройте использование технологии iSwift и запись информации об обнаруженных объектах в статистику приложения.

e. На вкладке **Дополнительно** в блоке **Эвристический анализатор** настройте использование эвристического анализатора и выберите уровень защиты, который применяет эвристический анализатор.

f. Нажмите на кнопку **OK**, чтобы сохранить внесенные изменения и закрыть окно **Параметры: Проверка**.

- В блоке **Действие** выберите действие, которое Kaspersky Endpoint Security выполнит при обнаружении зараженного объекта.

- Если вы хотите указать область проверки, в блоке **Область проверки** нажмите на кнопку **Параметры** и в открывшемся окне **Область проверки** выполните следующие действия:

  - Если вы хотите, чтобы Kaspersky Endpoint Security проверял объекты из списка по умолчанию, установите флажок рядом с нужным объектом.

  - Если вы хотите, чтобы Kaspersky Endpoint Security проверял другие файлы или папки, нажмите на кнопку **Добавить** и укажите файл, папку или маску имени файла или папки.

  - Нажмите на кнопку **OK**, чтобы сохранить внесенные изменения и закрыть окно **Область проверки**.

5. Сохраните внесенные изменения одним из следующих способов:

   - Нажмите на кнопку **Применить**, чтобы остаться в окне **Свойства: Полная проверка** после сохранения внесенных изменений.

   - Нажмите на кнопку **OK**, чтобы закрыть окно **Свойства: Полная проверка** после сохранения внесенных изменений.

Настройка параметров задачи Выборочная проверка

1. Откройте список локальных задач для клиентского компьютера.

2. В списке локальных задач выберите задачу Выборочная проверка и откройте ее свойства одним из следующих способов:

   - дважды щелкните по названию задачи;

- по правой кнопке мыши откройте контекстное меню задачи и выберите пункт **Свойства**;

- нажмите на кнопку **Свойства**.

3. Выберите раздел **Проверка**.

4. Если требуется, настройте следующие параметры:

- Если вы хотите выбрать один из предустановленных уровней безопасности, в блоке **Уровень безопасности** переместите ползунок по шкале.

- Если вы хотите настроить параметры безопасности вручную, нажмите на кнопку **Параметры** и в открывшемся окне **Параметры: Проверка** выполните следующие действия:

  a. На вкладке **Основные** в блоке **Типы файлов** выберите типы файлов, которые Kaspersky Endpoint Security проверяет.

  b. На вкладке **Основные** в блоке **Оптимизация** настройте параметры, которые определяют производительность проверки.

  c. На вкладке **Основные** в блоке **Составные файлы** выберите, какие составные файлы Kaspersky Endpoint Security проверяет.

  d. На вкладке **Дополнительно** в блоке **Дополнительные параметры** настройте использование технологии iSwift и запись информации об обнаруженных объектах в статистику приложения.

  e. На вкладке **Дополнительно** в блоке **Эвристический анализатор** настройте использование эвристического анализатора и выберите уровень защиты, который применяет эвристический анализатор.

  f. Нажмите на кнопку **ОК**, чтобы сохранить внесенные изменения и закрыть окно **Параметры: Проверка**.

- В блоке **Действие** выберите действие, которое Kaspersky Endpoint Security выполнит при обнаружении зараженного объекта.

- Если вы хотите указать область проверки, в блоке **Область проверки** нажмите на кнопку **Параметры** и в открывшемся окне **Область проверки** выполните следующие действия:

  - Нажмите на кнопку **Добавить** и укажите файл, папку или имя маски файла или папки.

- Нажмите на кнопку **OK**, чтобы сохранить внесенные изменения и закрыть окно **Область проверки**.

5. Сохраните внесенные изменения одним из следующих способов:

   - Нажмите на кнопку **Применить**, чтобы остаться в окне **Свойства: Выборочная проверка** после сохранения внесенных изменений.

   - Нажмите на кнопку **OK**, чтобы закрыть окно **Свойства: Выборочная проверка** после сохранения внесенных изменений.

Настройка параметров задачи Защита от сетевых угроз

1. Откройте список локальных задач для клиентского компьютера.

2. В списке локальных задач выберите задачу Защита от сетевых угроз и откройте ее свойства одним из следующих способов:

   - дважды щелкните по названию задачи;

   - по правой кнопке мыши откройте контекстное меню задачи и выберите пункт **Свойства**;

   - нажмите на кнопку **Свойства**.

3. Выберите раздел **Защита от сетевых угроз**.

4. Если требуется, настройте следующие параметры:

   - Включите или выключите Защиту от сетевых угроз на клиентском компьютере.

   - В блоке **Параметры Защиты от сетевых угроз** установите или снимите флажок **Блокировать атакующие компьютеры на <значение> мин** и укажите значение.

   - Вы также можете указать IP-адреса компьютеров, сетевая активность которых не будет блокироваться. Для этого выполните следующие действия:

     a. Нажмите на кнопку **Исключения**.

        Откроется окно **Исключения**.

     b. Нажмите на кнопку **Добавить**.

        Откроется окно **IP-адрес**.

c. Укажите IP-адрес компьютера, сетевая активность которого не будет блокироваться и нажмите на кнопку **OK**.

d. Нажмите на кнопку **OK**, чтобы сохранить внесенные изменения и закрыть окно **Исключения**.

5. Сохраните внесенные изменения одним из следующих способов:

- Нажмите на кнопку **Применить**, чтобы остаться в окне **Свойства: Защита от сетевых угроз** после сохранения внесенных изменений.
- Нажмите на кнопку **OK**, чтобы сохранить закрыть окно **Свойства: Защита от сетевых угроз** после сохранения внесенных изменений.

Создание политик и управление ими

В этом разделе содержится информация о создании и настройке политик для Kaspersky Endpoint Security.

Политика определяет параметры работы приложения и доступ к настройке приложения, установленного на компьютерах группы администрирования. Для каждого приложения требуется создать свою политику. Вы можете создать несколько различных политик для приложений, установленных на компьютерах в каждой группе администрирования, но в пределах группы администрирования только одна политика может применяться единовременно к каждому приложению.

Примечание. При создании и настройке политики вы можете разрешить или запретить изменение каждой группы параметров в политиках с помощью кнопок и .

Над пользовательскими политиками вы можете выполнять следующие действия:

- создавать политики;
- настраивать параметры политик;
- копировать и переносить политики из одной группы в другую;
- удалять политики;
- изменять статус политик;
- экспортировать политики в файл;

- импортировать политики из файла.

Подробную информацию о политиках Kaspersky Security Center вы можете найти в справке Kaspersky Security Center.

Создание политики

Этот раздел содержит инструкции по запуску шагов мастера создания политики и описание шагов мастера создания политики.

Создание политики из папки группы администрирования

1. Запустите Консоль администрирования Kaspersky Security Center.
2. Разверните узел **Сервер администрирования <Имя сервера>**.
3. В дереве консоли выберите папку **Управляемые устройства**.
4. Выберите группу администрирования, в которую входит клиентский компьютер.
5. В рабочей области выберите вкладку **Политики** и нажмите на кнопку **Новая политика**.

   Запустится мастер создания политики.
6. Следуйте шагам мастера создания политики, чтобы создать политику.

Создание политики из папки Политики

1. Запустите Консоль администрирования Kaspersky Security Center.
2. Разверните узел **Сервер администрирования <Имя сервера>**.
3. В дереве консоли выберите папку **Политики**.
4. В рабочей области нажмите на кнопку **Новая политика**.

   Запустится мастер создания политики.
5. Следуйте шагам мастера создания политики, чтобы создать политику.

Чтобы перейти к следующему шагу мастера, нажмите на кнопку **Далее**. Чтобы вернуться к предыдущему шагу мастера, нажмите на кнопку . Чтобы завершить работу мастера на любом шаге, нажмите на кнопку **Отмена**.

Примечание. Вид кнопок может отличаться в зависимости от используемой версии Windows.

Шаг 1. Выбор программы

В окне **Выбор программы для создания групповой политики** в списке программ выберите **Kaspersky Endpoint Security для Mac (12.2)**.

Шаг 2. Ввод имени политики

1. В окне **Введите название для групповой политики** в поле **Имя** укажите имя создаваемой политики. Имя не может содержать символы " * < : > ? \ |.
2. Установите флажок **Использовать параметры политики для предыдущей версии программы**, если вы хотите импортировать параметры существующей политики Kaspersky Endpoint Security в новую политику.

Шаг 3. Настройка параметров защиты

Если требуется, в окне **Защита** настройте следующие параметры:

- Настройте параметры защиты операционной системы клиентского компьютера.
- Сформируйте Доверенную зону.

  Вы можете создать список объектов, которые Kaspersky Endpoint Security не проверяет и не контролирует.
- Настройте Доверенные приложения.

  Вы можете создать список приложений, сетевую и файловую активность которых Kaspersky Endpoint Security не контролирует.
- Выберите категории обнаруживаемых объектов.
- Выключите или включите запуск задач по расписанию при работе компьютера от аккумулятора.

- Ограничивать сканирующий поток в использовании CPU.

Шаг 4. Настройка параметров Защиты от файловых угроз

Если требуется, в окне **Защита от файловых угроз** выполните следующие действия:

- Включите или выключите Защиту от файловых угроз.

  По умолчанию Защита от файловых угроз включена.

- Выберите уровень безопасности.

  По умолчанию выбран уровень безопасности, рекомендованный специалистами "Лаборатории Касперского".

- Настройте параметры Защиты от файловых угроз.

- Выберите действие, которое приложение выполнит при обнаружении вредоносного объекта.

Шаг 5. Настройка параметров Защиты от веб-угроз

Если требуется, в окне **Защита от веб-угроз** выполните следующие действия:

- Включите или выключите Защиту от веб-угроз.

  По умолчанию Защита от веб-угроз включена.

- Выберите уровень безопасности.

  По умолчанию выбран уровень безопасности, рекомендованный специалистами "Лаборатории Касперского".

- Настройте параметры Защиты от веб-угроз.

- Выберите действие, которое приложение выполнит при обнаружении опасного объекта веб-трафика.

Шаг 6. Настройка параметров Защиты от сетевых угроз

Если требуется, в окне **Защита от сетевых угроз** выполните следующие действия:

- Включите или выключите Защиту от сетевых угроз.

  По умолчанию Защита от сетевых угроз включена.

- Настройте параметры Защиты от сетевых угроз.
- Создайте или измените список IP-адресов удаленных компьютеров, сетевую активность которых Kaspersky Endpoint Security не блокирует никогда.

Шаг 7. Настройка параметров обновления

Если требуется, в окне **Обновление** выполните следующие действия:

- Включите или выключите обновление модулей приложения.
- Укажите источники обновлений.

Шаг 8. Настройка параметров использования KSN

Если требуется, в окне **Kaspersky Security Network** выполните следующие действия:

- Ознакомьтесь с полным текстом Положения о Kaspersky Security Network, нажав на кнопку **Положение о KSN**.
- Просмотрите информацию об инфраструктуре KSN, которую предоставляет Kaspersky Security Center.
- Включите или выключите использование Kaspersky Security Network.
- Включите или выключите расширенный режим использования KSN.
- Включите или выключите использование KSN-прокси.
- Включите или выключите использование серверов "Лаборатории Касперского", если KSN-прокси недоступен.

Примечание. Использование Kaspersky Security Network и KSN-прокси на удаленных компьютерах доступно только если Сервер администрирования Kaspersky Security Center используется в качестве прокси-сервера. Подробную информацию о настройке Сервера администрирования вы можете найти в справке Kaspersky Security Center.

Если Kaspersky Security Center использует глобальный KSN и вы присоединились к Kaspersky Security Network в параметрах политики, статистика Kaspersky Endpoint Security с клиентских компьютеров, к которым была применена политика, автоматически отправляется в "Лабораторию Касперского" для улучшения защиты этих компьютеров.

Примечание. "Лаборатория Касперского" не осуществляет получение, обработку и хранение любых персональных данных без вашего явного согласия.

Данные, предоставляемые в "Лабораторию Касперского" при использовании Kaspersky Security Network в глобальном KSN

Если флажок **Я принимаю условия использования Kaspersky Security Network** установлен, а флажок **Включить расширенный режим работы KSN** снят, Kaspersky Endpoint Security отправляет в "Лабораторию Касперского" следующие данные:

- Информация об используемой лицензии: тип лицензии и срок ее действия, количество дней до истечения срока действия лицензии, идентификатор партнера, у которого приобретена лицензия, идентификатор регионального центра активации, контрольная сумма кода активации, хеш-сумма тела тикета, рассчитанная по алгоритму SHA1, дата и время создания лицензионного тикета, идентификатор информации о лицензии, идентификатор лицензионного тикета, идентификатор последовательности лицензионного тикета, уникальный идентификатор компьютера пользователя, дата начала и окончания периода валидности лицензионного тикета, текущее состояние лицензионного тикета, версия заголовка тикета, версия лицензии, идентификатор сертификата подписи заголовка тикета, контрольная сумма файла ключа, серийный номер подписчика заголовка тикета, токен авторизации.

- Полная версия установленного ПО;

тип установленного ПО; идентификатор обновления ПО; идентификатор службы репутации; идентификатор типа протокола; идентификатор регионального центра активации; версия списка отозванных заключений службы ПО; идентификатор сработавшей записи в антивирусных базах ПО; временная метка сработавшей записи в антивирусных базах ПО; тип сработавшей записи в антивирусных базах ПО; уникальный идентификатор установки ПО на компьютере; дата активации лицензии; дата окончания срока действия лицензии; идентификатор лицензии; статус лицензии, по которой используется ПО; тип контрольной суммы обрабатываемого объекта; название обнаруженной вредоносной программы или легальной программы, которая может быть использована для нанесения вреда устройству или данным пользователя; контрольная сумма обрабатываемого объекта; контрольная сумма кода активации ПО; полная версия ПО; уникальный идентификатор устройства; идентификатор ПО; контрольная сумма файла ключа, которым активировано ПО; идентификатор информационной модели, примененной при предоставлении лицензии на использование ПО; идентификатор сертификата, которым подписан заголовок лицензионного тикета ПО; дата и время создания лицензионного тикета ПО; контрольная сумма лицензионного тикета ПО; версия лицензионного тикета ПО; версия кода активации ПО; формат данных в запросе к инфраструктуре Правообладателя; идентификатор тикета текущей лицензии; идентификатор компонента ПО; результат действий, выполненных ПО; код ошибки; адрес веб-службы, на который осуществлялось обрабатываемое обращение (веб-адрес, IP); номер порта; веб-адрес источника запроса к веб-службе (referrer); публичный ключ сертификата; отпечаток цифрового сертификата проверяемого объекта и алгоритм хеширования.

Если флажки **Я принимаю условия использования Kaspersky Security Network** и **Включить расширенный режим работы KSN** установлены, Kaspersky Endpoint Security отправляет в "Лабораторию Касперского" следующие данные:

- Информация о версиях установленной на компьютере операционной системы (ОС) и установленных пакетов обновлений, версия и контрольные суммы (MD5, SHA2-256, SHA1) файла ядра ОС, параметры режима работы ОС. версия ОС, номер сборки ОС, номер обновления ОС, редакция ОС, расширенная информация о редакции ОС; версия пакета обновления ОС; дата и время запуска ОС; время задержки обработки события о совершении действия в ОС в подсистеме поведенческого анализа; количество задержанных событий текущего типа, совершенных в ОС; время задержки обработки события о совершении действия в ОС в подсистеме проактивной защиты; количество обработанных событий, совершенных в ОС; количество обработанных синхронных событий, совершенных в ОС; суммарная задержка всех событий текущего типа, совершенных в ОС; время задержки обработки события о совершении действия в ОС в подсистеме постоянного хранения событий; суммарная задержка всех событий, совершенных в ОС; количество ожидающих

синхронных событий, совершенных в ОС; дата и время получения события о совершении действия в ОС.

- Информация о последней неуспешной перезагрузке ОС: количество неуспешных перезагрузок.

- Информация об установленном ПО Правообладателя и состоянии антивирусной защиты компьютера: идентификатор установки ПО (PCID); версия записи в базе данных ПО; уникальный идентификатор установки программы на компьютере, тип программы, идентификатор типа программы, полная версия установленной программы, идентификатор версии настроек программы, идентификатор типа компьютера, уникальный идентификатор компьютера, на котором установлена программа, уникальный идентификатор пользователя в службах Правообладателя, язык локали и ее рабочее состояние, версия установленных компонентов ПО и их рабочее состояние, версия протокола, который используется для подключения к службам Правообладателя; полная версия установленного ПО; тип установленного ПО; идентификатор обновления ПО; идентификатор службы репутации; идентификатор типа протокола; идентификатор регионального центра активации; версия списка отозванных заключений службы ПО; идентификатор сработавшей записи в антивирусных базах ПО; временная метка сработавшей записи в антивирусных базах ПО; тип сработавшей записи в антивирусных базах ПО; уникальный идентификатор установки ПО на компьютере; дата активации лицензии; дата окончания срока действия лицензии; идентификатор лицензии; статус лицензии, по которой используется ПО; тип контрольной суммы обрабатываемого объекта; название обнаруженной вредоносной программы или легальной программы, которая может быть использована для нанесения вреда устройству или данным пользователя; контрольная сумма обрабатываемого объекта; контрольная сумма кода активации ПО; полная версия ПО; идентификатор ПО; контрольная сумма файла ключа, которым активировано ПО; идентификатор информационной модели, примененной при предоставлении лицензии на использование ПО; идентификатор сертификата, которым подписан заголовок лицензионного тикета ПО; дата и время создания лицензионного тикета ПО; контрольная сумма лицензионного тикета ПО; версия лицензионного тикета ПО; версия кода активации ПО; формат данных в запросе к инфраструктуре Правообладателя; идентификатор тикета текущей лицензии; идентификатор компонента ПО; результат действий, выполненных ПО; код ошибки; адрес веб-службы, на который осуществлялось обрабатываемое обращение (веб-адрес, IP); номер порта; веб-адрес источника запроса к веб-службе (referrer); количество циклов обновления и применения антивирусных баз; дата и время последнего обновления и применения антивирусных баз; дата и время выпуска баз ПО; версия компонента ПО; идентификатор обновления ПО; тип установленного ПО; дата и время запуска компонента мониторинг активности; дата и время установки ПО; вероятность отправки статистики компонентом мониторинг активности; код события, обрабатываемого компонентом мониторинг активности дольше

стандартного времени обработки; время обработки события в базах, обработка которого компонентом мониторинг активности длилась дольше стандартного времени; максимально допустимое время обработки события компонентом мониторинг активности; время обработки события, обработка которого компонентом мониторинг активности длилась дольше стандартного времени; общее количество событий, обработка которых компонентом мониторинг активности длилась дольше стандартного времени.

- Данные обо всех обрабатываемых объектах и действиях: заключение ПО по обрабатываемому объекту; код каталога файлов; размер обрабатываемого объекта; контрольная сумма (SHA256) обрабатываемого объекта; номер обнаруженного ПО в контексте компонента мониторинг активности; дата и время обнаружения стороннего ПО компонентом мониторинг активности; характеристики обнаружения; идентификатор сработавшей записи в антивирусных базах ПО; причина обнаружения стороннего ПО компонентом мониторинг активности; контрольная сумма (MD5) обрабатываемого объекта; результат проверки подписи модуля, целостность которого проверяется ПО; имя обрабатываемого объекта; тип сработавшей записи в антивирусных базах ПО; путь к обрабатываемому объекту; имя проверяемого объекта; дата и время проверки; URL-адрес и Referrer, по которому он был загружен; размер проверяемых файлов и пути к ним; признак нахождения в архиве; дата и время создания файла; имя, размер и контрольные суммы (MD5, SHA2-256) упаковщика (если файл был упакован); энтропия файла; тип файла; код типа файла; признак исполняемого файла, идентификатор исполняемого файла и формат исполняемого файла; контрольная сумма объекта (MD5, SHA2-256); тип и значение дополнительной контрольной суммы объекта; данные о ЭЦП (сертификате) объекта: данные об издателе сертификата, количество запусков объекта с момента последней отправки статистики, идентификатор задачи проверки, способ получения информации о репутации объекта, значение фильтра target, технические характеристики по применяемым технологиям обнаружения; путь к обрабатываемому объекту; код каталога файлов.

- Для исполняемых файлов: энтропия разделов файла, признак проверки репутации или подписи файла, название, тип, идентификатор типа, контрольная сумма (MD5) и размер приложения, загруженного проверяемым объектом, путь к приложению и пути к шаблонам, признак нахождения в списке автозапуска, дата записи, список атрибутов, название упаковщика, информация о цифровой подписи приложения: издатель сертификата, название отправляемого файла в формате MIME, дата и время сборки файла.

- Информация о запускаемых программах и их модулях: контрольные суммы запускаемых файлов (MD5, SHA2-256), размер, атрибуты, дата создания, имя упаковщика (если файл был упакован), имена файлов, данные о запущенных в системе процессах (идентификатор процесса в системе (PID), имя процесса, данные об учетной записи, от которой запущен процесс, приложении и команде, запустившей процесс, полный путь к файлам процесса и командная

строка запуска, описание приложения, к которому относится процесс (название приложения и данные об издателе), а также данные об используемых цифровых сертификатах и информация, необходимая для проверки подлинности этих сертификатов, или данные об отсутствии цифровой подписи файла), также информация о загружаемых в процессы модулях: их имена, размер, типы, даты создания, атрибуты, контрольные суммы (MD5, SHA2-256, SHA1), пути к ним, информация заголовка PE-файлов, имена упаковщиков (если файл был упакован), информация о наличии и валидности данных этой статистики, идентификатор условия формирования передаваемой статистики.

- В случае обнаружения угрозы или уязвимости, дополнительно к информации об обнаруженном объекте предоставляется информация об идентификаторе, версии и типе записи в антивирусных базах, название угрозы согласно классификации Правообладателя, дата и время последнего обновления антивирусных баз, имя исполняемого файла, контрольная сумма (MD5) файла приложения, запросившего URL-адрес, в котором произошло обнаружение, IP-адрес (IPv4 или IPv6) обнаруженной угрозы, идентификатор уязвимости и класс ее опасности, URL-адрес и Referrer страницы обнаружения уязвимости.

- В случае обнаружения потенциально вредоносного объекта предоставляется информация о данных в памяти процессов.

- Информация о сетевой атаке: IP-адрес атакующего компьютера и номер порта компьютера пользователя, на который была направлена сетевая атака, идентификатор протокола, по которому выполнялась атака, название и тип атаки.

- Информация о сетевых соединениях: версия и контрольные суммы (MD5, SHA2-256, SHA1) файла процесса, открывшего порт, путь к файлу процесса и его цифровая подпись, локальный и удаленный IP-адреса, номера локального и удаленного портов соединения, состояние соединения, время открытия порта.

- URL и IP-адрес веб-страницы, на которой был обнаружен вредоносный или подозрительный контент, имя, размер и контрольная сумма файла, запросившего данный URL, идентификатор, вес и степень применимости правила, по которому был вынесен вердикт, цель атаки.

- Информация об обновлении установленной программы и антивирусных баз: статус завершения задачи обновления, тип ошибки, которая могла произойти при обновлении, число неуспешных завершений обновления, идентификатор компонента программы, который выполняет обновление.

- Информация об использовании Kaspersky Security Network (далее "KSN"): идентификатор KSN, идентификатор ПО, полная версия ПО, обезличенный IP-адрес устройства пользователя, показатели качества выполнения запросов к KSN, показатели качества обработки пакетов для KSN, показатели количества

запросов в KSN и информация о типах запросов в KSN, дата и время начала передачи статистики, дата и время окончания передачи статистики, информация об обновлениях конфигурации KSN: идентификатор активной конфигурации, идентификатор полученной конфигурации, код ошибки при обновлении конфигурации.

- Информация о событиях в системных журналах: время события, название журнала, в котором обнаружено событие, тип и категория события, название источника события и его описание.

- Информация для определения репутации файлов, URL-адресов и сертификатов: URL-адрес, для которого запрашивается репутация и Referrer, тип протокола соединения, внутренний идентификатор типа программы, номер используемого порта, идентификатор пользователя, контрольная сумма проверяемого файла (MD5), тип обнаруженной угрозы, информация о записи, которая была использована для обнаружения угрозы (идентификатор записи в антивирусной базе, время создания и тип записи); публичный ключ сертификата; отпечаток цифрового сертификата проверяемого объекта и алгоритм хеширования.

- Данные о территориальной распространенности программы: дата установки и дата активации программы, идентификатор партнера, предоставившего лицензию для активации программы, идентификатор программы, идентификатор языковой локализации программы, серийный номер лицензии, по которой программа активирована, признак участия в KSN.

- Информация об используемой лицензии: тип лицензии и срок ее действия, количество дней до истечения срока действия лицензии, идентификатор партнера, у которого приобретена лицензия, идентификатор регионального центра активации, контрольная сумма кода активации, хеш-сумма тела тикета, рассчитанная по алгоритму SHA1, дата и время создания лицензионного тикета, идентификатор информации о лицензии, идентификатор лицензионного тикета, идентификатор последовательности лицензионного тикета, уникальный идентификатор компьютера пользователя, дата начала и окончания периода валидности лицензионного тикета, текущее состояние лицензионного тикета, версия заголовка тикета, версия лицензии, идентификатор сертификата подписи заголовка тикета, контрольная сумма файла ключа, серийный номер подписчика заголовка тикета, токен авторизации.

- Информация об установленном на компьютере аппаратном обеспечении: тип, название, модель, версия прошивки, характеристики встроенных и подключенных устройств.

- Информация об устройстве: идентификатор устройства.

- Информация о работе компонента "Веб-Контроль":

версия компонента, причина категоризации, дополнительная информация о причине категоризации, категоризированный URL-адрес, IP-адрес хоста заблокированного/категоризированного объекта.

Если Kaspersky Security Center использует Локальный KSN, и вы присоединились к Kaspersky Security Network в параметрах политики, Kaspersky Endpoint Security не отправляет статистику с клиентских компьютеров, к которым была применена политика, в "Лабораторию Касперского".

После удаления политики или ее деактивации настройки KSN на клиентском компьютере возвращаются к исходному состоянию.

Шаг 9. Настройка параметров взаимодействия с пользователем

Если требуется, в окне **Взаимодействие с пользователем** настройте параметры взаимодействия Kaspersky Endpoint Security с пользователем клиентского компьютера.

Шаг 10. Настройка параметров соединения с сетью

Если требуется, в окне **Сеть** выполните следующие действия:

- Настройте параметры подключения к прокси-серверу.
- Включите или выключите проверку информации, которая поступает на компьютер и отправляется с него по протоколу HTTPS.
- Выберите хранилище сертификатов для проверки зашифрованного HTTPS-трафика в браузере Mozilla Firefox.
- Настройте список доверенных корневых сертификатов.
- Настройте контролируемые порты.

  Вы можете создать список портов, которые Kaspersky Endpoint Security контролирует.

Шаг 11. Настройка параметров отчетов и резервного хранилища

Если требуется, в окне **Отчеты и резервное хранилище** выполните следующие действия:

- Настройте параметры формирования и хранения отчетов.
- Настройте параметры хранения объектов в резервном хранилище.

Шаг 12. Настройка шифрования дисков с помощью FileVault

Если требуется, в окне **Шифрование диска FileVault** выполните следующие действия:

- Включите или выключите управление шифрованием диска FileVault для загрузочного диска компьютера пользователя.

  По умолчанию управление шифрованием диска FileVault выключено.

- Выберите опцию **Зашифровать диск**, если вы хотите зашифровать загрузочный диск компьютера пользователя, когда политика будет применена к клиентскому компьютеру.

Если флажок **Управление шифрованием диска FileVault** снят, пользователи с правами администратора могут зашифровать и расшифровать загрузочный диск Mac из Системных настроек.

Если флажок **Управление шифрованием диска FileVault** установлен и выбрана опция **Зашифровать диск**, пользователи с правами администратора не могут расшифровать загрузочный диск Mac из Системных настроек.

Если флажок **Управление шифрованием диска FileVault** установлен и выбрана опция **Расшифровать диск**, пользователи с правами администратора не могут зашифровать загрузочный диск Mac из Системных настроек.

Шаг 13. Настройка Веб-Контроля

Если требуется, в окне **Веб-Контроль** выполните следующие действия:

- Включите или выключите Веб-Контроль.

Примечание. Когда вы включаете Веб-Контроль, чтобы блокировать доступ к опасным веб-ресурсам, Kaspersky Endpoint Security показывает уведомление **Веб-Контроль включен** в Центре защиты на удаленном компьютере. Когда пользователь пытается получить доступ к веб-ресурсам, заблокированным Веб-Контролем на удаленном компьютере, Kaspersky Endpoint Security показывает уведомления, если в окне **Сеть** мастера создания политики установлен флажок **Проверять защищенные соединения (HTTPS)**.

- Добавьте новое правило Веб-Контроля, нажав на кнопку **Добавить**.

  Вы можете указать имя правила и выбрать, будет ли правило активным; указать область применения правила, создав список веб-адресов или выбрав категории сайтов, а также выбрать действие, которое Kaspersky Endpoint Security выполнит, когда пользователь откроет сайт, на который распространяется это правило.

- Отредактируйте, удалите или упорядочьте созданные правила в списке.

Порядок, в котором расположены правила, определяет приоритет их применения программой Kaspersky Endpoint Security.

Шаг 14. Настройка параметров Managed Detection and Response

Если требуется, в окне **Managed Detection and Response** выполните следующие действия:

- Включите или выключите компонент Managed Detection and Response.

  По умолчанию компонент Managed Detection and Response выключен.

- Импортируйте или удалите конфигурационный файл, который используется для активации компонента Managed Detection and Response на управляемых устройствах.

Если флажок **Managed Detection and Response** установлен и конфигурационный файл MDR импортирован, то компонент Managed Detection and Response активен и взаимодействует с решением Kaspersky Managed Detection and Response. Это решение обеспечивает непрерывный поиск, обнаружение и устранение угроз, направленных на вашу организацию.

Шаг 15. Настройка Endpoint Detection and Response (KATA)

Если требуется, в окне **Endpoint Detection and Response (KATA)** выполните следующие действия:

- Включите или выключите компонент Endpoint Detection and Response (KATA).

  По умолчанию компонент Endpoint Detection and Response (KATA) выключен.

- Настройте параметры подключения к серверу и добавьте TLS-сертификат.

- Добавьте сервер KATA.

Если флажок **Endpoint Detection and Response (KATA)** установлен, а TLS-сертификат и сервер KATA добавлены, компонент Endpoint Detection and Response (KATA) активен и взаимодействует с решением Kaspersky Anti Targeted Attack Platform. Это решение оперативно обнаруживает сложные угрозы, таких как целевые атаки, сложные постоянные угрозы, атаки "нулевого дня" и другие.

Шаг 16. Настройка проверки внешних дисков

В окне **Проверка внешних дисков** настройте следующие параметры:

- Действие, которое Kaspersky Endpoint Security выполняет при подключении внешнего диска.

- Действие, которое Kaspersky Endpoint Security выполняет при обнаружении зараженного объекта.

Шаг 17. Настройка Анализа поведения

В окне **Анализ поведения** при необходимости выполните следующие действия:

- Включите или выключите Анализ поведения.

  По умолчанию Анализ поведения включен.

- Выберите действие, которое будет выполнено при обнаружении активности вредоносного ПО.

- Включите или выключите защиту папок общего доступа от внешнего шифрования.

  - Выберите действие, которое будет выполнено при обнаружении активности вредоносного ПО.

Шаг 18. Настройте Защиту от почтовых угроз

Если требуется, в окне **Защита от почтовых угроз** выполните следующие действия:

- Включите или выключите Защиту от почтовых угроз.

  По умолчанию Защита от сетевых угроз включена.

- Выберите действие, которое приложение выполнит при обнаружении вредоносного объекта.

- Настройте параметры Защиты от почтовых угроз.

Шаг 19. Настройте Защиту от эксплойтов

В окне **Защита от эксплойтов** при необходимости выполните следующие действия:

- Включите или выключите Защиту от эксплойтов.

  По умолчанию Защита от эксплойтов включена.

- Выберите действие, которое будет выполнено при обнаружении эксплойта.

Шаг 20. Настройте Откат вредоносных действий

В окне **Откат вредоносных действий** при необходимости выполните следующие действия:

- Включите или выключите Откат вредоносных действий.

  По умолчанию Откат вредоносных действий включен.

Шаг 21. Настройте Контроль устройств

Если требуется, в окне **Контроль устройств** выполните следующие действия:

- Включите или выключите Контроль устройств.

  По умолчанию Контроль устройств включен.

- Настройте параметры Контроля устройств.

Шаг 22. Настроить Сетевой экран

Если требуется, в окне **Сетевой экран** выполните следующие действия:

- Включите или выключите Сетевой экран.

  По умолчанию сетевой экран включен.

- Настройте параметры Сетевого экрана.

Шаг 23. Выбор группы администрирования, к которой будет применена политика

В окне **Целевая группа** нажмите на кнопку **Обзор** и выберите группу администрирования, к которой вы хотите применить политику.

Шаг 24. Выбор статуса политики и завершение создания политики

В окне **Создание групповой политики для программы** выполните следующие действия:

1. Выберите статус, который будет присвоен политике:

   - *Активная политика*: политика применяется к выбранной группе администрирования.
   - *Неактивная политика*: политика не применяется.
   - *Политика для автономных пользователей*: политика применяется к выбранной группе администрирования при отключении компьютеров от сети организации.

   Примечание. В группе администрирования для одного приложения вы можете создать несколько политик, но активной может быть только одна из них.

   Подробную информацию о статусах политики вы можете найти в справке Kaspersky Security Center.

2. Установите флажок **Открыть свойства политики сразу после создания**, если вы хотите просмотреть параметры политики после ее создания.

3. Нажмите на кнопку **Готово** для завершения работы мастера создания политики.

Созданная политика появится на вкладке **Политики** в рабочей области группы администрирования. Политика будет применена к клиентским компьютерам после первой синхронизации клиентских компьютеров с Сервером администрирования.

Вы можете изменить параметры созданной политики. Также вы можете запретить или разрешить изменение каждой группы параметров с клиентского компьютера с помощью кнопок и для каждой группы параметров. Кнопка рядом с группой параметров означает, что пользователь клиентского компьютера не может изменить эти параметры на своем компьютере. Кнопка рядом с группой параметров означает, что пользователь клиентского компьютера может изменить эти параметры на своем компьютере.

Просмотр списка политик

Вы можете создать неограниченное количество различных политик для приложений, установленных на компьютерах в каждой группе администрирования, но в пределах группы администрирования только одна политика может применяться единовременно к каждому приложению.

Просмотр списка политик для группы администрирования

1. Запустите Консоль администрирования Kaspersky Security Center.
2. Разверните узел **Сервер администрирования <Имя сервера>**.
3. В дереве консоли выберите папку **Управляемые устройства**.
4. Выберите группу администрирования, в которую входит клиентский компьютер.
5. В рабочей области выберите вкладку **Политики**.

   Отобразится список политик.

Настройка параметров политики

Развернуть всё | Свернуть всё

Вы можете вносить изменения в политику, созданную вами в Kaspersky Security Center, а также запретить изменение ее параметров в политиках вложенных групп и параметрах задач.

Параметры политики Kaspersky Endpoint Security включают в себя параметры приложения и параметры задач.

Настройка параметров политики

1. Запустите Консоль администрирования Kaspersky Security Center.
2. Разверните узел **Сервер администрирования <Имя сервера>**.
3. В дереве консоли выберите папку **Управляемые устройства**.
4. В рабочей области выберите вкладку **Политики**.
5. По правой клавише мыши откройте контекстное меню политики, параметры которой вы хотите настроить, и выберите **Свойства**.
6. В окне **Свойства: <Имя политики>** настройте параметры политики:

   - В разделе **Базовая защита**

     Настройте следующие параметры Защиты от файловых угроз

     - Включите или выключите Защиту от файловых угроз.
     - Выберите один из предустановленных уровней безопасности или настройте параметры безопасности вручную.
     - Выберите действие, которое приложение выполнит при обнаружении вредоносного объекта.

     Настройте следующие параметры Защиты от веб-угроз

     - Включите или выключите Защиту от веб-угроз.
     - Выберите один из предустановленных уровней безопасности или настройте параметры безопасности вручную.
     - Включите или выключите проверку присутствия веб-адресов в базе вредоносных веб-адресов.
     - Настройте параметры антифишинга.
     - Добавьте доверенные адреса, веб-трафик с которых Защита от веб-угроз не проверяет.
     - Выберите действие, которое приложение выполнит при обнаружении опасного объекта веб-трафика.

Настройте следующие параметры Защиты от почтовых угроз

- Включите или выключите Защиту от почтовых угроз.
- Выберите действие, которое приложение выполнит при обнаружении вредоносного объекта.
- Настройте параметры Защиты от почтовых угроз.

Настройте следующие параметры Защиты от сетевых угроз

- Включите или выключите Защиту от сетевых угроз.
- Настройте параметры Защиты от сетевых угроз.
- Укажите IP-адреса компьютеров, сетевая активность которых не будет блокироваться.

Настройте следующие параметры Сетевого экрана

- Включите или выключите Сетевой экран.
- Настройте параметры Сетевого экрана.

- В разделе **Продвинутая защита**

  Настройте следующие параметры KSN

  - Ознакомьтесь с полным текстом Положения о Kaspersky Security Network, нажав на кнопку **Положение о KSN**.
  - Включите или выключите использование Kaspersky Security Network.
  - Включите или выключите расширенный режим использования KSN.
  - Включите или выключите облачный режим.
  - Включите или выключите использование KSN-прокси.

- Включите или выключите использование серверов "Лаборатории Касперского", если KSN-прокси недоступен.

Примечание. Использование Kaspersky Security Network и KSN-прокси на удаленных компьютерах доступно только если Сервер администрирования Kaspersky Security Center используется в качестве прокси-сервера. Подробную информацию о настройке Сервера администрирования вы можете найти в справке Kaspersky Security Center .

Настройте следующие параметры Анализа поведения

- Включите или выключите Анализ поведения.

  По умолчанию Анализ поведения включен.

- Выберите действие, которое будет выполнено при обнаружении активности вредоносного ПО.

Настройте следующие параметры Защиты от эксплойтов

- Включите или выключите Защиту от эксплойтов.
- Выберите действие, которое будет выполнено при обнаружении эксплойта.

Настройте следующие параметры Отката вредоносных действий

Включите или выключите Откат вредоносных действий.

- В разделе **Контроль безопасности**

  Настройте следующие параметры Контроля устройств

  - Включите или выключите Контроль устройств.
  - Настройте параметры Контроля устройств.

  Настройте следующие параметры Веб-Контроля

- Включите или выключите Веб-Контроль.
- Добавьте новое правило Веб-Контроля, нажав на кнопку **Добавить**.
- Отредактируйте, удалите или упорядочьте созданные правила в списке.

- В разделе **Шифрование данных**

  Настройте следующие параметры шифрования дисков с помощью FileVault

  - Включите и выключите управление шифрованием диска FileVault для клиентских компьютеров.
  - Зашифруйте и расшифруйте загрузочный диск на клиентских компьютерах.

    Если флажок **Управление шифрованием диска FileVault** снят, пользователи с правами администратора могут зашифровать и расшифровать загрузочный диск Mac из Системных настроек.

    Если флажок **Управление шифрованием диска FileVault** установлен и выбрана опция **Зашифровать диск**, пользователи с правами администратора не могут расшифровать загрузочный диск Mac из Системных настроек.

    Если флажок **Управление шифрованием диска FileVault** установлен и выбрана опция **Расшифровать диск**, пользователи с правами администратора не могут зашифровать загрузочный диск Mac из Системных настроек.

- В разделе **Detection and Response**

  Настройте следующие параметры Managed Detection and Response

  - Включите или выключите компонент Managed Detection and Response.
  - Импортируйте или удалите конфигурационный файл, который используется для активации компонента Managed Detection and Response на управляемых устройствах.

  Настройте следующие параметры Endpoint Detection and Response (KATA)

  - Включите или выключите компонент Endpoint Detection and Response (KATA).

- Настройте параметры подключения к серверу и добавьте TLS-сертификат.
- Добавьте сервер KATA.

- В разделе **Локальные задачи**

  Настройте следующие параметры проверки внешних дисков

  - Действие, которое Kaspersky Endpoint Security выполняет при подключении внешнего диска.
  - Действие, которое Kaspersky Endpoint Security выполняет при обнаружении зараженного объекта.

- В разделе **Обновление**

  Настройте следующие параметры обновления

  - Включите или выключите обновление модулей приложения.
  - Укажите источники обновлений.

- В разделе **Дополнительные параметры**

  Настройте следующие параметры защиты

  - Включите или выключите постоянную защиту клиентского компьютера.
  - Включите или выключите запуск Kaspersky Endpoint Security при включении клиентского компьютера.
  - Сформируйте Доверенную зону.
  - Настройте Доверенные приложения.
  - Выберите категории обнаруживаемых объектов.
  - Выключите или включите запуск задач по расписанию при работе компьютера от аккумулятора.

Настройте следующие параметры сети

- Включите или выключите использование прокси-сервера.
- Укажите адрес прокси-сервера.
- Включите или выключите использование прокси-сервера для локальных адресов.
- Укажите имя пользователя и пароль для аутентификации на прокси-сервере.
- Включите или выключите проверку информации, которая поступает на компьютер и отправляется с него по протоколу HTTPS.
- Выберите хранилище сертификатов для проверки зашифрованного HTTPS-трафика в браузере Mozilla Firefox.
- Настройте контролируемые порты.

Настройте следующие параметры отчетов и резервного хранилища

- Включите или выключите запись некритических событий в отчет.
- Включите или выключите запись в отчет только последних событий.
- Включите или выключите удаление событий через указанный промежуток времени.
- Укажите срок хранения событий.
- Включите или выключите удаление объектов из резервного хранилища по истечении указанного срока.
- Укажите срок хранения объектов в резервном хранилище.

Настройте следующие параметры взаимодействия с пользователем

- Включите или выключите уведомления о событиях.

- Выберите способ, которым Kaspersky Endpoint Security уведомляет пользователя о событиях.
- Включите или выключите отображение значка Kaspersky Endpoint Security в строке меню.
- Выберите, может ли пользователь открывать главное окно Kaspersky Endpoint Security и использовать интерфейс приложения на клиентском компьютере.
- Включите или выключите доступность команды **Выход** в меню значка Kaspersky Endpoint Security на клиентском компьютере.
- Выберите язык, на котором отображаются события Kaspersky Security Center.
- Укажите параметры Kaspersky Endpoint Security, которые доступны для изменения пользователям на клиентском компьютере.
- Настройте Защиту паролем, чтобы ограничить нежелательные действия на пользовательских устройствах.

7. Нажмите на кнопку **OK**, чтобы сохранить внесенные изменения и закрыть окно свойств политики.

Изменение статуса политики

Статус политики определяет ее работоспособность. Политика может быть активной, для автономных пользователей и неактивной. Вы можете изменить статус политики в ее параметрах.

Изменение статуса политики

1. Запустите Консоль администрирования Kaspersky Security Center.
2. Разверните узел **Сервер администрирования <Имя сервера>**.
3. В дереве консоли выберите папку **Управляемые устройства**.
4. Выберите группу администрирования, в которую входит клиентский компьютер.
5. В рабочей области выберите вкладку **Политики**.

6. По правой клавише мыши откройте контекстное меню политики, статус которой вы хотите изменить, и выберите пункт **Свойства**.

7. В окне **Свойства: <Имя политики>** выберите раздел **Общие**.

8. В блоке **Состояние политики** выберите один из следующих статусов политики:

   - **Активная политика**. Политика применяется к выбранной группе администрирования.
   - **Политика для автономных пользователей**. Политика применяется к выбранной группе администрирования при отключении компьютеров от сети организации.
   - **Неактивная политика**. Политика не применяется к выбранной группе администрирования.

9. Нажмите на кнопку **ОК**, чтобы сохранить внесенные изменения и закрыть окно **Свойства: <Имя политики>**.

Экспорт политики в файл формата KLP

Вы можете экспортировать параметры политики в файл, чтобы использовать эту политику для другого Сервера администрирования.

Экспорт политики в файл формата KLP

1. Запустите Консоль администрирования Kaspersky Security Center.

2. Разверните узел **Сервер администрирования <Имя сервера>**.

3. В дереве консоли выберите папку **Управляемые устройства**.

4. Выберите группу администрирования, в которую входит клиентский компьютер.

5. В рабочей области выберите вкладку **Политики**.

6. По правой клавише мыши откройте контекстное меню политики, которую вы хотите экспортировать, и выберите пункт **Экспортировать**.

   Откроется окно **Сохранить как**.

7. Выберите папку, в которую вы хотите сохранить файл политики в формате KLP.

8. Укажите название файла.

9. Нажмите **Сохранить**, чтобы сохранить файл в указанную папку.

Импорт политики из файла формата KLP

Вы можете импортировать уже существующую политику с предустановленными параметрами из файла.

Импорт политики из файла формата KLP

1. Запустите Консоль администрирования Kaspersky Security Center.
2. Разверните узел **Сервер администрирования <Имя сервера>**.
3. В дереве консоли выберите папку **Управляемые устройства**.
4. Выберите группу администрирования, в которую входит клиентский компьютер.
5. В рабочей области выберите вкладку **Политики**.
6. Откройте окно выбора файла одним из следующих способов:
   - Нажмите на кнопку **Импортировать политику из файла**.
   - По правой клавише откройте контекстное меню рабочей области и выберите пункт **Импортировать**.
7. Выберите файл политики в формате KLP и нажмите на кнопку **Открыть**.

Импортированная политика будет добавлена в список политик в рабочей области.

Создание профилей политик и управление ими

Профиль политики – это набор изменяемых параметров политики, который активируется на клиентском компьютере при возникновении определенных условий. Активация профиля приводит к изменению параметров политики, которая активна на устройстве в момент активации профиля.

Создание профиля политики

1. В дереве консоли выберите группу администрирования, для которой вы хотите создать профиль политики.

2. В рабочей области выберите вкладку **Политики**.

3. Откройте свойства политики, для которой вы хотите создать профиль, одним из следующих способов:

   - дважды щелкните по имени политики;
   - по правой клавише мыши откройте контекстное меню политики и выберите пункт **Свойства**;
   - нажмите на ссылку **Настроить параметры политики**.

4. В окне **Свойства: <Имя политики>** выберите раздел **Профили политики**.

5. В рабочей области нажмите на кнопку **Добавить**.

6. В окне **Назначение профилей политики** ознакомьтесь с информацией о политиках и нажмите на кнопку **Далее**.

   Если вы хотите, чтобы это окно не отображалось в дальнейшем во время создания профилей политик, установите флажок **Больше не показывать это окно** до нажатия на кнопку **Далее**.

7. В окне **Имя профиля политики** выполните следующие действия, чтобы настроить параметры профиля политики:

   - Введите имя нового профиля политики.

     > **Примечание.** Имя профиля должно включать в себя не более 100 символов.

   - В блоке **Состояние профиля политики** укажите, включен или выключен профиль политики.
   - В раскрывающемся списке в блоке **Состояние профиля политики** выберите, можно ли изменять параметры профиля политики.
   - Если вы хотите настроить правила активации для профиля политики, установите флажок **После закрытия мастера создания профиля политики перейти к настройке правила активации профиля политики**.

8. Нажмите на кнопку **Готово**.

9. Если вы установили флажок **После закрытия мастера создания профиля политики перейти к настройке правила активации профиля политики**, следуйте шагам мастера создания правила активации профиля политики.

Профиль, который вы создали, отобразится в разделе **Профили политики** окна **Свойства**: **<Имя политики>**.

Создание правила активации профиля политики

1. В дереве консоли выберите группу администрирования, для которой вы хотите создать правило активации профиля политики.

2. В рабочей области выберите вкладку **Политики**.

3. Откройте свойства политики одним из следующих способов:

   - дважды щелкните по имени политики;
   - по правой клавише мыши откройте контекстное меню политики и выберите пункт **Свойства**;
   - нажмите на ссылку **Настроить параметры политики**.

4. В окне **Свойства: <Имя политики>** выберите раздел **Профили политики**.

5. В рабочей области выберите профиль политики, для которого вы хотите создать правило активации и нажмите на кнопку **Свойства**.

   Откроется окно **Свойства: <Название профиля политики>**.

6. Выберите раздел **Правила активации**.

7. В рабочей области нажмите на кнопку **Добавить**.

   Запустится мастер создания правила активации профиля политики.

Следуйте шагам мастера создания правила активации профиля политики.

Изменение профиля политики

1. В дереве консоли выберите группу администрирования, для которой вы хотите изменить профиль политики.

2. В рабочей области выберите вкладку **Политики**.

3. Откройте свойства политики, для которой вы хотите изменить профиль, одним из следующих способов:

   - дважды щелкните по имени политики;
   - по правой клавише мыши откройте контекстное меню политики и выберите пункт **Свойства**;
   - нажмите на ссылку **Настроить параметры политики**.

4. В окне **Свойства: <Имя политики>** выберите раздел **Профили политики**.

5. В рабочей области выберите профиль, который вы хотите изменить, и нажмите **Свойства**.

   Откроется окно **Свойства: <Название профиля политики>**.

6. Если требуется, настройте профиль:

   - В блоке **Общие** переименуйте профиль и включите/выключите профиль с помощью флажка **Включить профиль**.
   - В блоке **Правила активации** создайте, измените или удалите правила активации.
   - В блоке **Устройства** выберите устройства, для которых этот профиль политики будет применяться.
   - Измените параметры профиля в соответствующих разделах.

7. Нажмите **ОК**.

Если профиль политики включен, изменения параметров профиля будут применены после синхронизации клиентского компьютера с Сервером администрирования. Если профиль политики выключен, изменения параметров будут применены после срабатывания правила активации.

Изменение приоритета профиля политики

1. В дереве консоли выберите группу администрирования, для которой вы хотите изменить приоритет профиля политики.
2. В рабочей области выберите вкладку **Политики**.
3. Откройте свойства политики, для которой вы хотите изменить приоритет профиля одним из следующих способов:
   - дважды щелкните по имени политики;
   - по правой клавише мыши откройте контекстное меню политики и выберите пункт **Свойства**;
   - нажмите на ссылку **Настроить параметры политики**.
4. В окне **Свойства: <Имя политики>** выберите раздел **Профили политики**.
5. В рабочей области выберите профиль политики, приоритет которого вы хотите изменить.
6. Повысьте/понизьте приоритет выбранного профиля с помощью кнопок /.

Удаление профиля политики

1. В дереве консоли выберите группу администрирования, для которой вы хотите удалить профиль политики.
2. В рабочей области выберите вкладку **Политики**.
3. Откройте свойства политики, для которой вы хотите удалить профиль, одним из следующих способов:
   - дважды щелкните по имени политики;
   - по правой клавише мыши откройте контекстное меню политики и выберите пункт **Свойства**;
   - нажмите на ссылку **Настроить параметры политики**.
4. В окне **Свойства: <Имя политики>** выберите раздел **Профили политики**.

5. В рабочей области выберите профиль, который вы хотите удалить, и нажмите на кнопку **Удалить**.

Подробную информацию о профилях политики вы можете найти в справке Kaspersky Security Center .

Создание отчета об обнаруженных объектах

Создание отчета об обнаруженных объектах

1. Запустите Консоль администрирования Kaspersky Security Center.
2. Разверните узел **Сервер администрирования <Имя сервера>**.
3. В дереве консоли выберите папку **Управляемые устройства**.
4. Выберите группу администрирования, в которую входит клиентский компьютер.
5. Выберите вкладку **Устройства**.
6. Выберите компьютер в списке клиентских компьютеров.
7. По правой клавише мыши откройте контекстное меню клиентского компьютера и выберите пункт **Все задачи** > **Просмотреть отчет об угрозах**.

Сформированный отчет откроется в окне браузера.

Информацию о других способах формирования отчета об объектах, которые приложение обнаружило на клиентском компьютере, вы можете найти в справке Kaspersky Security Center .

Получение ключа восстановления для зашифрованного диска

Если пользователь клиентского компьютера забыл или потерял учетные данные и не может получить доступ к зашифрованному диску, вы можете получить ключ восстановления.

Получение ключа восстановления

1. Запустите Консоль администрирования Kaspersky Security Center.

2. Разверните узел **Сервер администрирования <Имя сервера>**.

3. В дереве консоли выберите папку **Дополнительно**, в ней подпапку **Шифрование и защита данных**, а в ней подпапку **Зашифрованные жесткие диски**.

4. В рабочей области по правой клавише мыши откройте контекстное меню устройства с зашифрованным диском и выберите **Get recovery key for macOS**.

   Откроется окно с ключом восстановления.

5. Сохраните ключ восстановления любым удобным для вас способом.

Вы можете использовать ключ восстановления на клиентском компьютере для получения доступа к зашифрованному диску.

Удаленное управление приложением через Kaspersky Security Center Web Console и Cloud Console

Kaspersky Security Center Web Console (Web Console) – это веб-приложение, предназначенное для централизованного решения основных задач по управлению и обслуживанию защиты сети организации. Web Console является компонентом Kaspersky Security Center, предоставляющим пользовательский интерфейс для управления Kaspersky Endpoint Security в окне браузера. Подробную информацию о Kaspersky Security Center Web Console вы можете найти в справке Kaspersky Security Center .

Kaspersky Security Center Cloud Console (Cloud Console) – это облачное решение для защиты сети организации и управления этой сетью. Подробную информацию о Kaspersky Security Center Cloud Console вы можете найти в справке Kaspersky Security Center Cloud Console .

Также вы можете управлять Kaspersky Endpoint Security с помощью графического пользовательского интерфейса программы, Консоли администрирования Kaspersky Security Center и из командной строки.

Установка веб-плагина Kaspersky Endpoint Security

Веб-плагин Kaspersky Endpoint Security обеспечивает взаимодействие Kaspersky Endpoint Security с Kaspersky Security Center. Веб-плагин требуется установить на устройство с установленным приложением Kaspersky Security Center Web Console. При этом функции веб-плагина доступны всем администраторам, у которых есть доступ к Kaspersky Security Center Web Console в браузере.

Вы можете установить веб-плагин следующими способами:

- С помощью мастера первоначальной настройки Kaspersky Security Center Web Console.

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

- Вручную с помощью дистрибутива в Web Console из стороннего источника.

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

Чтобы установить веб-плагин Kaspersky Endpoint Security вручную:

1. В главном окне Kaspersky Security Center Web Console выберите **Параметры консоли → Веб-плагины**.

   Откроется список установленных веб-плагинов.

2. Запустите установку веб-плагина Kaspersky Endpoint Security одним из следующих способов:

   - Установка из списка веб-плагинов "Лаборатории Касперского":

     a. Нажмите на кнопку **Добавить**.

     Откроется список всех доступных веб-плагинов "Лаборатории Касперского". Список обновляется автоматически после выпуска новых версий веб-плагинов.

     b. Найдите в списке веб-плагин Kaspersky Endpoint Security для Mac 12.2 и нажмите на его название.

     c. В открывшемся окне с описанием веб-плагина нажмите на кнопку **Установить плагин**.

     d. Дождитесь окончания установки и нажмите на кнопку **ОК** в информационном окне.

   - Установка веб-плагина из стороннего источника (архивы, необходимые для установки веб-плагинов, входят в комплект поставки):

     a. Нажмите на кнопку **Добавить из файла**.

     b. В открывшемся окне укажите путь к ZIP-архиву с дистрибутивом веб-плагина и путь к файлу подписи в формате TXT. Этот файл находится в архиве с веб-плагином.

c. Нажмите на кнопку **Добавить**.

d. Дождитесь окончания установки и нажмите на кнопку **OK** в информационном окне.

Новый плагин отображается в списке установленных веб-плагинов (**Параметры консоли** → **Веб-плагины**).

Примечание. Если в свойствах Сервера администрирования Kaspersky Security Center вы выбрали язык, которого нет в дистрибутиве приложения Kaspersky Endpoint Security, то Лицензионное соглашение и весь интерфейс в Kaspersky Security Center Web Console будут отображаться на английском языке.

Создание политики

В этом разделе содержится информация о создании и настройке политик для Kaspersky Endpoint Security с помощью Kaspersky Security Center Web Console и Cloud Console.

Политика определяет параметры работы приложения и доступ к настройке приложения, установленного на компьютерах группы администрирования. Для каждого приложения требуется создать свою политику. Вы можете создать несколько различных политик для приложений, установленных на компьютерах в каждой группе администрирования, но в пределах группы администрирования только одна политика может применяться единовременно к каждому приложению.

Примечание. При создании и настройке политики вы можете разрешить или запретить изменение каждой группы параметров в политиках с помощью переключателя **Принудительно**.

Создание политики

1. В разделе **Устройства** слева выберите подраздел **Политики и профили политик**.
2. Нажмите на кнопку **Добавить**.
3. Выберите приложение, для которого вы хотите создать политику, и нажмите на кнопку **Далее**.

   Откроется окно **Новая политика**.
4. На вкладке **Общие** укажите имя политики, выберите состояние политики и настройте опции наследования параметров политики.

5. На вкладке **Параметры программы** настройте параметры Kaspersky Endpoint Security, которые будут применены к клиентским компьютерам после того, как к ним будет применена политика

6. Нажмите на кнопку **Сохранить**.

Над пользовательскими политиками вы можете выполнять следующие действия:

- создавать политики;
- настраивать параметры политик;
- копировать и переносить политики из одной группы в другую;
- удалять политики;
- изменять статус политик.

Подробную информацию о политиках Kaspersky Security Center Web Console вы можете найти в справке Kaspersky Security Center.

Подробную информацию о политиках Kaspersky Security Center Cloud Console вы можете найти в справке Kaspersky Security Center Cloud Console.

Примечание. После создания профиля политики для политики Kaspersky Endpoint Security с помощью Kaspersky Security Center Web Console или Cloud Console вам нужно проверить правильность применения настроек к клиентским компьютерам.

Настройка параметров продвинутой защиты

В разделе **Продвинутая защита** вы можете выбрать, участвует ли Kaspersky Endpoint Security на клиентских компьютерах в Kaspersky Security Network, и настроить использование KSN-прокси.

Если необходимо, выполните следующие действия:

- Ознакомьтесь с полным текстом Положения о Kaspersky Security Network, нажав на ссылку **Положение о KSN**.
- Просмотрите информацию об инфраструктуре KSN, которую предоставляет Kaspersky Security Center, нажав на ссылку **Положение о KSN**.

Примечание. По умолчанию Kaspersky Security Center использует глобальный KSN. Если вы управляете Kaspersky Endpoint Security через Kaspersky Security Center Web Console и в зависимости от настроек Kaspersky Security Center, вы можете участвовать в Kaspersky Private Security Network вместо Kaspersky Security Network. Если вы управляете Kaspersky Endpoint Security через Kaspersky Security Center Cloud Console, участие в Kaspersky Private Security Network невозможно. Подробную информацию об участии в Kaspersky Private Security Network вы можете найти в справке Kaspersky Security Center.

- Включите или выключите использование Kaspersky Security Network.
- Включите или выключите расширенный режим работы KSN.
- Включите или выключите облачный режим.
- Включите или выключите использование KSN-прокси.
- Включите или выключите использование серверов "Лаборатории Касперского", если KSN-прокси недоступен.

Примечание. Если вы управляете Kaspersky Endpoint Security через Kaspersky Security Center Web Console, использование Kaspersky Security Network и KSN-прокси на удаленных компьютерах доступно только если Сервер администрирования Kaspersky Security Center используется в качестве прокси-сервера. Подробную информацию о настройке Сервера администрирования вы можете найти в справке Kaspersky Security Center.
Если вы управляете Kaspersky Endpoint Security через Kaspersky Security Center Cloud Console, вы можете использовать Kaspersky Security Network и KSN-прокси на удаленных компьютерах через точки распространения, на которых установлена операционная система Windows.

Если Kaspersky Security Center использует глобальный KSN и вы присоединились к Kaspersky Security Network в параметрах политики, статистика Kaspersky Endpoint Security с клиентских компьютеров, к которым была применена политика, автоматически отправляется в "Лабораторию Касперского" для улучшения защиты этих компьютеров.

Примечание. "Лаборатория Касперского" не осуществляет получение, обработку и хранение любых персональных данных без вашего явного согласия.

Данные, предоставляемые в "Лабораторию Касперского" при использовании Kaspersky Security Network в глобальном KSN

Если переключатель **Использование Kaspersky Security Network** включен, а переключатель **Расширенный режим работы KSN** выключен, Kaspersky Endpoint Security отправляет в "Лабораторию Касперского" следующие данные:

- Информация об используемой лицензии: тип лицензии и срок ее действия, количество дней до истечения срока действия лицензии, идентификатор партнера, у которого приобретена лицензия, идентификатор регионального центра активации, контрольная сумма кода активации, хеш-сумма тела тикета, рассчитанная по алгоритму SHA1, дата и время создания лицензионного тикета, идентификатор информации о лицензии, идентификатор лицензионного тикета, идентификатор последовательности лицензионного тикета, уникальный идентификатор компьютера пользователя, дата начала и окончания периода валидности лицензионного тикета, текущее состояние лицензионного тикета, версия заголовка тикета, версия лицензии, идентификатор сертификата подписи заголовка тикета, контрольная сумма файла ключа, серийный номер подписчика заголовка тикета, токен авторизации.

- Полная версия установленного ПО;

  тип установленного ПО; идентификатор обновления ПО; идентификатор службы репутации; идентификатор типа протокола; идентификатор регионального центра активации; версия списка отозванных заключений службы ПО; идентификатор сработавшей записи в антивирусных базах ПО; временная метка сработавшей записи в антивирусных базах ПО; тип сработавшей записи в антивирусных базах ПО; уникальный идентификатор установки ПО на компьютере; дата активации лицензии; дата окончания срока действия лицензии; идентификатор лицензии; статус лицензии, по которой используется ПО; тип контрольной суммы обрабатываемого объекта; название обнаруженной вредоносной программы или легальной программы, которая может быть использована для нанесения вреда устройству или данным пользователя; контрольная сумма обрабатываемого объекта; контрольная сумма кода активации ПО; полная версия ПО; уникальный идентификатор устройства; идентификатор ПО; контрольная сумма файла ключа, которым активировано ПО; идентификатор информационной модели, примененной при предоставлении лицензии на использование ПО; идентификатор сертификата, которым подписан заголовок лицензионного тикета ПО; дата и время создания лицензионного тикета ПО; контрольная сумма лицензионного тикета ПО; версия лицензионного тикета ПО; версия кода активации ПО; формат данных в запросе к инфраструктуре Правообладателя; идентификатор тикета текущей лицензии; идентификатор компонента ПО; результат действий, выполненных ПО; код ошибки; адрес веб-службы, на который осуществлялось обрабатываемое обращение (веб-адрес, IP); номер порта; веб-адрес источника запроса к веб-службе (referrer); публичный ключ сертификата; отпечаток цифрового сертификата проверяемого объекта и алгоритм хеширования.

Если переключатели **Использование Kaspersky Security Network** и **Расширенный режим работы KSN** включены, Kaspersky Endpoint Security отправляет в "Лабораторию Касперского" следующие данные:

- Информация о версиях установленной на компьютере операционной системы (ОС) и установленных пакетов обновлений, версия и контрольные суммы (MD5, SHA2-256, SHA1) файла ядра ОС, параметры режима работы ОС; версия ОС, номер сборки ОС, номер обновления ОС, редакция ОС, расширенная информация о редакции ОС; версия пакета обновления ОС; дата и время запуска ОС; время задержки обработки события о совершении действия в ОС в подсистеме поведенческого анализа; количество задержанных событий текущего типа, совершенных в ОС; время задержки обработки события о совершении действия в ОС в подсистеме проактивной защиты; количество обработанных событий, совершенных в ОС; количество обработанных синхронных событий, совершенных в ОС; суммарная задержка всех событий текущего типа, совершенных в ОС; время задержки обработки события о совершении действия в ОС в подсистеме постоянного хранения событий; суммарная задержка всех событий, совершенных в ОС; количество ожидающих синхронных событий, совершенных в ОС; дата и время получения события о совершении действия в ОС.

- Информация о последней неуспешной перезагрузке ОС: количество неуспешных перезагрузок.

- Информация об установленном ПО Правообладателя и состоянии антивирусной защиты компьютера: идентификатор установки ПО (PCID); версия записи в базе данных ПО; уникальный идентификатор установки программы на компьютере, тип программы, идентификатор типа программы, полная версия установленной программы, идентификатор версии настроек программы, идентификатор типа компьютера, уникальный идентификатор компьютера, на котором установлена программа, уникальный идентификатор пользователя в службах Правообладателя, язык локали и ее рабочее состояние, версия установленных компонентов ПО и их рабочее состояние, версия протокола, который используется для подключения к службам Правообладателя; полная версия установленного ПО; тип установленного ПО; идентификатор обновления ПО; идентификатор службы репутации; идентификатор типа протокола; идентификатор регионального центра активации; версия списка отозванных заключений службы ПО; идентификатор сработавшей записи в антивирусных базах ПО; временная метка сработавшей записи в антивирусных базах ПО; тип сработавшей записи в антивирусных базах ПО; уникальный идентификатор установки ПО на компьютере; дата активации лицензии; дата окончания срока действия лицензии; идентификатор лицензии; статус лицензии, по которой используется ПО; тип контрольной суммы обрабатываемого объекта; название обнаруженной вредоносной программы или легальной программы, которая может быть использована для нанесения вреда устройству или данным пользователя; контрольная сумма обрабатываемого объекта; контрольная сумма кода активации ПО; полная версия ПО; идентификатор ПО; контрольная сумма файла ключа, которым активировано ПО; идентификатор информационной модели, примененной при предоставлении лицензии на использование ПО; идентификатор сертификата, которым подписан заголовок лицензионного тикета ПО; дата и время создания лицензионного тикета ПО; контрольная сумма лицензионного тикета ПО; версия лицензионного тикета ПО; версия кода активации ПО; формат данных в запросе к

инфраструктуре Правообладателя; идентификатор тикета текущей лицензии; идентификатор компонента ПО; результат действий, выполненных ПО; код ошибки; адрес веб-службы, на который осуществлялось обрабатываемое обращение (веб-адрес, IP); номер порта; веб-адрес источника запроса к веб-службе (referrer); количество циклов обновления и применения антивирусных баз; дата и время последнего обновления и применения антивирусных баз; дата и время выпуска баз ПО; версия компонента ПО; идентификатор обновления ПО; тип установленного ПО; дата и время запуска компонента мониторинг активности; дата и время установки ПО; вероятность отправки статистики компонентом мониторинг активности; код события, обрабатываемого компонентом мониторинг активности дольше стандартного времени обработки; время обработки события в базах, обработка которого компонентом мониторинг активности длилась дольше стандартного времени; максимально допустимое время обработки события компонентом мониторинг активности; время обработки события, обработка которого компонентом мониторинг активности длилась дольше стандартного времени; общее количество событий, обработка которых компонентом мониторинг активности длилась дольше стандартного времени.

- Данные обо всех обрабатываемых объектах и действиях: заключение ПО по обрабатываемому объекту; код каталога файлов; размер обрабатываемого объекта; контрольная сумма (SHA256) обрабатываемого объекта; номер обнаруженного ПО в контексте компонента мониторинг активности; дата и время обнаружения стороннего ПО компонентом мониторинг активности; характеристики обнаружения; идентификатор сработавшей записи в антивирусных базах ПО; причина обнаружения стороннего ПО компонентом мониторинг активности; контрольная сумма (MD5) обрабатываемого объекта; результат проверки подписи модуля, целостность которого проверяется ПО; имя обрабатываемого объекта; тип сработавшей записи в антивирусных базах ПО; путь к обрабатываемому объекту; имя проверяемого объекта; дата и время проверки; URL-адрес и Referrer, по которому он был загружен; размер проверяемых файлов и пути к ним; признак нахождения в архиве; дата и время создания файла; имя, размер и контрольные суммы (MD5, SHA2-256) упаковщика (если файл был упакован); энтропия файла; тип файла; код типа файла; признак исполняемого файла, идентификатор исполняемого файла и формат исполняемого файла; контрольная сумма объекта (MD5, SHA2-256); тип и значение дополнительной контрольной суммы объекта; данные о ЭЦП (сертификате) объекта: данные об издателе сертификата, количество запусков объекта с момента последней отправки статистики, идентификатор задачи проверки, способ получения информации о репутации объекта, значение фильтра target, технические характеристики по применяемым технологиям обнаружения; путь к обрабатываемому объекту; код каталога файлов.

- Для исполняемых файлов: энтропия разделов файла, признак проверки репутации или подписи файла, название, тип, идентификатор типа, контрольная сумма (MD5) и размер приложения, загруженного проверяемым объектом, путь к приложению и пути к шаблонам, признак нахождения в списке автозапуска, дата записи, список атрибутов, название упаковщика, информация о цифровой подписи приложения:

издатель сертификата, название отправляемого файла в формате MIME, дата и время сборки файла.

- Информация о запускаемых программах и их модулях: контрольные суммы запускаемых файлов (MD5, SHA2-256), размер, атрибуты, дата создания, имя упаковщика (если файл был упакован), имена файлов, данные о запущенных в системе процессах (идентификатор процесса в системе (PID), имя процесса, данные об учетной записи, от которой запущен процесс, приложении и команде, запустившей процесс, полный путь к файлам процесса и командная строка запуска, описание приложения, к которому относится процесс (название приложения и данные об издателе), а также данные об используемых цифровых сертификатах и информация, необходимая для проверки подлинности этих сертификатов, или данные об отсутствии цифровой подписи файла), также информация о загружаемых в процессы модулях: их имена, размер, типы, даты создания, атрибуты, контрольные суммы (MD5, SHA2-256, SHA1), пути к ним, информация заголовка PE-файлов, имена упаковщиков (если файл был упакован), информация о наличии и валидности данных этой статистики, идентификатор условия формирования передаваемой статистики.

- В случае обнаружения угрозы или уязвимости, дополнительно к информации об обнаруженном объекте предоставляется информация об идентификаторе, версии и типе записи в антивирусных базах, название угрозы согласно классификации Правообладателя, дата и время последнего обновления антивирусных баз, имя исполняемого файла, контрольная сумма (MD5) файла приложения, запросившего URL-адрес, в котором произошло обнаружение, IP-адрес (IPv4 или IPv6) обнаруженной угрозы, идентификатор уязвимости и класс ее опасности, URL-адрес и Referrer страницы обнаружения уязвимости.

- В случае обнаружения потенциально вредоносного объекта предоставляется информация о данных в памяти процессов.

- Информация о сетевой атаке: IP-адрес атакующего компьютера и номер порта компьютера пользователя, на который была направлена сетевая атака, идентификатор протокола, по которому выполнялась атака, название и тип атаки.

- Информация о сетевых соединениях: версия и контрольные суммы (MD5, SHA2-256, SHA1) файла процесса, открывшего порт, путь к файлу процесса и его цифровая подпись, локальный и удаленный IP-адреса, номера локального и удаленного портов соединения, состояние соединения, время открытия порта.

- URL и IP-адрес веб-страницы, на которой был обнаружен вредоносный или подозрительный контент, имя, размер и контрольная сумма файла, запросившего данный URL, идентификатор, вес и степень применимости правила, по которому был вынесен вердикт, цель атаки.

- Информация об обновлении установленной программы и антивирусных баз: статус завершения задачи обновления, тип ошибки, которая могла произойти при

обновлении, число неуспешных завершений обновления, идентификатор компонента программы, который выполняет обновление.

- Информация об использовании Kaspersky Security Network (далее "KSN"): идентификатор KSN, идентификатор ПО, полная версия ПО, обезличенный IP-адрес устройства пользователя, показатели качества выполнения запросов к KSN, показатели качества обработки пакетов для KSN, показатели количества запросов в KSN и информация о типах запросов в KSN, дата и время начала передачи статистики, дата и время окончания передачи статистики, информация об обновлениях конфигурации KSN: идентификатор активной конфигурации, идентификатор полученной конфигурации, код ошибки при обновлении конфигурации.

- Информация о событиях в системных журналах: время события, название журнала, в котором обнаружено событие, тип и категория события, название источника события и его описание.

- Информация для определения репутации файлов, URL-адресов и сертификатов: URL-адрес, для которого запрашивается репутация и Referrer, тип протокола соединения, внутренний идентификатор типа программы, номер используемого порта, идентификатор пользователя, контрольная сумма проверяемого файла (MD5), тип обнаруженной угрозы, информация о записи, которая была использована для обнаружения угрозы (идентификатор записи в антивирусной базе, время создания и тип записи); публичный ключ сертификата; отпечаток цифрового сертификата проверяемого объекта и алгоритм хеширования.

- Данные о территориальной распространенности программы: дата установки и дата активации программы, идентификатор партнера, предоставившего лицензию для активации программы, идентификатор программы, идентификатор языковой локализации программы, серийный номер лицензии, по которой программа активирована, признак участия в KSN.

- Информация об используемой лицензии: тип лицензии и срок ее действия, количество дней до истечения срока действия лицензии, идентификатор партнера, у которого приобретена лицензия, идентификатор регионального центра активации, контрольная сумма кода активации, хеш-сумма тела тикета, рассчитанная по алгоритму SHA1, дата и время создания лицензионного тикета, идентификатор информации о лицензии, идентификатор лицензионного тикета, идентификатор последовательности лицензионного тикета, уникальный идентификатор компьютера пользователя, дата начала и окончания периода валидности лицензионного тикета, текущее состояние лицензионного тикета, версия заголовка тикета, версия лицензии, идентификатор сертификата подписи заголовка тикета, контрольная сумма файла ключа, серийный номер подписчика заголовка тикета, токен авторизации.

- Информация об установленном на компьютере аппаратном обеспечении: тип, название, модель, версия прошивки, характеристики встроенных и подключенных устройств.

- Информация об устройстве: идентификатор устройства.
- Информация о работе компонента "Веб-Контроль":

  версия компонента, причина категоризации, дополнительная информация о причине категоризации, категоризированный URL-адрес, IP-адрес хоста заблокированного/категоризированного объекта.

Если Kaspersky Security Center использует Локальный KSN, и вы присоединились к Kaspersky Security Network в параметрах политики, Kaspersky Endpoint Security не отправляет статистику с клиентских компьютеров, к которым была применена политика, в "Лабораторию Касперского".

Настройка параметров базовой защиты

Если требуется, в разделе **Базовая защита** вы можете настроить параметры работы следующих компонентов:

- Защита от файловых угроз
- Защита от веб-угроз
- Защита от сетевых угроз

Вы можете открыть окно настройки параметров работы компонента, нажав на соответствующую ссылку.

Настройка параметров Защиты от файловых угроз

Если требуется, в окне **Защита от файловых угроз** выполните следующие действия:

- Включите или выключите Защиту от файловых угроз.

  По умолчанию Защита от файловых угроз включена.
- Сформируйте область защиты.
- Выберите действие, которое приложение выполнит при обнаружении вредоносного объекта.
- Выберите, будет ли Kaspersky Endpoint Security проверять только новые и измененные файлы или все файлы.
- Выберите, будет ли Kaspersky Endpoint Security пропускать проверку системного тома "только для чтения" на клиентских компьютерах.

- Выберите, будет ли Kaspersky Endpoint Security использовать технологию iSwift при выполнении проверки.

  > **Примечание.** Технология iSwift позволяет Kaspersky Endpoint Security использовать специальный алгоритм для исключения некоторых объектов из проверки. Это помогает увеличить скорость проверки.

- Выберите типы файлов, которые Kaspersky Endpoint Security будет проверять.
- Выберите действия, которые Kaspersky Endpoint Security выполнит с составными файлами.

Настройка параметров Защиты от веб-угроз

Если требуется, в окне **Защита от веб-угроз** выполните следующие действия:

- Включите или выключите Защиту от веб-угроз.

  По умолчанию Защита от веб-угроз включена.

- Выберите действие, которое приложение выполнит при обнаружении опасного объекта веб-трафика.
- Создайте или измените список доверенных веб-адресов.

Настройка параметров Защиты от сетевых угроз

Если требуется, в окне **Защита от сетевых угроз** выполните следующие действия:

- Включите или выключите Защиту от сетевых угроз.

  По умолчанию Защита от сетевых угроз включена.

- Включите или выключите блокировку атакующих компьютеров.
- Создайте или измените список IP-адресов удаленных компьютеров, сетевую активность которых Kaspersky Endpoint Security не блокирует никогда.

Настройка параметров контроля безопасности

Если требуется, в разделе **Контроль безопасности** выполните следующие действия:

- Включите или выключите Веб-Контроль.

Примечание. Когда вы включаете Веб-Контроль, чтобы блокировать доступ к опасным веб-ресурсам, Kaspersky Endpoint Security показывает уведомление **Веб-Контроль включен** в Центре защиты на удаленном компьютере.
Когда пользователь пытается получить доступ к веб-ресурсам, заблокированным Веб-Контролем на удаленном компьютере, Kaspersky Endpoint Security показывает уведомления, если в окне **Сеть** мастера новой политики включен переключатель **Проверка защищенных соединений (HTTPS)**.

- Добавьте правила, которые определяют, какие веб-адреса или категории сайтов будут контролироваться Веб-Контролем на компьютере пользователя.
- Отредактируйте, удалите или упорядочьте созданные правила в списке.

Порядок, в котором расположены правила, определяет приоритет их применения приложением Kaspersky Endpoint Security.

Настройка шифрования данных

В разделе **Шифрование данных** вы можете включить или выключить шифрование загрузочного диска на клиентских компьютерах, чтобы предотвратить доступ других пользователей к важной информации, которая хранится на диске. По умолчанию шифрование диска FileVault выключено.

Настройка параметров Detection and Response

В блоке **Detection and Response** вы можете настроить следующие компоненты:

- Managed Detection and Response;
- Endpoint Detection and Response;
- Endpoint Detection and Response (KATA).

Вы можете открыть окно настройки параметров работы компонента, нажав на соответствующую ссылку.

Настройка параметров Managed Detection and Response

Если требуется, в окне **Managed Detection and Response** выполните следующие действия:

- Включите или выключите компонент Managed Detection and Response.
- Импортируйте или удалите конфигурационный файл MDR.

Компонент Managed Detection and Response взаимодействует с решением Kaspersky Managed Detection and Response, которое обеспечивает непрерывный поиск, обнаружение и устранение угроз, направленных на вашу организацию.

По умолчанию компонент Managed Detection and Response выключен.

Настройка параметров Endpoint Detection and Response

Если требуется, в окне **Endpoint Detection and Response** выполните следующие действия:

- Включите или выключите компонент Endpoint Detection and Response.
- Настройте параметры Сетевой изоляции для устройства пользователя:
  - Укажите задержку для автоматического отключения Сетевой изоляции.
  - Настройте исключения из Сетевой изоляции.
- Включите или выключите Запрет запуска.
- Выберите действие, которое будет выполнено при запуске или открытии запрещенного объекта.
- Сформируйте список правил Запрета запуска.
- Включите или выключите технологию Cloud Sandbox.

Компонент Endpoint Detection and Response сочетает автоматическое обнаружение угроз с возможностью реагирования на эти угрозы для противодействия сложным атакам, в том числе новым эксплойтам (exploits), программам-вымогателям (ransomware), бесфайловым атакам (fileless attacks), а также методам, использующим законные системные инструменты.

По умолчанию компонент Endpoint Detection and Response выключен.

Настройка Endpoint Detection and Response (KATA)

Если требуется, в окне **Endpoint Detection and Response (KATA)** выполните следующие действия:

- Включите или выключите компонент Endpoint Detection and Response (KATA).
- Настройте параметры соединения с сервером:
  - Укажите время ожидания ответа сервера KATA.

    - Добавьте TLS-сертификат для настройки доверенного соединения.
    - Укажите, будет ли Kaspersky Endpoint Security использовать двустороннюю аутентификацию при подключении к серверу KATA.
    - Загрузите криптоконтейнер, защищенный паролем, чтобы включить двустороннюю аутентификацию.
- Добавьте сервер KATA.
- Выберите, будет ли Kaspersky Endpoint Security использовать TTL для пакетов, отправляемых на сервер KATA.
- Настройте параметры для отправки данных на серверы KATA.
- Ограничьте количество событий, передаваемых Kaspersky Endpoint Security на сервер KATA.

Компонент Endpoint Detection and Response (KATA) обеспечивает взаимодействие с решением Kaspersky Anti Targeted Attack Platform, которое обнаруживает сложные угрозы, такие как целевые атаки, сложные постоянные угрозы, атаки "нулевого дня" и другие.

По умолчанию компонент Endpoint Detection and Response (KATA) выключен.

Настройка параметров обновления

Если требуется, в разделе **Обновление** выполните следующие действия:

- Включите или выключите обновление модулей приложения.
- Добавьте или удалите источники обновлений, которые Kaspersky Endpoint Security будет использовать.

Настройка дополнительных параметров

Если требуется, в разделе **Дополнительные параметры** выполните следующие действия:

- Настройте параметры защиты операционной системы клиентского компьютера.
- Выберите категории обнаруживаемых объектов.
- Выключите или включите запуск задач по расписанию при работе компьютера от аккумулятора.
- Настройте параметры формирования и хранения отчетов.

- Настройте параметры хранения объектов в резервном хранилище.
- Настройте параметры Kaspersky Endpoint Security, которые нужны для взаимодействия с пользователем на клиентском компьютере.
- Настройте параметры подключения к прокси-серверу.
- Включите или выключите проверку информации, которая поступает на компьютер и отправляется с него по протоколу HTTPS.
- Выберите хранилище сертификатов для проверки зашифрованного HTTPS-трафика в браузере Mozilla Firefox.
- Настройте контролируемые порты.
- Измените списки доверенных файлов, папок и программ, которые Kaspersky Endpoint Security не контролирует.

Создание задачи

Этот раздел содержит информацию об использовании Kaspersky Security Center Web Console и Cloud Console для создания и настройки задач Kaspersky Endpoint Security на клиентском компьютере или на группе клиентских компьютеров под управлением Kaspersky Security Center.

Задача – набор действий с настраиваемыми параметрами, который Kaspersky Endpoint Security выполняет на клиентском компьютере.

С помощью Kaspersky Security Center Web Console и Cloud Console вы можете создать следующие задачи:

- Проверка
- Обновление
- Откат обновления
- Добавление ключа

Создание задачи

1. В разделе **Устройства** слева выберите подраздел **Задачи**.
2. Нажмите на кнопку **Добавить**.

Запустится мастер добавления задачи.

3. В раскрывающемся списке **Программа** выберите **Kaspersky Endpoint Security для Mac 12.2**.
4. В раскрывающемся списке **Тип задачи** выберите задачу, которую вы хотите создать.
5. Если необходимо, измените название задачи в поле **Название задачи**.
6. Выберите устройства, которым будет назначена задача.
7. Настройте параметры выбранного типа задачи.
8. Завершите мастер добавления задачи, нажав на кнопку **Готово**.

Примечание. Если вы установили флажок **Открыть окно свойств задачи после ее создания** в окне **Завершение создания задачи**, вы можете продолжить изменение параметров задачи по умолчанию. Если этот флажок не установлен, задача создается с параметрами по умолчанию. Вы можете изменить параметры задачи по умолчанию позднее в любое удобное время.

Над задачами вы можете выполнять следующие действия:

- запускать и останавливать задачи;
- настраивать параметры задачи;
- отслеживать выполнение задачи;
- копировать и переносить задачи из одной группы в другую;
- удалять задачи.

Подробную информацию о задачах Kaspersky Security Center Web Console вы можете найти в справке Kaspersky Security Center.

Подробную информацию о задачах Kaspersky Security Center Cloud Console вы можете найти в справке Kaspersky Security Center Cloud Console.

Настройка параметров задачи Проверка

На вкладке **Параметры программы** вы можете настроить параметры задачи **Проверка** для Kaspersky Endpoint Security на удаленных компьютерах.

Как открыть параметры задачи Проверка

1. Перейдите в раздел **Устройства** > **Задачи**.
2. Двойным щелчком мыши откройте задачу **Проверка**.
3. Выберите вкладку **Параметры программы**.

Если необходимо, выполните следующие действия:

- Сформируйте область проверки.
- Укажите действие, которое Kaspersky Endpoint Security выполняет при обнаружении зараженного объекта.
- Выберите типы файлов, которые Kaspersky Endpoint Security проверяет.
- Настройте параметры производительности проверки.
- Выберите составные файлы, которые Kaspersky Endpoint Security анализирует.

Примечание. Kaspersky Endpoint Security не проверяет файлы, расположенные в хранилищах OneDrive, iCloud и других облачных хранилищах. Исключите эти файлы из области проверки. В противном случае задача проверки может завершиться с ошибкой *Зараженный файл не удален*.

Настройка параметров задачи Добавление ключа

На вкладке **Параметры программы** вы можете настроить параметры задачи **Добавление ключа** для Kaspersky Endpoint Security на удаленных компьютерах.

Как открыть параметры задачи Добавление ключа

1. Перейдите в раздел **Устройства** > **Задачи**.
2. Двойным щелчком мыши откройте задачу **Добавление ключа**.
3. Выберите вкладку **Параметры программы**.

Если необходимо, выполните следующие действия:

- Добавьте действующий лицензионный ключ в качестве резервного ключа.
- Выберите другой ключ для активации Kaspersky Endpoint Security на компьютере пользователя.
- Добавьте новый лицензионный ключ в хранилище Kaspersky Security Center.

Настройка задачи Обновление

На вкладке **Параметры программы** вы можете настроить параметры задачи **Обновление** для Kaspersky Endpoint Security на удаленных компьютерах.

Как открыть параметры задачи Обновление

1. Перейдите в раздел **Устройства** > **Задачи**.
2. Двойным щелчком мыши откройте задачу **Обновление**.
3. Выберите вкладку **Параметры программы**.

Основным источником обновлений Kaspersky Endpoint Security являются специальные серверы обновлений "Лаборатории Касперского". Kaspersky Endpoint Security также может использовать в качестве *источника обновлений* точки распространения, локальные папки или другие веб-серверы.

Если вы управляете Kaspersky Endpoint Security через Kaspersky Security Center Web Console, список источников обновлений по умолчанию включает в себя серверы обновлений "Лаборатории Касперского" и серверы Kaspersky Security Center. Сначала Kaspersky Endpoint Security загружает обновления с серверов Kaspersky Security Center, а затем с серверов обновлений "Лаборатории Касперского".

Если вы управляете Kaspersky Endpoint Security через Kaspersky Security Center Cloud Console, список источников обновлений по умолчанию включает в себя серверы обновлений "Лаборатории Касперского" и точки распространения. Сначала Kaspersky Endpoint Security загружает обновления из точек распространения, а затем с серверов обновлений "Лаборатории Касперского". Подробную информацию о точках распространения вы можете найти в справке Kaspersky Security Center.

Если необходимо, выполните следующие действия:

- Включите или выключите обновление модулей приложения.

- Добавьте или удалите источники обновлений, которые Kaspersky Endpoint Security будет использовать.

Получение ключа восстановления для зашифрованного диска

Если пользователь клиентского компьютера забыл или потерял учетные данные и не может получить доступ к зашифрованному диску, вы можете получить ключ восстановления.

Получение ключа восстановления

1. Нажмите на имя учетной записи администратора в левом нижнем углу окна Kaspersky Security Center Web Console или Cloud Console.
2. Выберите **Параметры интерфейса**.
3. В открывшемся диалоговом окне включите переключатель **Показать Шифрование и защита данных**, чтобы включить управление шифрованием данных, и нажмите на кнопку **Сохранить**.
4. Перейдите в раздел **Операции** > **Шифрование и защита данных** > **Зашифрованные жесткие диски**.

   Откроется список устройств с зашифрованными дисками.
5. Установите флажок рядом с устройством с зашифрованным диском.
6. Нажмите на кнопку **Предоставить доступ к устройству в автономном режиме**.
7. В диалоговом окне **Предоставить доступ к устройству в автономном режиме** выберите веб-плагин для Kaspersky Endpoint Security и нажмите на кнопку **ОК**.
8. Нажмите на кнопку **Получить ключ восстановления**.

   Ключ восстановления отобразится в текущем диалоговом окне.
9. Сохраните ключ восстановления любым удобным для вас способом.

Вы можете использовать ключ восстановления на клиентском компьютере для получения доступа к зашифрованному диску.

Окно Тип установки

Развернуть всё | Свернуть всё

В блоке **Выберите пакеты для установки** вы можете выбрать компоненты приложения, которые вы хотите установить на клиентский компьютер.

Проверка

Флажок добавляет компонент Проверка в инсталляционный пакет Kaspersky Endpoint Security.

По умолчанию флажок установлен, снять его нельзя.

Защита от файловых угроз

Флажок включает/выключает добавление компонента Защита от файловых угроз в инсталляционный пакет Kaspersky Endpoint Security.

Если флажок установлен, компонент Защита от файловых угроз добавляется в инсталляционный пакет Kaspersky Endpoint Security.

Если флажок снят, компонент Защита от файловых угроз не включается в инсталляционный пакет Kaspersky Endpoint Security.

Этот флажок установлен по умолчанию.

Защита от веб-угроз

Флажок включает/выключает добавление компонента Защита от веб-угроз в инсталляционный пакет Kaspersky Endpoint Security.

Если флажок установлен, компонент Защита от веб-угроз добавляется в инсталляционный пакет Kaspersky Endpoint Security.

Если флажок снят, компонент Защита от веб-угроз не включается в инсталляционный пакет Kaspersky Endpoint Security.

Этот флажок установлен по умолчанию.

Защита от сетевых угроз

Флажок включает/выключает добавление компонента Защита от сетевых угроз в инсталляционный пакет Kaspersky Endpoint Security.

Если флажок установлен, компонент Защита от сетевых угроз добавляется в инсталляционный пакет Kaspersky Endpoint Security.

Если флажок снят, компонент Защита от сетевых угроз не включается в инсталляционный пакет Kaspersky Endpoint Security.

Этот флажок установлен по умолчанию.

Коннектор к Агенту администрирования

Флажок добавляет компонент Коннектор к Агенту администрирования в инсталляционный пакет Kaspersky Endpoint Security.

По умолчанию флажок установлен, снять его нельзя.

Окно Информация о лицензии

Развернуть всё | Свернуть всё

В окне **Информация о лицензии** вы можете просмотреть информацию о лицензии: дату истечения срока действия лицензии, количество компьютеров, на которых вы можете использовать Kaspersky Endpoint Security по этой лицензии, тип лицензии.

Добавить в качестве резервного ключа

Флажок включает/выключает добавление указанного файла ключа или кода активации в качестве резервного ключа.

Если флажок установлен, Kaspersky Endpoint Security добавляет указанный файл ключа или код активации как резервный ключ.

Если флажок снят, Kaspersky Endpoint Security добавляет указанный файл ключа или код активации как активный ключ.

Этот флажок по умолчанию снят.

Окно Проверка

Развернуть всё | Свернуть всё

Область проверки

При нажатии на ссылку открывается окно, в котором вы можете сформировать область проверки.

В блоке **Если обнаружен вредоносный объект** вы можете выбрать действие, которое Kaspersky Endpoint Security выполняет при обнаружении зараженного объекта.

Запрашивать по окончании проверки

Kaspersky Endpoint Security не обрабатывает объекты до окончания проверки. Kaspersky Endpoint Security выводит на экран уведомление с информацией о каждом обнаруженном зараженном объекте, в котором вам нужно выбрать действие над этим объектом. Варианты дальнейших действий зависят от типа объекта.

Этот вариант выбран по умолчанию.

Запрашивать во время проверки

Во время проверки Kaspersky Endpoint Security выводит на экран уведомление с информацией о каждом обнаруженном зараженном объекте, в котором вам нужно выбрать действие над этим объектом. Варианты дальнейших действий зависят от типа объекта.

Не запрашивать

Kaspersky Endpoint Security фиксирует информацию об обнаруженных объектах в отчете, не обрабатывая их.

Лечить автоматически

Флажок включает/выключает лечение обнаруженных Kaspersky Endpoint Security зараженных объектов без запроса подтверждения пользователя.

Если флажок установлен, Kaspersky Endpoint Security автоматически лечит обнаруженные зараженные объекты.

Если флажок снят, Kaspersky Endpoint Security оставляет обнаруженные зараженные объекты без изменений.

Флажок доступен, если выбрана опция **Не запрашивать**.

Этот флажок установлен по умолчанию.

Лечить. Удалять, если лечение невозможно

Флажок включает/выключает удаление зараженных и возможно зараженных объектов после неудачной попытки их вылечить.

Если флажок установлен, Kaspersky Endpoint Security автоматически удаляет зараженные объекты, которые не удалось вылечить.

Если флажок снят, Kaspersky Endpoint Security не удаляет зараженные объекты, которые не удалось вылечить.

Флажок отображается, если выбрана опция **Не запрашивать** и установлен флажок **Лечить автоматически**.

Этот флажок установлен по умолчанию.

В блоке **Типы файлов** вы можете выбрать формат файлов, которые Kaspersky Endpoint Security проверяет.

Проверять все файлы

Kaspersky Endpoint Security проверяет все запускаемые, открываемые и сохраняемые объекты файловой системы.

Проверять программы и документы по содержимому

Kaspersky Endpoint Security проверяет только заражаемые файлы на основании формата файла.

Перечень форматов файлов определен "Лабораторией Касперского" и является частью баз Kaspersky Endpoint Security.

Проверять программы и документы по расширению

Kaspersky Endpoint Security проверяет только заражаемые файлы на основании расширения файла.

Перечень расширений файлов определен "Лабораторией Касперского" и является частью баз Kaspersky Endpoint Security.

Kaspersky Endpoint Security всегда проверяет файлы без расширения.

В блоке **Оптимизация** вы можете настроить производительность проверки.

Проверять только новые и измененные файлы

Флажок включает/выключает проверку только тех файлов, которые Kaspersky Endpoint Security распознает как новые или измененные с момента последней проверки.

Если флажок установлен, Kaspersky Endpoint Security проверяет только файлы, признанные новыми или измененными с момента последней проверки.

Если флажок снят, Kaspersky Endpoint Security проверяет все файлы.

Пропускать проверку системного тома «только для чтения»

Флажок включает/выключает проверку системного тома "только для чтения".

Если флажок установлен, Kaspersky Endpoint Security пропускает проверку системного тома "только для чтения". Время выполнения проверки значительно уменьшается.

Если флажок снят, Kaspersky Endpoint Security проверяет системный том "только для чтения".

Этот флажок установлен по умолчанию.

Пропускать, если размер файла больше <значение> МБ

Флажок включает/выключает исключение из антивирусной проверки файлов, размер которых превышает указанный.

Если флажок установлен, Kaspersky Endpoint Security пропускает файлы, размер которых превышает указанный.

Если флажок снят, Kaspersky Endpoint Security проверяет все файлы вне зависимости от их размера.

Этот флажок по умолчанию снят.

По умолчанию установлен размер 100 МБ.

Пропускать, если проверка длится более <значение> сек.

Флажок включает/выключает ограничение времени проверки одного файла. Kaspersky Endpoint Security пропускает файл, если его проверка длится дольше указанного времени.

Если флажок установлен, Kaspersky Endpoint Security пропускает файл, если его проверка длится дольше указанного времени.

Если флажок снят, Kaspersky Endpoint Security проверяет все файлы вне зависимости от длительности их проверки.

По умолчанию установлено значение 30 секунд.

В блоке **Составные файлы** вы можете выбрать типы составных файлов, которые Kaspersky Endpoint Security проверяет.

Проверять архивы

Флажок включает/выключает проверку архивов.

Если флажок установлен, Kaspersky Endpoint Security проверяет архивы.

Если флажок снят, Kaspersky Endpoint Security пропускает архивы при проверке.

Все

Kaspersky Endpoint Security проверяет все архивы.

Опция доступна, если установлен флажок **Проверять архивы**.

Новые

Kaspersky Endpoint Security проверяет только новые архивы.

Опция доступна, если установлен флажок **Проверять архивы**.

Проверять архивы, защищенные паролем

Флажок включает/выключает проверку архивов, защищенных паролем.

Если флажок установлен, Kaspersky Endpoint Security проверяет архивы, защищенные паролем.

Если флажок снят, Kaspersky Endpoint Security пропускает архивы, защищенные паролем, при проверке.

Проверять вложенные OLE-объекты

Флажок включает/выключает проверку вложенных в файлы объектов (например, Excel-таблицы, макросы, вложения в сообщениях электронной почты).

Если флажок установлен, Kaspersky Endpoint Security проверяет вложенные OLE-объекты.

Если флажок снят, Kaspersky Endpoint Security пропускает вложенные OLE-объекты при проверке.

Все

Kaspersky Endpoint Security проверяет все OLE-объекты.

Опция доступна, если установлен флажок **Проверять вложенные OLE-объекты**.

Новые

Kaspersky Endpoint Security проверяет только новые вложенные OLE-объекты.

Опция доступна, если установлен флажок **Проверять вложенные OLE-объекты**.

Проверять файлы почтовых форматов

Флажок включает/выключает проверку файлов почтовых форматов, а также почтовых баз данных.

Если флажок установлен, Kaspersky Endpoint Security проверяет файлы почтовых форматов, а также почтовые базы данных.

Если флажок снят, Kaspersky Endpoint Security пропускает файлы почтовых форматов, а также почтовые базы данных при проверке.

Окно Область проверки

Развернуть всё | Свернуть всё

Добавить

При нажатии на кнопку открывается диалоговое окно, в котором вы можете указать файл, папку или маску имени файла или папки для добавления в область проверки.

Удалить

При нажатии на кнопку объект удаляется из области проверки.

Кнопка доступна, если установлен флажок рядом с объектом.

Вы не можете удалить объекты, добавленные в область проверки по умолчанию.

Область проверки

В этой графе отображаются объекты, которые проверяются при выполнении задач проверки.

Статус

Переключатель в этой графе включает/выключает проверку объектов, добавленных в область проверки.

Если переключатель включен, Kaspersky Endpoint Security проверяет соответствующий объект.

Если переключатель выключен, Kaspersky Endpoint Security не проверяет соответствующий объект.

Дополнительно

Значение в этой графе показывает, проверяет ли Kaspersky Endpoint Security папки, вложенные в соответствующий объект.

Примечание. Kaspersky Endpoint Security не проверяет файлы, расположенные в хранилищах OneDrive, iCloud и других облачных хранилищах. Исключите эти файлы из области проверки. В противном случае задача проверки может завершиться с ошибкой *Зараженный файл не удален*.

Диалог Добавление объекта в область проверки

Развернуть всё | Свернуть всё

Укажите имя либо маску имени файла или папки

Путь к файлу, папке или маска имени файла или папки.

Объект является папкой

Флажок включает/выключает проверку объекта как папки.

Если флажок установлен, Kaspersky Endpoint Security проверяет объект, который вы указали в поле **Укажите имя либо маску имени файла или папки**, как папку.

Если флажок снят, Kaspersky Endpoint Security проверяет объект, который вы указали в поле **Укажите имя либо маску имени файла или папки**, как файл.

Этот флажок установлен по умолчанию.

Включить вложенные папки

Флажок включает/выключает проверку папок, вложенных в папку, указанную в поле **Укажите имя либо маску имени файла или папки**.

Если флажок установлен, Kaspersky Endpoint Security проверяет вложенные папки при поиске вредоносного ПО.

Если флажок снят, Kaspersky Endpoint Security проверяет только файлы в папке, указанной в поле **Укажите имя либо маску имени файла или папки**.

Этот флажок установлен по умолчанию.

Примечание. Kaspersky Endpoint Security не проверяет файлы, расположенные в хранилищах OneDrive, iCloud и других облачных хранилищах. Исключите эти файлы из области проверки. В противном случае задача проверки может завершиться с ошибкой *Зараженный файл не удален*.

Окно параметры файла

Поддерживаются следующие типы файловых хешей:

- **MD5**

  Хеш этого типа должен быть длиной 32 символа и содержать 0–9, a-f, A-F.

- **SHA256**

  Хеш этого типа должен быть длиной 64 символа и содержать 0–9, a-f, A-F.

Окно Сеть

Развернуть всё | Свернуть всё

В блоке **Параметры прокси-сервера** вы можете настроить использование прокси-сервера, а также настроить параметры подключения к прокси-серверу.

Не использовать прокси-сервер

Если выбрана эта опция, Kaspersky Endpoint Security не использует прокси-сервер для подключения к источникам обновлений для получения обновлений баз и модулей приложения.

Использовать системные параметры прокси-сервера

Если выбрана эта опция, Kaspersky Endpoint Security подключается к источникам обновлений для получения обновлений баз и модулей приложения с помощью параметров прокси-сервера, указанных в настройках операционной системы.

Этот вариант выбран по умолчанию.

Использовать указанные параметры прокси-сервера

Если выбрана эта опция, Kaspersky Endpoint Security подключается к источникам обновлений для получения обновлений баз и модулей приложения с помощью параметров прокси-сервера, указанных вами.

Адрес

IP-адрес или символьное имя прокси-сервера.

Поле доступно, если выбрана опция **Использовать указанные параметры прокси-сервера**.

Порт

Номер порта прокси-сервера.

По умолчанию установлен порт 8080.

Поле доступно, если выбрана опция **Использовать указанные параметры прокси-сервера**.

Использовать аутентификацию

Флажок включает/выключает использование аутентификации при соединении с прокси-сервером.

Если флажок установлен, Kaspersky Endpoint Security запрашивает учетные данные пользователя для соединения с прокси-сервером.

Если флажок снят, Kaspersky Endpoint Security не запрашивает учетные данные пользователя для соединения с прокси-сервером.

Этот флажок установлен по умолчанию.

Флажок доступен, если выбрана опция **Использовать указанные параметры прокси-сервера**.

Имя пользователя

Имя пользователя для соединения с прокси-сервером.

Поле доступно, если выбрана опция **Использовать указанные параметры прокси-сервера** и установлен флажок **Использовать аутентификацию**.

Пароль

Пароль для указанного имени пользователя.

Поле доступно, если выбрана опция **Использовать указанные параметры прокси-сервера** и установлен флажок **Использовать аутентификацию**.

Показать

При нажатии на кнопку отображаются символы пароля, который вы ввели в поле **Пароль**.

Не использовать прокси-сервер для локальных адресов

Флажок включает/выключает использование прокси-сервера при обновлении баз и модулей приложения из сетевой или локальной папки.

Если флажок установлен, Kaspersky Endpoint Security не использует прокси-сервер при обновлении баз и модулей приложения из сетевой или локальной папки.

Если флажок снят, Kaspersky Endpoint Security использует прокси-сервер при обновлении баз и модулей приложения из сетевой или локальной папки.

Этот флажок установлен по умолчанию.

Флажок доступен, если выбрана опция **Использовать указанные параметры прокси-сервера**.

В блоке **Проверять защищенные соединения** вы можете настроить, проверяет ли Kaspersky Endpoint Security защищенные соединения (HTTPS).

Проверка защищенных соединений (HTTPS)

Переключатель **Проверка защищенных соединений (HTTPS)** включает/выключает проверку защищенных соединений, выполняемых по протоколу HTTPS, а также отображение уведомлений о случаях, когда Веб-Контроль блокирует пользователю доступ к опасным веб-ресурсам.

Если переключатель **Проверка защищенных соединений (HTTPS)** включен, Kaspersky Endpoint Security выполняет следующие действия:

- Защита от веб-угроз проверяет данные, поступающие на ваш компьютер и отправляющиеся с него по протоколу HTTPS через веб-браузеры Safari, Google Chrome и Firefox.

- Приложение показывает уведомления, когда пользователи пытаются открыть веб-ресурсы, заблокированные Веб-Контролем на удаленных компьютерах.

Если переключатель **Проверка защищенных соединений (HTTPS)** выключен, Kaspersky Endpoint Security выполняет следующие действия:

- Защита от веб-угроз не проверяет данные, поступающие на ваш компьютер и отправляющиеся с него по протоколу HTTPS.

- Приложение не показывает уведомления, когда пользователи пытаются открыть веб-ресурсы, заблокированные Веб-Контролем на удаленных компьютерах.

Этот переключатель включен по умолчанию.

В блоке **Выберите, какое хранилище сертификатов будет использовать браузер Firefox** вы можете выбрать хранилище сертификатов для проверки зашифрованного HTTPS-трафика в браузере Mozilla Firefox.

Связка ключей для корневых системных сертификатов (рекомендовано)

Если выбран этот вариант, Kaspersky Endpoint Security использует корневой сертификат из связки ключей System Roots для проверки зашифрованного HTTPS-трафика в браузере Mozilla Firefox.

Этот вариант выбран по умолчанию.

Хранилище сертификатов в настройках браузера Mozilla Firefox

Если выбран этот вариант, Kaspersky Endpoint Security использует сертификат из хранилища сертификатов браузера.

В этом случае вам нужно вручную добавить сертификат Kaspersky Endpoint Security в хранилище сертификатов браузера Mozilla Firefox. Дополнительные сведения см. в разделе Как добавить сертификат Kaspersky в хранилище сертификатов Mozilla Firefox.

В блоке **Доверенные корневые сертификаты** вы можете управлять списком доверенных корневых сертификатов.

Управлять доверенными корневыми сертификатами

При нажатии на ссылку открывается окно, в котором вы можете создать список доверенных корневых сертификатов для подключения к соответствующим серверам без уведомлений.

В блоке **Контролируемые порты** вы можете настроить порты, которые проверяются Kaspersky Endpoint Security.

Выбранные порты

При нажатии на ссылку открывается окно, в котором вы можете создать или изменить список портов, которые проверяются Kaspersky Endpoint Security.

Принудительно

Если переключатель **Принудительно** включен, Kaspersky Endpoint Security запрещает изменение значений в параметрах задач, параметрах приложения, в политиках вложенных групп и подчиненных Серверов администрирования.

Если переключатель **Принудительно** выключен, Kaspersky Endpoint Security разрешает изменение значений в параметрах задач, параметрах приложения, в политиках вложенных групп и подчиненных Серверов администрирования.

Окно Управлять доверенными корневыми сертификатами

Развернуть всё | Свернуть всё

Добавить

При нажатии на эту кнопку открывается диалоговое окно для добавления сертификата, который будет считаться доверенным.

Удалить

При нажатии на кнопку выбранный сертификат удаляется из списка доверенных сертификатов.

Список доверенных сертификатов

Список, отображающий имена доверенных корневых сертификатов.

Список доверенных корневых сертификатов по умолчанию пуст.

Принудительно

Если переключатель **Принудительно** включен, Kaspersky Endpoint Security запрещает изменение значений в параметрах задач, параметрах приложения, в политиках вложенных групп и подчиненных Серверов администрирования.

Если переключатель **Принудительно** выключен, Kaspersky Endpoint Security разрешает изменение значений в параметрах задач, параметрах приложения, в политиках вложенных групп и подчиненных Серверов администрирования.

Окно Контролируемые порты

Развернуть всё | Свернуть всё

Список контролируемых портов

Список портов, для которых вы можете настроить проверку проходящих через них данных.

По умолчанию список содержит порты, которые наиболее часто используются службами.

Добавить

При нажатии на кнопку открывается диалоговое окно, в котором вы можете добавить порт, который Kaspersky Endpoint Security будет контролировать.

Удалить

При нажатии на кнопку выбранный порт удаляется из списка.

Кнопка доступна, если установлен флажок рядом с портом.

Порт

В этой графе отображаются номера портов.

Статус

Эта графа содержит переключатель, который показывает статус проверки проходящих через порт данных.

Если установлен статус **Проверяется**, Kaspersky Endpoint Security проверяет данные, проходящие через соответствующий порт.

Если установлен статус **Не проверяется**, Kaspersky Endpoint Security не проверяет данные, проходящие через соответствующий порт.

Описание

В этой графе отображается описание порта.

Диалог Добавление порта

Развернуть всё | Свернуть всё

Поле ввода порта

Номер порта, для которого Kaspersky Endpoint Security будет проверять проходящие через порт данные.

Поле ввода описания

Дополнительная информация о порте, например, тип порта.

Окно Доверенная зона: раздел Файлы и папки

Развернуть всё | Свернуть всё

Добавить

При нажатии на кнопку открывается диалоговое окно, в котором вы можете добавить файл или папку в Доверенную зону.

Удалить

При нажатии на кнопку выбранный файл или папка удаляется из списка исключений.

Кнопка доступна, если установлен флажок рядом с файлом или папкой.

Файл или папка

В этой графе отображаются файлы и папки, которые вы добавили в Доверенную зону.

Статус

Переключатель в этой графе включает/выключает проверку файла или папки, которые вы добавили в Доверенную зону.

Если переключатель включен, Kaspersky Endpoint Security не проверяет соответствующий файл или папку.

Если переключатель выключен, Kaspersky Endpoint Security проверяет соответствующий файл или папку.

Комментарий

Информация о файле или папке, которые вы добавили в Доверенную зону.

Принудительно

Если переключатель **Принудительно** включен, Kaspersky Endpoint Security запрещает изменение значений в параметрах задач, параметрах приложения, в политиках вложенных групп и подчиненных Серверов администрирования.

Если переключатель **Принудительно** выключен, Kaspersky Endpoint Security разрешает изменение значений в параметрах задач, параметрах приложения, в политиках вложенных групп и подчиненных Серверов администрирования.

Диалог Добавление исключения

Развернуть всё | Свернуть всё

Поле ввода имени либо маски имени файла или папки

Путь к файлу или папке либо маска имени файла или папки, которые будут исключены из области защиты.

Включить вложенные папки

Флажок включает/выключает проверку папок, вложенных в папку, указанную в поле **Укажите имя либо маску имени файла или папки**.

Если флажок установлен, при поиске вредоносного ПО Kaspersky Endpoint Security не проверяет папки, вложенные в указанную папку.

Если флажок снят, Kaspersky Endpoint Security исключает из проверки только файлы, которые расположены в папке, указанной в поле **Укажите имя либо маску имени файла или папки**. Папки, вложенные в указанную папку, проверяются.

Этот флажок установлен по умолчанию.

В блоке **Компоненты** вы можете выбрать компоненты, которые не будут проверять файл или папку, указанные вами.

Любой

Компоненты Проверка и Защита от файловых угроз не будут проверять файл или папку, указанные вами.

Из списка

Эта опция позволяет вам выбрать компоненты.

Защита от файловых угроз

Если флажок установлен, компонент Защита от файловых угроз не будет проверять файл или папку, указанные вами.

Флажок доступен, если выбрана опция **Из списка**.

Проверка

Если флажок установлен, компонент Проверка не будет проверять файл или папку, указанные вами.

Флажок доступен, если выбрана опция **Из списка**.

Поле ввода комментария

Информация о файле или папке, которые вы добавили в Доверенную зону.

В блоке **Статус** вы можете выбрать, будет ли исключение активным или нет.

Выключено

Kaspersky Endpoint Security проверяет соответствующий файл или папку.

Включено

Kaspersky Endpoint Security не проверяет соответствующий файл или папку.

Окно Доверенная зона: раздел Доверенные приложения

Развернуть всё | Свернуть всё

Список доверенных приложений

Список доверенных приложений, сетевую активность которых Kaspersky Endpoint Security не контролирует.

Добавить

При нажатии на кнопку открывается диалоговое окно, в котором вы можете ввести путь к приложению, сетевую активность которого Kaspersky Endpoint Security не контролирует.

Удалить

При нажатии на кнопку выбранное доверенное приложение удаляется из списка.

Кнопка доступна, если установлен флажок рядом с доверенным приложением.

Приложение

В этой графе отображается название приложения или последний сегмент пути в приложении.

Статус

Эта графа содержит переключатель, который показывает статус контроля сетевой активности приложения.

Если установлен статус **Включено**, Kaspersky Endpoint Security не контролирует сетевую активность соответствующего приложения.

Если установлен статус **Выключено**, Kaspersky Endpoint Security контролирует сетевую активность соответствующего приложения.

Путь

В этой графе отображается путь к приложению на клиентском компьютере, который вы вводите вручную.

Принудительно

Если переключатель **Принудительно** включен, Kaspersky Endpoint Security запрещает изменение значений в параметрах задач, параметрах приложения, в политиках вложенных групп и подчиненных Серверов администрирования.

Если переключатель **Принудительно** выключен, Kaspersky Endpoint Security разрешает изменение значений в параметрах задач, параметрах приложения, в политиках вложенных групп и подчиненных Серверов администрирования.

Диалог Добавление приложения

Развернуть всё | Свернуть всё

Поле ввода пути

Путь к приложению, файловую или сетевую активность которого приложение Kaspersky Endpoint Security не будет контролировать.

Требование к подписи кода

Требования к подписи кода приложения, активность которого не будет отслеживаться Kaspersky Endpoint Security.

Это необязательный параметр.

Опции

В этом разделе вы можете выбрать типы активностей, которые вы хотите, чтобы приложение Kaspersky Endpoint Security не контролировало.

Не контролировать файловую активность

Флажок включает/выключает контроль операций приложения с файлами на клиентском компьютере.

Если флажок установлен, Kaspersky Endpoint Security не контролирует файловую активность приложения.

Если флажок снят, Kaspersky Endpoint Security контролирует файловую активность приложения.

Этот флажок установлен по умолчанию.

Не контролировать сетевую активность

Этот флажок включает/выключает контроль входящего и исходящего интернет-трафика приложения на клиентском компьютере.

Если флажок установлен, Kaspersky Endpoint Security не контролирует сетевую активность приложения.

Если флажок снят, Kaspersky Endpoint Security контролирует сетевую активность приложения.

Этот флажок установлен по умолчанию.

Раздел Дополнительные параметры

Развернуть всё | Свернуть всё

Защита

При нажатии на ссылку открывается окно **Защита**, в котором вы можете управлять основными параметрами работы Kaspersky Endpoint Security на компьютерах пользователей и выбрать типы объектов, которые Kaspersky Endpoint Security обнаруживает.

Отчеты и резервное хранилище

При нажатии на ссылку открывается окно **Отчеты и резервное хранилище**, в котором вы можете настроить параметры отчетов и резервного хранилища.

Взаимодействие с пользователем

При нажатии на ссылку открывается окно **Взаимодействие с пользователем**, в котором вы можете настроить уведомления Kaspersky Endpoint Security, язык отображения для событий в Kaspersky Security Center и дополнительные параметры работы Kaspersky Endpoint Security.

Сеть

При нажатии на ссылку открывается окно **Сеть**, в котором вы можете управлять настройками прокси-сервера, включать или выключать проверку зашифрованных соединений (HTTPS), выбирать хранилище сертификатов для проверки зашифрованного HTTPS-трафика в браузере Mozilla Firefox и настраивать контролируемые порты.

Доверенная зона

При нажатии на кнопку открывается окно **Доверенная зона**, в котором вы можете добавить исключения для Защиты от файловых угроз и задач проверки.

Окно Защита

Развернуть всё | Свернуть всё

В блоке **Основные** вы можете выключить или выключить защиту файлов на удаленном компьютере и настроить автозапуск приложения при включении компьютера или после перезагрузки операционной системы.

Запускать приложение при включении компьютера

Флажок включает/выключает режим автоматического запуска Kaspersky Endpoint Security при включении удаленного компьютера или после перезагрузки его операционной системы.

Если флажок установлен, Kaspersky Endpoint Security запускается автоматически при включении удаленного компьютера или после перезагрузки его операционной системы.

Если флажок снят, Kaspersky Endpoint Security не запускается автоматически при включении удаленного компьютера или после перезагрузки его операционной системы.

Этот флажок установлен по умолчанию.

Важно! Если вы установите этот флажок, когда Kaspersky Endpoint Security не запущен, изменения будут применены только после запуска приложения локально или с помощью Kaspersky Security Center.

Включить защиту

Флажок включает/выключает защиту удаленного компьютера, на котором установлен Kaspersky Endpoint Security.

Если флажок установлен, защита удаленного компьютера включена.

Если флажок снят, защита удаленного компьютера выключена.

Этот флажок установлен по умолчанию.

В блоке **Типы обнаруживаемых объектов** вы можете выбрать типы объектов, которые Kaspersky Endpoint Security будет обнаруживать.

Вирусы, черви, троянские программы, вредоносные утилиты, рекламные программы и программы автодозвона

Флажок включает/выключает контроль следующих типов программ:

- Все типы вредоносных программ.
- Программы, которые отображают рекламные материалы (например, баннеры) на вашем компьютере или заменяют результаты поиска в вашем браузере на рекламные сайты.
- Программы, которые незаметно устанавливают телефонные соединения через компьютерный модем.

По умолчанию флажок установлен, снять его нельзя.

Легальные программы, которые могут быть использованы злоумышленником для нанесения вреда компьютеру или данным пользователя

Флажок включает/выключает контроль программ, которые не являются вредоносными или опасными, однако при некотором стечении обстоятельств могут быть использованы для нанесения вреда компьютеру пользователя.

Если флажок установлен, Kaspersky Endpoint Security обнаруживает легальные программы, которые могут быть использованы злоумышленником для нанесения вреда компьютеру или данным пользователя.

Если флажок снят, Kaspersky Endpoint Security не обнаруживает легальные программы, которые могут быть использованы злоумышленником для нанесения вреда компьютеру или данным пользователя.

Этот флажок по умолчанию снят.

Блок **Дополнительно** позволяет включить режим экономичного энергопотребления.

Не запускать задачи по расписанию при работе от аккумулятора

Флажок включает/выключает запуск задач проверки по расписанию для компьютеров, работающих от аккумулятора.

Если флажок установлен, Kaspersky Endpoint Security не запускает задачи проверки по расписанию на компьютерах, работающих от аккумулятора.

Если флажок снят, Kaspersky Endpoint Security запускает задачи проверки по расписанию на компьютерах, работающих от аккумулятора.

Этот флажок установлен по умолчанию.

Ограничивать сканирующий поток в использовании CPU

Kaspersky Endpoint Security ограничивает использование процессора защищаемого устройства в задачах проверки по требованию значением, указанным в соответствующем поле ввода.

Включение этой опции может негативно сказаться на производительности Kaspersky Endpoint Security.

По умолчанию эта опция выключена.

Предельное значение (в процентах)

Максимально допустимое значение загрузки процессора для задач проверки приложением Kaspersky Endpoint Security.

Это поле доступно, если выбран параметр **Ограничивать сканирующий поток в использовании CPU**.

Примечание. Это совокупный лимит для всех ядер CPU. В приложении "Мониторинг системы" отображается сумма загрузки отдельных ядер CPU, которая может превышать 100%.

Принудительно

Если переключатель **Принудительно** включен, Kaspersky Endpoint Security запрещает изменение значений в параметрах задач, параметрах приложения, в политиках вложенных групп и подчиненных Серверов администрирования.

Если переключатель **Принудительно** выключен, Kaspersky Endpoint Security разрешает изменение значений в параметрах задач, параметрах приложения, в политиках вложенных групп и подчиненных Серверов администрирования.

Окно Отчеты и резервное хранилище

Развернуть всё | Свернуть всё

В блоке **Отчеты** вы можете настроить параметры создания и хранения отчетов о событиях, которые происходят во время работы Kaspersky Endpoint Security.

Удалять отчеты через <значение> дней

Флажок включает/выключает удаление отчетов приложения по истечении указанного срока.

Если флажок установлен, Kaspersky Endpoint Security удаляет отчеты по истечении указанного срока. По умолчанию Kaspersky Endpoint Security хранит отчеты 30 дней.

Если флажок снят, Kaspersky Endpoint Security хранит отчеты бессрочно.

Этот флажок установлен по умолчанию.

Записывать некритические события

Флажок включает/выключает запись событий некритического характера (например, информационных событий) в отчет. События некритического характера не влияют на обеспечение защиты.

Если флажок установлен, Kaspersky Endpoint Security записывает информационные события в отчет.

Если флажок снят, Kaspersky Endpoint Security не записывает информационные события в отчет.

Этот флажок по умолчанию снят.

Сохранять только недавние события

Флажок включает/выключает хранение информации только о важных событиях, которые произошли с момента предыдущего запуска задачи.

Если флажок установлен, во время каждого запуска задачи Kaspersky Endpoint Security удаляет информацию о некритических событиях, которые произошли с момента предыдущего запуска задачи, но сохраняет в отчете важную информацию (например, об обнаруженных вредоносных объектах).

Если флажок снят, Kaspersky Endpoint Security сохраняет информацию о всех событиях, которые произошли с момента предыдущего запуска задачи.

Этот флажок по умолчанию снят.

В блоке **Резервное хранилище** вы можете установить максимальный срок хранения объектов в резервном хранилище.

Удалять объекты через <значение> дней

Флажок включает/выключает удаление объектов из резервного хранилища по истечении указанного срока.

Если флажок установлен, Kaspersky Endpoint Security удаляет объекты из резервного хранилища по истечении указанного срока. По умолчанию срок хранения составляет 30 дней.

Если флажок снят, Kaspersky Endpoint Security хранит объекты в резервном хранилище бессрочно.

Этот флажок установлен по умолчанию.

Принудительно

Если переключатель **Принудительно** включен, Kaspersky Endpoint Security запрещает изменение значений в параметрах задач, параметрах приложения, в политиках вложенных групп и подчиненных Серверов администрирования.

Если переключатель **Принудительно** выключен, Kaspersky Endpoint Security разрешает изменение значений в параметрах задач, параметрах приложения, в политиках вложенных групп и подчиненных Серверов администрирования.

Окно Взаимодействие с пользователем

Развернуть всё | Свернуть всё

В блоке **Интерфейс приложения** вы можете настроить отображение значка приложения в строке меню на удаленном компьютере, а также выбрать, может ли пользователь открывать главное окно Kaspersky Endpoint Security и использовать интерфейс приложения.

Отображать значок приложения в строке меню

Флажок включает/выключает отображение значка приложения в строке меню на удаленном компьютере.

Если флажок установлен, значок приложения отображается в строке меню.

Если флажок снят, значок приложения в строке меню скрыт.

Этот флажок установлен по умолчанию.

Разрешить пользователю открывать приложение

Флажок разрешает/запрещает пользователю открывать главное окно Kaspersky Endpoint Security и использовать интерфейс приложения на удаленном компьютере.

Если флажок установлен, пользователь может открывать главное окно Kaspersky Endpoint Security и использовать интерфейс приложения на удаленном компьютере.

Если флажок снят, Kaspersky Endpoint Security запрещает пользователю открывать главное окно приложения и скрывает интерфейс приложения на удаленном компьютере.

Этот флажок установлен по умолчанию.

В блоке **Уведомления** вы можете включить получение уведомлений о событиях в работе Kaspersky Endpoint Security и выбрать тип уведомлений, которые вы хотите получать.

Уведомления

Переключатель **Уведомления** включает/выключает получение уведомлений о событиях в работе Kaspersky Endpoint Security.

Если переключатель **Уведомления** включен, Kaspersky Endpoint Security выводит на экран уведомления о событиях, которые происходят во время работы компонентов Kaspersky Endpoint Security.

Если переключатель **Уведомления** выключен, Kaspersky Endpoint Security не выводит на экран уведомления о событиях, которые происходят во время работы компонентов Kaspersky Endpoint Security.

Этот переключатель включен по умолчанию.

Уведомления пользователя

При нажатии на ссылку открывается окно, в котором вы можете выбрать тип уведомлений для всех типов событий.

В блоке **Разрешить пользователю завершать работу приложения** вы можете настроить, может ли пользователь на удаленном компьютере завершать работу Kaspersky Endpoint Security.

Отображать команду «Выход» в контекстном меню значка приложения

Флажок включает/выключает отображение пункта **Выход** в контекстном меню значка приложения, расположенного в строке меню.

Если флажок установлен, пункт **Выход** отображается в контекстном меню значка приложения. Пользователь удаленного компьютера может завершить работу Kaspersky Endpoint Security на удаленном компьютере.

Если флажок снят, пункт **Выход** недоступен в контекстном меню значка приложения. Пользователь удаленного компьютера не может завершить работу Kaspersky Endpoint Security на удаленном компьютере.

Этот флажок установлен по умолчанию.

В блоке **События в Kaspersky Security Center** вы можете выбрать язык отображения событий Kaspersky Endpoint Security в Kaspersky Security Center.

Язык отображения

В раскрывающемся списке вы можете выбрать язык отображения событий Kaspersky Endpoint Security в Kaspersky Security Center.

В блоке **Ограничения** вы можете разрешить локальное управление ключами и обновлениями Kaspersky Endpoint Security на удаленном компьютере.

Разрешить пользователю локально управлять обновлениями

Флажок включает/выключает возможность локального управления обновлениями Kaspersky Endpoint Security на удаленном компьютере.

Если флажок установлен, пользователь может локально управлять обновлениями Kaspersky Endpoint Security на удаленном компьютере.

Если флажок снят, вы можете управлять обновлениями Kaspersky Endpoint Security на удаленном компьютере только с помощью плагина управления Kaspersky Endpoint Security в Kaspersky Security Center.

Этот флажок установлен по умолчанию.

Разрешить пользователю локально управлять ключами

Флажок включает/выключает возможность локального управления ключами Kaspersky Endpoint Security на удаленном компьютере.

Если флажок установлен, пользователь может локально управлять ключами Kaspersky Endpoint Security на удаленном компьютере.

Если флажок снят, вы можете управлять ключами Kaspersky Endpoint Security на удаленном компьютере только с помощью плагина управления Kaspersky Endpoint Security в Kaspersky Security Center.

Этот флажок установлен по умолчанию.

В блоке **Защита паролем** вы можете установить и настроить пароль для ограничения нежелательных действий на устройствах пользователя.

Защита паролем

Переключатель **Защита паролем** включает/выключает защиту паролем от нежелательных действий на устройствах пользователей.

Если переключатель **Защита паролем** включен, вы можете установить и настроить пароль, чтобы ограничить действия пользователей на их устройствах.

Если переключатель **Защита паролем** выключен, пользователь может выполнить нежелательное действие, не вводя пароль.

Этот переключатель выключен по умолчанию.

При включении этого переключателя открывается окно, в котором вы можете настроить пароль для ограничения нежелательных действий на устройствах пользователей.

Параметры

При нажатии на эту кнопку открывается окно, в котором вы можете настроить пароль для ограничения нежелательных действий на устройствах пользователей.

Принудительно

Если переключатель **Принудительно** включен, Kaspersky Endpoint Security запрещает изменение значений в параметрах задач, параметрах приложения, в политиках вложенных групп и подчиненных Серверов администрирования.

Если переключатель **Принудительно** выключен, Kaspersky Endpoint Security разрешает изменение значений в параметрах задач, параметрах приложения, в политиках вложенных групп и подчиненных Серверов администрирования.

Окно Уведомления пользователя

Развернуть всё | Свернуть всё

События

В графе перечислены события, которые могут возникнуть во время работы Kaspersky Endpoint Security:

- **Критические события**. События первостепенной важности с точки зрения безопасности компьютера.
- **Отказ функциональности**. События, приводящие к неработоспособности приложения.
- **Важные события**. События, на которые нужно обратить внимание.
- **Информационные события**. События информационного характера.

Уведомления

Всплывающие сообщения уведомляют пользователя о событии.

Флажок в графе **Уведомления** включает/выключает появление всплывающих уведомлений о событиях соответствующей категории.

Звуковое оповещение

Звуковое оповещение о возникновении события.

Флажок в графе **Звуковое оповещение** включает/выключает звуковое оповещение о возникновении события соответствующей категории.

Раздел Обновление

Развернуть всё | Свернуть всё

Обновлять модули приложения

Флажок включает/выключает обновление модулей приложения. Базы приложения обновляются всегда.

Если флажок установлен, Kaspersky Endpoint Security обновляет модули приложения.

Если флажок снят, Kaspersky Endpoint Security не обновляет модули приложения.

Этот флажок установлен по умолчанию.

Источники обновлений

Список содержит адреса ресурсов, с которых Kaspersky Endpoint Security загружает и устанавливает обновления модулей и баз приложения. Вы можете указать в качестве источника обновлений локальную или сетевую папку, FTP- или HTTP-сервер.

По умолчанию, список источников обновлений содержит серверы обновлений "Лаборатории Касперского".

Если вы управляете Kaspersky Endpoint Security через Kaspersky Security Center Web Console, список источников обновлений по умолчанию также содержит серверы Kaspersky Security Center.

Если вы управляете Kaspersky Endpoint Security через Kaspersky Security Center Cloud Console, список источников обновлений по умолчанию также содержит точки распространения. Подробную информацию о точках распространения вы можете найти в справке Kaspersky Security Center.

Вы не можете удалить из списка источники обновлений, добавленные по умолчанию.

Добавить

При нажатии на кнопку открывается диалоговое окно, в котором вы можете указать путь к локальной или сетевой папке или веб-адрес для добавления в список источников обновлений.

Удалить

При нажатии на кнопку выбранный источник обновлений удаляется из списка.

Кнопка доступна, если установлен флажок рядом с источником обновлений.

Источник обновлений

В этой графе отображаются источники обновлений Kaspersky Endpoint Security.

Статус

Если переключатель в этой графе включен, Kaspersky Endpoint Security использует соответствующий источник обновлений в графе **Источник обновлений** для получения обновлений.

Если переключатель в этой графе выключен, Kaspersky Endpoint Security не использует соответствующий источник обновлений в графе **Источник обновлений** для получения обновлений.

Принудительно

Если переключатель **Принудительно** включен, Kaspersky Endpoint Security запрещает изменение значений в параметрах задач, параметрах приложения, в политиках вложенных групп и подчиненных Серверов администрирования.

Если переключатель **Принудительно** выключен, Kaspersky Endpoint Security разрешает изменение значений в параметрах задач, параметрах приложения, в политиках вложенных групп и подчиненных Серверов администрирования.

Диалог Добавление источника обновлений

Развернуть всё | Свернуть всё

Поле ввода веб-адреса или пути к локальной или сетевой папке

Адрес ресурса, с которого Kaspersky Endpoint Security получает обновления.

В качестве адреса ресурса вы можете указать путь к локальной или сетевой папке, а также веб-адрес или IP-адрес FTP- или HTTP-сервера.

Вы можете указать веб-адрес FTP-сервера в формате ftp://<имя пользователя>:<пароль>@<хост>:<порт>.

В блоке **Статус** вы можете выбрать, будет ли Kaspersky Endpoint Security использовать указанный веб-адрес как источник обновлений.

Выключено

Веб-адрес добавляется в список источников обновлений, но Kaspersky Endpoint Security не использует его для получения обновлений.

Включено

Веб-адрес добавляется в список источников обновлений, и Kaspersky Endpoint Security использует его для получения обновлений.

Раздел Шифрование данных

Развернуть всё | Свернуть всё

Шифрование диска FileVault

Переключатель **Шифрование диска FileVault** включает/выключает управление шифрованием диска FileVault.

Если переключатель **Шифрование диска FileVault** включен, шифрование диска FileVault можно применить к клиентским компьютерам с помощью Kaspersky Security Center.

Если переключатель **Шифрование диска FileVault** выключен, шифрование диска FileVault не применимо к клиентским компьютерам с помощью Kaspersky Security Center.

Этот переключатель выключен по умолчанию.

Примечание. Если переключатель **Шифрование диска FileVault** выключен, пользователи с правами администратора могут зашифровать и расшифровать загрузочный диск Mac из Системных настроек. Вы можете найти дополнительную информацию о FileVault в документации Apple.

Зашифровать диск

Kaspersky Endpoint Security отображает окно запроса учетных данных для клиентских компьютеров, к которым применяется эта политика. Когда пользователь вводит учетные данные, Kaspersky Endpoint Security запускает шифрование загрузочного диска компьютера.

Если переключатель **Шифрование диска FileVault** включен и выбрана опция **Зашифровать диск**, пользователи с правами администратора не могут расшифровать загрузочный диск Mac из Системных настроек.

Расшифровать диск

Kaspersky Endpoint Security отображает окно запроса учетных данных для клиентских компьютеров, к которым применяется эта политика. Когда пользователь вводит учетные данные, Kaspersky Endpoint Security начинает расшифровку загрузочного диска компьютера.

Если переключатель **Шифрование диска FileVault** включен и выбрана опция **Расшифровать диск**, пользователи с правами администратора не могут зашифровать загрузочный диск Mac из Системных настроек.

Принудительно

Если переключатель **Принудительно** включен, Kaspersky Endpoint Security запрещает изменение значений в параметрах задач, параметрах приложения, в политиках вложенных групп и подчиненных Серверов администрирования.

Если переключатель **Принудительно** выключен, Kaspersky Endpoint Security разрешает изменение значений в параметрах задач, параметрах приложения, в политиках вложенных групп и подчиненных Серверов администрирования.

Раздел Detection and Response

Развернуть всё | Свернуть всё

Managed Detection and Response

При нажатии на ссылку открывается окно, в котором можно настроить параметры Managed Detection and Response.

Endpoint Detection and Response

При нажатии на ссылку открывается окно, в котором можно настроить параметры Endpoint Detection and Response.

Endpoint Detection and Response (KATA)

При нажатии на ссылку открывается окно, в котором можно настроить параметры Endpoint Detection and Response (KATA).

Окно Managed Detection and Response

Развернуть всё | Свернуть всё

Managed Detection and Response

Переключатель **Managed Detection and Response** включает/выключает компонент Managed Detection and Response, который взаимодействует с решением Kaspersky Managed Detection and Response. Это решение обеспечивает непрерывный поиск, обнаружение и устранение угроз, направленных на вашу организацию.

Если переключатель **Managed Detection and Response** включен и конфигурационный файл MDR импортирован, компонент Managed Detection and Response работает.

Если переключатель **Managed Detection and Response** выключен, компонент Managed Detection and Response не работает.

Этот переключатель выключен по умолчанию.

Импортировать

При нажатии на кнопку открывается окно, в котором вы можете импортировать конфигурационный файл MDR в политику Kaspersky Endpoint Security.

Удалить конфигурационный файл

При нажатии на кнопку удаляется конфигурационный файл MDR из политики Kaspersky Endpoint Security.

Принудительно

Если переключатель **Принудительно** включен, Kaspersky Endpoint Security запрещает изменение значений в параметрах задач, параметрах приложения, в политиках вложенных групп и подчиненных Серверов администрирования.

Если переключатель **Принудительно** выключен, Kaspersky Endpoint Security разрешает изменение значений в параметрах задач, параметрах приложения, в политиках вложенных групп и подчиненных Серверов администрирования.

Окно Endpoint Detection and Response

Развернуть всё | Свернуть всё

Endpoint Detection and Response

Переключатель **Endpoint Detection and Response** включает/выключает компонент Endpoint Detection and Response, который взаимодействует с решением Kaspersky Endpoint Detection and Response. Решение защищает компьютеры от сложных атак, в том числе от новых эксплойтов, приложений-вымогателей, безфайловых атак.

Если переключатель **Endpoint Detection and Response** включен, компонент Endpoint Detection and Response включен.

Если переключатель **Endpoint Detection and Response** выключен, компонент Endpoint Detection and Response выключен.

Этот переключатель выключен по умолчанию.

В разделе **Сетевая изоляция** вы можете настроить параметры изоляции компьютеров от сети в ответ на обнаружение индикатора компрометации.

Настроить разблокировку компьютера

При нажатии на эту ссылку открывается окно, в котором можно указать задержку автоматического отключения Сетевой изоляции.

Исключения

При нажатии на эту ссылку открывается окно, в котором можно указать сетевые подключения, которые не блокируются на компьютере после автоматического включения Сетевой изоляции.

В разделе **Запрет запуска** вы можете настроить параметры запуска исполняемых файлов и скриптов, а также открытия файлов офисного формата.

Запрет запуска

Переключатель **Запрет запуска** включает/выключает Запрет запуска.

Если переключатель **Запрет запуска** включен, вы можете создать и отредактировать список правил запрета запуска, а также выбрать действие, которое будет выполняться при запуске или открытии запрещенных объектов.

Если переключатель **Запрет запуска** выключен, вы не можете управлять объектами, которые пользователи запускают или открывают на своих устройствах.

Этот переключатель выключен по умолчанию.

Действие при запуске или открытии объекта

Блокировать и записывать в отчет

Если выбран этот режим, приложение блокирует запуск объектов или открытие документов, соответствующих критериям правил запрета. Также приложение публикует в журнал событий Kaspersky Security Center и в единую систему логирования событие о попытках запуска объектов или открытия документов.

Только записывать в отчет

Если выбран этот режим, Kaspersky Endpoint Security публикует в журнал событий Kaspersky Security Center и в единую систему логирования событие о попытках запуска исполняемых объектов или открытия документов, соответствующих критериям правил запрета, но не блокирует их запуск или открытие. Этот режим выбран по умолчанию.

Добавить

При нажатии на эту кнопку открывается окно, в котором вы можете создать новое правило запрета запуска.

Изменить

При нажатии на эту кнопку открывается окно, в котором вы можете изменить существующее правило запрета запуска.

Кнопка доступна, если правило выбрано в списке.

Удалить

При нажатии на кнопку выбранное правило запрета запуска удаляется из списка правил.

Кнопка доступна, если правило выбрано в списке правил.

В разделе **Настройка Cloud Sandbox** вы можете включить или выключить компонент Cloud Sandbox.

Cloud Sandbox

Переключатель **Cloud Sandbox** включает/выключает технологию Cloud Sandbox, которая помогает обнаруживать комплексные угрозы на компьютере. Kaspersky Endpoint Security автоматически отправляет обнаруженные файлы в Cloud Sandbox для анализа. Cloud Sandbox запускает эти файлы в изолированной среде для выявления вредоносной активности и принимает решение о репутации этих файлов. Далее данные об этих файлах попадают в Kaspersky Security Network. Таким образом, если Cloud Sandbox обнаруживает вредоносный файл, Kaspersky Endpoint Security выполнит действие для устранения угрозы на всех компьютерах, на которых обнаружит этот файл.

Если переключатель **Cloud Sandbox** включен, технология Cloud Sandbox включена.

Если переключатель **Cloud Sandbox** выключен, технология Cloud Sandbox выключена.

Этот переключатель выключен по умолчанию.

Принудительно

Если переключатель **Принудительно** включен, Kaspersky Endpoint Security запрещает изменение значений в параметрах задач, параметрах приложения, в политиках вложенных групп и подчиненных Серверов администрирования.

Если переключатель **Принудительно** выключен, Kaspersky Endpoint Security разрешает изменение значений в параметрах задач, параметрах приложения, в политиках вложенных групп и подчиненных Серверов администрирования.

Окно настроек разблокировки компьютера

Развернуть всё | Свернуть всё

Разблокировать автоматически изолированный компьютер через

Этот флажок включает/выключает автоматическое отключение Сетевой изоляции по истечении заданного времени.

Если этот флажок установлен, вы можете указать задержку автоматического отключения Сетевой изоляции компьютера.

Если флажок снят, Kaspersky Endpoint Security отключает Сетевую изоляцию через 8 часов после начала изоляции.

Этот флажок установлен по умолчанию.

Часы

Интервал времени, по истечении которого Сетевая изоляция будет автоматически отключена.

Это поле доступно для редактирования, только если флажок **Разблокировать автоматически изолированный компьютер через** установлен.

Окно Исключения из Сетевой изоляции

Развернуть всё | Свернуть всё

Исключения из сетевой изоляции

Этот список содержит сетевые подключения, которые вы добавили в качестве исключений Сетевой изоляции.

Добавить

При нажатии на эту кнопку открывается окно, в котором вы можете вручную указать параметры сетевого подключения, которое будет добавлено в качестве исключения.

Добавить из профиля

При нажатии на эту кнопку открывается окно, в котором вы можете выбрать стандартные сетевые профили для настройки исключений.

Удалить

При нажатии на эту кнопку сетевое соединение из списка исключений Сетевой изоляции удаляется.

Кнопка доступна, если соединение выбрано в списке исключений Сетевой изоляции.

Окно Свойства правила

Развернуть всё | Свернуть всё

Название правила

Название правила исключения из Сетевой изоляции.

Это необязательный параметр.

Направление

Направление трафика.

Протокол

Тип протокола.

Номер

Номер протокола.

Значение должно соответствовать списку назначенных номеров интернет-протоколов IANA.

Это поле доступно, если выбран тип протокола **Пользовательский**.

Локальный порт или диапазон

Локальный порт или диапазон локальных портов компьютера, для которого настраиваются исключения из Сетевой изоляции.

Удаленный порт или диапазон

Удаленный порт или диапазон удаленных портов компьютера, для которого настраиваются исключения из Сетевой изоляции.

Удаленный адрес

Сетевой адрес компьютера, для которого настраиваются исключения из Сетевой изоляции.

Приложения

Этот флажок позволяет добавить приложение, которому разрешено инициировать сетевое соединение, добавленное в исключения из Сетевой изоляции на изолированном компьютере.

Если этот флажок установлен, вы можете добавить такое приложение.

Если флажок снят, сетевое соединение, добавленное в исключения из Сетевой изоляции, может быть инициировано любым приложением на изолированном компьютере.

Этот флажок по умолчанию снят.

Добавление

При нажатии на эту кнопку открывается окно, в котором можно указать путь к приложению, которому разрешено инициировать сетевое соединение, добавленное в исключения Сетевой изоляции.

Изменить

При нажатии на эту кнопку открывается окно, в котором можно изменить путь к добавленному приложению.

Эта кнопка доступна, если приложение выбрано в списке.

Удалить

При нажатии на эту кнопку добавленное приложение удаляется.

Эта кнопка доступна, если приложение выбрано в списке.

Окно Правило запрета

Имя

Название правила.

Тип

Тип объекта, который вы хотите заблокировать.

В разделе **Путь к объекту** вы можете выбрать, следует ли указывать полный путь к запрещаемому объекту. Если вы выбрали указать путь, введите его значение в соответствующее поле.

В разделе **Контрольная сумма объекта** вы можете выбрать, следует ли указывать контрольную сумму для запрещенного объекта. Если вы выбрали указать контрольную сумму, выберите ее тип и введите значение в соответствующее поле.

Окно Endpoint Detection and Response (KATA)

Развернуть всё | Свернуть всё

Endpoint Detection and Response (KATA)

Переключатель **Endpoint Detection and Response (KATA)** включает/выключает компонент Endpoint Detection and Response (KATA), который взаимодействует с решением Kaspersky Anti Targeted Attack Platform. Это решение оперативно обнаруживает сложные угрозы, таких как целевые атаки, сложные постоянные угрозы, атаки "нулевого дня" и другие.

Если переключатель **Endpoint Detection and Response (KATA)** включен, компонент Endpoint Detection and Response (KATA) включен.

Если переключатель **Endpoint Detection and Response (KATA)** выключен, компонент Endpoint Detection and Response (KATA) выключен.

Этот переключатель выключен по умолчанию.

Параметры подключения к серверам

При нажатии на ссылку открывается окно, в котором вы можете настроить параметры подключения к серверам KATA.

Серверы KATA

Этот список содержит добавленные вами серверы KATA.

Добавить

При нажатии на кнопку открывается окно, в котором вы можете настроить подключение к серверу KATA.

Изменить

При нажатии на кнопку открывается окно, в котором вы можете изменить параметры подключения к серверу KATA.

Кнопка доступна, если сервер выбран в списке.

Удалить

При нажатии на кнопку сервер KATA удаляется из списка серверов.

Кнопка доступна, если сервер выбран в списке.

Адрес

IP-адрес сервера KATA.

Порт

Номер порта сервера KATA.

Отправлять запрос на синхронизацию на сервер KATA каждые (мин)

Интервал между запросами синхронизации, отправляемыми на сервер KATA.

По умолчанию установлено значение 5 минут.

Использовать TTL при отправке событий

Этот флажок включает/отключает TTL для пакетов, которые Kaspersky Endpoint Security отправляет на сервер KATA. Механизм TTL ограничивает время жизни для пакетов событий значением, указанным в поле **TTL (ч)**.

Если флажок установлен, TTL включен.

Если флажок снят, TTL выключен.

Этот флажок установлен по умолчанию.

TTL (ч)

Время жизни пакетов, которые Kaspersky Endpoint Security отправляет на сервер KATA.

По умолчанию установлено значение 24 часа.

В блоке **Параметры передачи данных** вы можете настроить параметры отправки данных на серверы KATA.

Максимальная задержка отправки событий (сек.)

Интервал, с которым Kaspersky Endpoint Security отправляет события на сервер KATA.

По умолчанию установлено значение 30 секунд.

Максимальное количество событий в пакете

Максимальное количество событий в одном пакете, отправляемых Kaspersky Endpoint Security на сервер KATA.

По умолчанию установлено значение 1024 события.

В блоке **Регулирование количества запросов** вы можете ограничить количество передаваемых событий.

Включить регулирование количества запросов

Этот флажок включает/отключает ограничение количества событий, которые Kaspersky Endpoint Security отправляет на сервер KATA.

Если этот флажок установлен, количество событий, отправляемых приложением, ограничено.

Если этот снят, количество событий, отправляемых приложением, не ограничено.

Этот флажок установлен по умолчанию.

Максимальное количество событий в час

Максимальное количество событий в час, которые Kaspersky Endpoint Security отправляет на сервер KATA. Kaspersky Endpoint Security восстанавливает передачу событий по истечении часа.

По умолчанию установлено значение 3000 событий в час.

Процент превышения лимита событий

Предельное значение для событий одного типа (в процентах).

Kaspersky Endpoint Security ограничивает передачу событий определенного типа, если отношение событий этого типа к общему количеству событий превышает установленное предельное значение.

По умолчанию установлено значение 15 %.

Принудительно

Если переключатель **Принудительно** включен, Kaspersky Endpoint Security запрещает изменение значений в параметрах задач, параметрах приложения, в политиках вложенных групп и подчиненных Серверов администрирования.

Если переключатель **Принудительно** выключен, Kaspersky Endpoint Security разрешает изменение значений в параметрах задач, параметрах приложения, в политиках вложенных групп и подчиненных Серверов администрирования.

Окно Сервер KATA

Развернуть всё | Свернуть всё

Адрес

IP-адрес сервера KATA.

Порт

Номер порта сервера KATA.

По умолчанию установлено значение 443.

Окно Параметры подключения к серверам

Развернуть всё | Свернуть всё

Время ожидания (сек.)

Время ожидания ответа сервера KATA. По истечении времени ожидания ответа Kaspersky Endpoint Security пытается подключиться к другому серверу KATA.

По умолчанию установлено значение 10 секунд.

В блоке **TLS-сертификат сервера** вы можете добавить или удалить TLS-сертификат и просмотреть информацию о добавленном вами сертификате.

Добавить TLS-сертификат

При нажатии на кнопку открывается окно, в котором вы можете выбрать TLS-сертификат, который будет использоваться для установки доверенного соединения с сервером KATA.

Удалить

При нажатии на кнопку текущий TLS-сертификат удаляется.

Кнопка доступна, если TLS-сертификат был добавлен.

В блоке **Дополнительная защита подключения** вы можете настроить расширенную защиту для соединения между Kaspersky Endpoint Security и сервером KATA.

Использовать двустороннюю аутентификацию

Этот флажок включает/отключает двустороннюю аутентификацию, которая делает соединение между Kaspersky Endpoint Security и сервером KATA более безопасным. Чтобы использовать двустороннюю аутентификацию, вам необходимо загрузить криптоконтейнер.

Если этот флажок установлен, Kaspersky Endpoint Security использует двустороннюю аутентификацию для подключения к серверу KATA.

Если этот флажок снят, Kaspersky Endpoint Security не использует двустороннюю аутентификацию для подключения к серверу KATA.

Этот флажок по умолчанию снят.

Загрузить криптоконтейнер

При нажатии на кнопку открывается окно, в котором вы можете выбрать криптоконтейнер, который будет использоваться для двусторонней аутентификации. Файл криптоконтейнера имеет расширение .PFX.

Примечание. Криптоконтейнер должен быть защищен паролем. Невозможно добавить криптоконтейнер с пустым паролем.

Пароль от криптоконтейнера

Пароль для криптоконтейнера, используемого для двусторонней аутентификации.

Раздел Контроль безопасности

Развернуть всё | Свернуть всё

Веб-Контроль

Переключатель **Веб-Контроль** включает/выключает Веб-Контроль.

Если переключатель **Веб-Контроль** включен, вы можете создавать правила посещения сайтов для пользователей удаленных компьютеров.

Если переключатель **Веб-Контроль** выключен, вы не можете управлять посещением сайтов пользователями удаленных компьютеров.

Этот переключатель выключен по умолчанию.

Список правил

Список содержит созданные вами правила для управления доступом к сайтам, которые пользователи открывают на удаленных компьютерах.

Порядок, в котором расположены правила, определяет приоритет их применения приложением Kaspersky Endpoint Security.

Добавить

При нажатии на кнопку открывается окно, в котором вы можете создать новое правило Веб-Контроля.

Удалить

При нажатии на кнопку выбранное правило удаляется из списка.

Кнопка доступна, если установлен флажок рядом с правилом.

Вверх

При нажатии на кнопку выбранное правило поднимается в списке правил, что повышает приоритет его выполнения приложением Kaspersky Endpoint Security.

Вниз

При нажатии на кнопку выбранное правило опускается в списке правил, что понижает приоритет его выполнения приложением Kaspersky Endpoint Security.

Имя

Название правила.

Состояние

Переключатель в этой графе определяет, активно правило или нет.

Вы можете включать/выключать переключатель для соответствующего правила, чтобы изменить состояние правила.

Действие

Действие, которое Kaspersky Endpoint Security выполняет, когда пользователь открывает веб-адрес, попадающий под действие правила.

Вы можете изменить выбранное действие, выбрав другой вариант действия в контекстном меню в этой графе.

Принудительно

Если переключатель **Принудительно** включен, Kaspersky Endpoint Security запрещает изменение значений в параметрах задач, параметрах приложения, в политиках вложенных групп и подчиненных Серверов администрирования.

Если переключатель **Принудительно** выключен, Kaspersky Endpoint Security разрешает изменение значений в параметрах задач, параметрах приложения, в политиках вложенных групп и подчиненных Серверов администрирования.

Окно Изменение правила

Развернуть всё | Свернуть всё

Поле ввода названия правила

Название правила.

В блоке **Состояние** вы можете выбрать, будет правило активным или неактивным.

Активное

Если выбран этот вариант, новое правило будет активным. Это правило будет выполняться для удаленного компьютера после того, как к нему будет применена политика.

Неактивное

Если выбран этот вариант, новое правило будет неактивным. Когда политика будет применена к удаленному компьютеру, это правило не будет выполняться.

В блоке **Действие** вы можете выбрать действие, которое Kaspersky Endpoint Security выполняет, когда пользователь открывает веб-адрес, попадающий под действие правила.

Разрешать

Kaspersky Endpoint Security разрешает пользователю посещение веб-адресов, попадающих под действие правила.

Примечание. Kaspersky Endpoint Security разрешает посещение веб-ресурсов на удаленном компьютере, если в окне **Сеть** мастера создания политики включен переключатель **Проверка защищенных соединений (HTTPS)**.

Этот вариант выбран по умолчанию.

Блокировать

Kaspersky Endpoint Security блокирует веб-адреса, попадающие под действие правила, когда пользователь пытается их открыть.

Примечание. Когда пользователь пытается получить доступ к веб-ресурсам, заблокированным Веб-Контролем на удаленном компьютере, Kaspersky Endpoint Security показывает уведомления, если в окне **Сеть** мастера создания политики включен переключатель **Проверка защищенных соединений (HTTPS)**.

Предупреждать

Kaspersky Endpoint Security показывает предупреждение, когда пользователь пытается открыть веб-адрес, попадающий под действие правила.

В блоке **Область применения** вы можете выбрать область, к которой будет применяться правило: веб-адрес или группа веб-адресов, или категории сайтов.

Категории

Вы можете создать правило для сайтов по категориям.

Выберите категории

При нажатии на ссылку открывается диалоговое окно, в котором вы можете выбрать категории сайтов, попадающие под действие правила.

Отдельные адреса

Вы можете создать правило для отдельного веб-адреса или группы веб-адресов.

Этот вариант выбран по умолчанию.

Добавить

При нажатии на кнопку открывается диалоговое окно, в котором вы можете ввести веб-адрес или маску веб-адресов, попадающих под действие правила.

Удалить

При нажатии на кнопку выбранный веб-адрес или маска веб-адресов удаляется из списка веб-адресов, попадающих под действие правила.

Кнопка доступна, если установлен флажок рядом с веб-адресом или маской веб-адресов.

Адрес

Веб-адреса или маски веб-адресов, попадающие под действие правила.

Диалог Добавление веб-адреса

Развернуть всё | Свернуть всё

Поле ввода веб-адреса

Веб-адрес или маска веб-адреса, к которому будет применено правило.

Диалог Категории веб-ресурсов

Развернуть всё | Свернуть всё

Список категорий веб-ресурсов

Список содержит категории сайтов, которые вы можете добавить в правило.

Флажок рядом с названием категории сайтов добавляет в правило или удаляет из правила все сайты, которые принадлежат к этой категории.

Все флажки по умолчанию сняты.

Раздел Базовая защита

Развернуть всё | Свернуть всё

Защита от файловых угроз

При нажатии на ссылку открывается окно, в котором вы можете настроить параметры Защиты от файловых угроз.

Защита от веб-угроз

При нажатии на ссылку открывается окно, в котором вы можете настроить параметры Защиты от веб-угроз.

Защита от сетевых угроз

При нажатии на ссылку открывается окно, в котором вы можете настроить параметры Защиты от сетевых угроз.

Защита от почтовых угроз

При нажатии на ссылку открывается окно, в котором вы можете настроить параметры Защиты от почтовых угроз.

Сетевой экран

При нажатии на ссылку открывается окно, в котором вы можете настроить параметры Сетевого экрана.

Окно Защита от файловых угроз

Развернуть всё | Свернуть всё

Защита от файловых угроз

Переключатель **Защита от файловых угроз** включает/выключает Защиту от файловых угроз.

Если переключатель **Защита от файловых угроз** включен, Kaspersky Endpoint Security постоянно контролирует файловую систему клиентских компьютеров, к которым применена политика.

Если переключатель **Защита от файловых угроз** выключен, Kaspersky Endpoint Security не защищает файловую систему клиентских компьютеров, к которым применена политика.

Этот переключатель включен по умолчанию.

В блоке **Область защиты** вы можете сформировать область защиты, выбрав объекты из списка по умолчанию или добавив другие файлы и папки.

Добавить

При нажатии на кнопку открывается диалоговое окно, в котором вы можете указать файл, папку или маску имени файла или папки для добавления в список объектов области защиты.

Удалить

При нажатии на кнопку объект удаляется из области защиты.

Кнопка доступна, если выбран объект в списке объектов области защиты.

Вы не можете удалить объекты, добавленные в область защиты по умолчанию.

Область защиты

В этой графе отображаются объекты, которые Kaspersky Endpoint Security проверяет, если Защита от файловых угроз включена.

По умолчанию Kaspersky Endpoint Security проверяет следующие объекты:

- **Все съемные диски**. Kaspersky Endpoint Security проверяет все съемные диски.
- **Все внутренние диски**. Kaspersky Endpoint Security проверяет все внутренние диски.
- **Все сетевые диски**. Kaspersky Endpoint Security проверяет все сетевые диски.

Статус

Если переключатель в этой графе включен, Kaspersky Endpoint Security проверяет соответствующий объект в графе **Область защиты**, когда Защита от файловых угроз включена.

Если переключатель в этой графе выключен, Kaspersky Endpoint Security не проверяет соответствующий объект в графе **Область защиты**, когда Защита от файловых угроз включена.

Дополнительно

Значение в этой графе показывает, проверяет ли Kaspersky Endpoint Security папки, вложенные в соответствующий объект.

В блоке **Если обнаружен вредоносный объект** вы можете выбрать действие, которое Kaspersky Endpoint Security выполнит при обнаружении вредоносного объекта.

Запрашивать действие

Kaspersky Endpoint Security выводит на экран окно уведомления с информацией о том, каким вредоносным объектом заражен файл, и предлагает выбрать, какое действие выполнит Kaspersky Endpoint Security. В зависимости от статуса объекта действия могут отличаться.

Этот вариант выбран по умолчанию.

Лечить. Удалять, если лечение невозможно

Kaspersky Endpoint Security блокирует доступ к зараженному файлу и пытается его лечить, не запрашивая подтверждения пользователя.

Если файл вылечен, Kaspersky Endpoint Security восстанавливает его в исходном месте под исходным именем. Если вылечить зараженный файл не удается, Kaspersky Endpoint Security удаляет зараженный файл.

Лечить. Блокировать, если лечение невозможно

Kaspersky Endpoint Security блокирует доступ к зараженному файлу и пытается его лечить, не запрашивая подтверждения пользователя.

Если файл вылечен, Kaspersky Endpoint Security восстанавливает его в исходном месте под исходным именем. Если вылечить зараженный файл не удается, Kaspersky Endpoint Security оставляет его заблокированным в исходном месте.

В блоке **Оптимизация** вы можете настроить производительность проверки и выбрать технологию проверки.

Проверять только новые и измененные файлы

Флажок включает/выключает проверку только тех файлов, которые Kaspersky Endpoint Security распознает как новые или измененные с момента последней проверки.

Если флажок установлен, Kaspersky Endpoint Security проверяет только файлы, признанные новыми или измененными с момента последней проверки.

Если флажок снят, Kaspersky Endpoint Security проверяет все файлы.

Этот флажок установлен по умолчанию.

Пропускать проверку системного тома «только для чтения»

Флажок включает/выключает проверку системного тома "только для чтения".

Если флажок установлен, Kaspersky Endpoint Security пропускает проверку системного тома "только для чтения". Время выполнения проверки значительно уменьшается.

Если флажок снят, Kaspersky Endpoint Security проверяет системный том "только для чтения".

Этот флажок установлен по умолчанию.

Использовать технологию iSwift

Флажок включает/выключает использование технологии iSwift при выполнении проверки. Технология iSwift позволяет Kaspersky Endpoint Security использовать специальный алгоритм для исключения некоторых объектов из проверки. Это помогает увеличить скорость проверки.

Если флажок установлен, Kaspersky Endpoint Security использует iSwift во время проверки.

Если флажок снят, Kaspersky Endpoint Security не использует iSwift во время проверки.

Этот флажок установлен по умолчанию.

В блоке **Типы файлов** вы можете выбрать файлы, которые Kaspersky Endpoint Security проверяет, когда Защита от файловых угроз включена.

Проверять все файлы

Kaspersky Endpoint Security проверяет все запускаемые, открываемые и сохраняемые объекты файловой системы.

Проверять программы и документы по содержимому

Kaspersky Endpoint Security проверяет только заражаемые файлы на основании содержимого файла.

Проверять программы и документы по расширению

Kaspersky Endpoint Security проверяет только заражаемые файлы на основании расширения файла.

Перечень расширений определен "Лабораторией Касперского" и является частью баз Kaspersky Endpoint Security.

Kaspersky Endpoint Security всегда проверяет файлы без расширения.

В блоке **Составные файлы** вы можете выбрать типы составных файлов, которые Kaspersky Endpoint Security проверяет, когда Защита от файловых угроз включена.

Проверять архивы

Флажок включает/выключает проверку архивов. Перечень расширений включен в справку Kaspersky Endpoint Security.

Если флажок установлен, Kaspersky Endpoint Security проверяет архивы.

Если флажок снят, Kaspersky Endpoint Security пропускает архивы при проверке.

Проверять инсталляционные пакеты

Этот флажок включает/выключает проверку инсталляционных пакетов.

Если флажок установлен, Kaspersky Endpoint Security проверяет инсталляционные пакеты.

Если флажок снят, Kaspersky Endpoint Security пропускает инсталляционные пакеты при проверке.

Проверять вложенные OLE-объекты

Флажок включает/выключает проверку вложенных в файлы объектов (например, Excel-таблицы, макросы, вложения в сообщениях электронной почты).

Если флажок установлен, Kaspersky Endpoint Security проверяет вложенные OLE-объекты.

Если флажок снят, Kaspersky Endpoint Security пропускает вложенные OLE-объекты при проверке.

Не распаковывать, если архив больше <значение> МБ

Этот флажок включает/выключает ограничение размера проверяемых архивов.

Если флажок установлен, Kaspersky Endpoint Security пропускает при проверке архивы, размер которых превышает указанное значение.

Если флажок снят, Kaspersky Endpoint Security распаковывает и проверяет архивы независимо от их размера.

Флажок доступен, если установлен флажок **Проверять архивы**.

Отложить распаковывание, если архив больше <значение> МБ

Параметр позволяет ограничить размер проверяемых архивов.

Если флажок установлен, Kaspersky Endpoint Security проверяет все архивы, размер которых превышает установленное значение, но с более низким приоритетом через две минуты после обнаружения такого архива.

Если флажок снят, Kaspersky Endpoint Security проверяет все архивы вне зависимости от приоритета.

Флажок доступен, если установлен флажок **Проверять архивы**.

Принудительно

Если переключатель **Принудительно** включен, Kaspersky Endpoint Security запрещает изменение значений в параметрах задач, параметрах приложения, в политиках вложенных групп и подчиненных Серверов администрирования.

Если переключатель **Принудительно** выключен, Kaspersky Endpoint Security разрешает изменение значений в параметрах задач, параметрах приложения, в политиках вложенных групп и подчиненных Серверов администрирования.

Диалог Добавление объекта в область защиты

Развернуть всё | Свернуть всё

Поле ввода имени либо маски имени файла или папки

Путь к файлу, папке или маска имени файла или папки.

Объект является папкой

Флажок включает/выключает проверку объекта как папки.

Если флажок установлен, Kaspersky Endpoint Security проверяет объект, который вы указали в поле **Укажите имя либо маску имени файла или папки**, как папку.

Если флажок снят, Kaspersky Endpoint Security проверяет объект, который вы указали в поле **Укажите имя либо маску имени файла или папки**, как файл.

Этот флажок установлен по умолчанию.

Включить вложенные папки

Флажок включает/выключает проверку папок, вложенных в папку, указанную в поле **Укажите имя либо маску имени файла или папки**.

Если флажок установлен, Kaspersky Endpoint Security проверяет вложенные папки при поиске вредоносного ПО.

Если флажок снят, Kaspersky Endpoint Security проверяет только файлы в папке, указанной в поле **Укажите имя либо маску имени файла или папки**.

Этот флажок установлен по умолчанию.

Окно Защита от веб-угроз

Развернуть всё | Свернуть всё

Защита от веб-угроз

Переключатель **Защита от веб-угроз** включает/выключает Защиту от веб-угроз.

Если переключатель **Защита от веб-угроз** включен, Защита от веб-угроз проверяет данные, полученные вашим компьютером или отправленные с него по протоколам HTTP и HTTPS через веб-браузеры Safari, Google Chrome и Firefox.

Если переключатель **Защита от веб-угроз** выключен, данные, поступающие на ваш компьютер и отправляющиеся с него через веб-браузеры, не проверяются.

Этот переключатель включен по умолчанию.

В блоке **Если обнаружен вредоносный объект** вы можете выбрать действие, которое Kaspersky Endpoint Security выполнит при обнаружении вредоносного объекта.

Запрашивать действие

Kaspersky Endpoint Security выводит на экран окно уведомления с информацией о том, какой вредоносной программой заражен объект веб-трафика, и предлагает выбрать, какое действие Kaspersky Endpoint Security выполнит над этим объектом. В зависимости от статуса объекта действия могут отличаться.

Этот вариант действия используется по умолчанию.

Блокировать автоматически

Kaspersky Endpoint Security автоматически блокирует доступ к опасным объектам веб-трафика.

В блоке **Доверенные веб-адреса** вы можете создать или изменить список доверенных веб-адресов и включить или выключить проверку трафика, поступающего с веб-адресов из этого списка.

Не проверять веб-трафик с доверенных веб-адресов

Флажок включает/выключает проверку веб-трафика с доверенных веб-адресов.

Если флажок установлен, Kaspersky Endpoint Security не проверяет веб-трафик с доверенных адресов.

Если флажок снят, Kaspersky Endpoint Security проверяет веб-трафик с доверенных адресов.

Этот флажок по умолчанию снят.

Список веб-адресов

Список содержит доверенные веб-адреса.

Вы можете снять флажок рядом с веб-адресом в списке. Если флажок снят, Защита от веб-угроз проверяет веб-трафик с этого веб-адреса.

Список доступен, если установлен флажок **Не проверять веб-трафик с доверенных веб-адресов**.

Добавить

При нажатии на кнопку открывается диалоговое окно, в котором вы можете ввести веб-адрес или маску веб-адреса для добавления в список доверенных веб-адресов.

Удалить

При нажатии на кнопку выбранный веб-адрес или маска веб-адреса удаляется из списка доверенных веб-адресов.

Кнопка доступна, если выбран веб-адрес или маска веб-адреса в списке доверенных веб-адресов.

Веб-адрес

В этой графе отображаются доверенные веб-адреса.

Статус

Если переключатель в этой графе включен, Kaspersky Endpoint Security не проверяет соответствующий объект в графе **Веб-адрес**, когда Защита от веб-угроз включена и установлен флажок **Не проверять веб-трафик с доверенных веб-адресов**.

Если переключатель в этой графе выключен, Kaspersky Endpoint Security проверяет соответствующий объект в графе **Веб-адрес**, когда Защита от веб-угроз включена и установлен флажок **Не проверять веб-трафик с доверенных веб-адресов**.

Принудительно

Если переключатель **Принудительно** включен, Kaspersky Endpoint Security запрещает изменение значений в параметрах задач, параметрах приложения, в политиках вложенных групп и подчиненных Серверов администрирования.

Если переключатель **Принудительно** выключен, Kaspersky Endpoint Security разрешает изменение значений в параметрах задач, параметрах приложения, в политиках вложенных групп и подчиненных Серверов администрирования.

Диалог Добавление веб-адреса

Развернуть всё | Свернуть всё

Поле ввода веб-адреса

Веб-адрес или маска веб-адреса, который не проверяется Защитой от веб-угроз.

В блоке **Статус** вы можете выбрать, будет ли Kaspersky Endpoint Security проверять трафик с этого веб-адреса или группы веб-адресов.

Выключить

Веб-адрес или группа веб-адресов добавляются в список **Доверенные веб-адреса**, но Kaspersky Endpoint Security проверяет поступающий с него/них трафик.

Включить

Веб-адрес или группа веб-адресов добавляются в список **Доверенные веб-адреса** и Kaspersky Endpoint Security не проверяет поступающий с него/них трафик.

Окно Защита от сетевых угроз

Развернуть всё | Свернуть всё

Защита от сетевых угроз

Переключатель **Защита от сетевых угроз** включает/выключает Защиту от сетевых угроз.

Если переключатель **Защита от сетевых угроз** включен, Kaspersky Endpoint Security защищает удаленный компьютер от сетевых атак.

Если переключатель **Защита от сетевых угроз** выключен, Kaspersky Endpoint Security не защищает удаленный компьютер от сетевых атак.

Этот переключатель включен по умолчанию.

В блоке **Параметры Защиты от сетевых угроз** вы можете изменить период времени, на который Kaspersky Endpoint Security блокирует атакующие компьютеры.

Блокировать атакующие компьютеры на <значение> мин

Флажок включает/выключает добавление атакующих компьютеров в список заблокированных компьютеров на указанный период времени.

Если флажок установлен, Kaspersky Endpoint Security добавляет атакующие компьютеры в список заблокированных компьютеров на указанный период времени.

Если флажок снят, Kaspersky Endpoint Security не блокирует атакующие компьютеры.

Этот флажок установлен по умолчанию.

По умолчанию атакующие компьютеры блокируются на 60 минут.

В блоке **Исключения** вы можете создать или изменить список IP-адресов удаленных компьютеров, сетевую активность которых Kaspersky Endpoint Security не блокирует никогда.

Список IP-адресов

Содержит IP-адреса удаленных компьютеров, сетевую активность которых Kaspersky Endpoint Security не блокирует никогда.

Добавить

При нажатии на кнопку открывается диалоговое окно, в котором вы можете ввести IP-адрес удаленного компьютера.

Удалить

При нажатии на кнопку выбранный IP-адрес удаляется из списка IP-адресов.

Кнопка доступна, если выбран IP-адрес удаленного компьютера в списке IP-адресов.

Принудительно

Если переключатель **Принудительно** включен, Kaspersky Endpoint Security запрещает изменение значений в параметрах задач, параметрах приложения, в политиках вложенных групп и подчиненных Серверов администрирования.

Если переключатель **Принудительно** выключен, Kaspersky Endpoint Security разрешает изменение значений в параметрах задач, параметрах приложения, в политиках вложенных групп и подчиненных Серверов администрирования.

Диалог Добавление исключения

Развернуть всё | Свернуть всё

Поле ввода IP-адреса

IP-адрес удаленного компьютера.

Раздел Продвинутая защита

Развернуть всё | Свернуть всё

В блоке **Параметры KSN** вы можете настроить параметры использования Kaspersky Security Network.

Kaspersky Security Network

Переключатель **Использование Kaspersky Security Network** включает/выключает участие в Kaspersky Security Network.

Если переключатель **Использование Kaspersky Security Network** включен, клиентские компьютеры, к которым применяется политика, принимают участие в Kaspersky Security Network.

Если переключатель **Использование Kaspersky Security Network** выключен, клиентские компьютеры, к которым применяется политика, не принимают участие в Kaspersky Security Network.

Этот переключатель выключен по умолчанию.

Расширенный режим работы KSN

Переключатель **Расширенный режим работы KSN** включает/выключает отправку дополнительных данных с удаленного компьютера в "Лабораторию Касперского". Эти данные нужны для улучшения защиты клиентских компьютеров и работы Kaspersky Endpoint Security.

Если переключатель **Расширенный режим работы KSN** включен, с клиентских компьютеров, к которым применяется политика, в Kaspersky Security Network отправляются и данные, которые нужны для работы служб обнаружения, и дополнительные данные.

Если переключатель **Расширенный режим работы KSN** выключен, с клиентских компьютеров, к которым применяется политика, в Kaspersky Security Network отправляются только данные, которые нужны для работы служб обнаружения. Дополнительные данные не отправляются.

Переключатель **Расширенный режим работы KSN** выключен по умолчанию.

Переключатель включается автоматически, если вы включаете переключатель **Использование Kaspersky Security Network**, но вы можете его выключить.

Данные, предоставляемые в "Лабораторию Касперского" при использовании Kaspersky Security Network в глобальном KSN

Если переключатель **Использование Kaspersky Security Network** включен, а переключатель **Расширенный режим работы KSN** выключен, Kaspersky Endpoint Security отправляет в "Лабораторию Касперского" следующие данные:

- Информация об используемой лицензии: тип лицензии и срок ее действия, количество дней до истечения срока действия лицензии, идентификатор партнера, у которого приобретена лицензия, идентификатор регионального центра активации, контрольная сумма кода активации, хеш-сумма тела тикета, рассчитанная по алгоритму SHA1, дата и время создания лицензионного тикета, идентификатор информации о лицензии, идентификатор лицензионного тикета, идентификатор последовательности лицензионного тикета, уникальный идентификатор компьютера пользователя, дата начала и окончания периода валидности лицензионного тикета, текущее состояние лицензионного тикета, версия заголовка тикета, версия лицензии, идентификатор сертификата подписи заголовка тикета, контрольная сумма файла ключа, серийный номер подписчика заголовка тикета, токен авторизации.

- Полная версия установленного ПО;

тип установленного ПО; идентификатор обновления ПО; идентификатор службы репутации; идентификатор типа протокола; идентификатор регионального центра активации; версия списка отозванных заключений службы ПО; идентификатор сработавшей записи в антивирусных базах ПО; временная метка сработавшей записи в антивирусных базах ПО; тип сработавшей записи в антивирусных базах ПО; уникальный идентификатор установки ПО на компьютере; дата активации лицензии; дата окончания срока действия лицензии; идентификатор лицензии; статус лицензии, по которой используется ПО; тип контрольной суммы обрабатываемого объекта; название обнаруженной вредоносной программы или легальной программы, которая может быть использована для нанесения вреда устройству или данным пользователя; контрольная сумма обрабатываемого объекта; контрольная сумма кода активации ПО; полная версия ПО; уникальный идентификатор устройства; идентификатор ПО; контрольная сумма файла ключа, которым активировано ПО; идентификатор информационной модели, примененной при предоставлении лицензии на использование ПО; идентификатор сертификата, которым подписан заголовок лицензионного тикета ПО; дата и время создания лицензионного тикета ПО; контрольная сумма лицензионного тикета ПО; версия лицензионного тикета ПО; версия кода активации ПО; формат данных в запросе к инфраструктуре Правообладателя; идентификатор тикета текущей лицензии; идентификатор компонента ПО; результат действий, выполненных ПО; код ошибки; адрес веб-службы, на который осуществлялось обрабатываемое обращение (веб-адрес, IP); номер порта; веб-адрес источника запроса к веб-службе (referrer); публичный ключ сертификата; отпечаток цифрового сертификата проверяемого объекта и алгоритм хеширования.

Если переключатели **Использование Kaspersky Security Network** и **Расширенный режим работы KSN** включены, Kaspersky Endpoint Security отправляет в "Лабораторию Касперского" следующие данные:

- Информация о версиях установленной на компьютере операционной системы (ОС) и установленных пакетов обновлений, версия и контрольные суммы (MD5, SHA2-256, SHA1) файла ядра ОС, параметры режима работы ОС; версия ОС, номер сборки ОС, номер обновления ОС, редакция ОС, расширенная информация о редакции ОС; версия пакета обновления ОС; дата и время запуска ОС; время задержки обработки события о совершении действия в ОС в подсистеме поведенческого анализа; количество задержанных событий текущего типа, совершенных в ОС; время задержки обработки события о совершении действия в ОС в подсистеме проактивной защиты; количество обработанных событий, совершенных в ОС; количество обработанных синхронных событий, совершенных в ОС; суммарная задержка всех событий текущего типа, совершенных в ОС; время задержки обработки события о совершении действия в ОС в подсистеме постоянного хранения событий; суммарная задержка всех событий, совершенных в ОС; количество ожидающих

синхронных событий, совершенных в ОС; дата и время получения события о совершении действия в ОС.

- Информация о последней неуспешной перезагрузке ОС: количество неуспешных перезагрузок.

- Информация об установленном ПО Правообладателя и состоянии антивирусной защиты компьютера: идентификатор установки ПО (PCID); версия записи в базе данных ПО; уникальный идентификатор установки программы на компьютере, тип программы, идентификатор типа программы, полная версия установленной программы, идентификатор версии настроек программы, идентификатор типа компьютера, уникальный идентификатор компьютера, на котором установлена программа, уникальный идентификатор пользователя в службах Правообладателя, язык локали и ее рабочее состояние, версия установленных компонентов ПО и их рабочее состояние, версия протокола, который используется для подключения к службам Правообладателя; полная версия установленного ПО; тип установленного ПО; идентификатор обновления ПО; идентификатор службы репутации; идентификатор типа протокола; идентификатор регионального центра активации; версия списка отозванных заключений службы ПО; идентификатор сработавшей записи в антивирусных базах ПО; временная метка сработавшей записи в антивирусных базах ПО; тип сработавшей записи в антивирусных базах ПО; уникальный идентификатор установки ПО на компьютере; дата активации лицензии; дата окончания срока действия лицензии; идентификатор лицензии; статус лицензии, по которой используется ПО; тип контрольной суммы обрабатываемого объекта; название обнаруженной вредоносной программы или легальной программы, которая может быть использована для нанесения вреда устройству или данным пользователя; контрольная сумма обрабатываемого объекта; контрольная сумма кода активации ПО; полная версия ПО; идентификатор ПО; контрольная сумма файла ключа, которым активировано ПО; идентификатор информационной модели, примененной при предоставлении лицензии на использование ПО; идентификатор сертификата, которым подписан заголовок лицензионного тикета ПО; дата и время создания лицензионного тикета ПО; контрольная сумма лицензионного тикета ПО; версия лицензионного тикета ПО; версия кода активации ПО; формат данных в запросе к инфраструктуре Правообладателя; идентификатор тикета текущей лицензии; идентификатор компонента ПО; результат действий, выполненных ПО; код ошибки; адрес веб-службы, на который осуществлялось обрабатываемое обращение (веб-адрес, IP); номер порта; веб-адрес источника запроса к веб-службе (referrer); количество циклов обновления и применения антивирусных баз; дата и время последнего обновления и применения антивирусных баз; дата и время выпуска баз ПО; версия компонента ПО; идентификатор обновления ПО; тип установленного ПО; дата и время запуска компонента мониторинг активности; дата и время установки ПО; вероятность отправки статистики компонентом мониторинг активности; код события, обрабатываемого компонентом мониторинг активности дольше

стандартного времени обработки; время обработки события в базах, обработка которого компонентом мониторинг активности длилась дольше стандартного времени; максимально допустимое время обработки события компонентом мониторинг активности; время обработки события, обработка которого компонентом мониторинг активности длилась дольше стандартного времени; общее количество событий, обработка которых компонентом мониторинг активности длилась дольше стандартного времени.

- Данные обо всех обрабатываемых объектах и действиях: заключение ПО по обрабатываемому объекту; код каталога файлов; размер обрабатываемого объекта; контрольная сумма (SHA256) обрабатываемого объекта; номер обнаруженного ПО в контексте компонента мониторинг активности; дата и время обнаружения стороннего ПО компонентом мониторинг активности; характеристики обнаружения; идентификатор сработавшей записи в антивирусных базах ПО; причина обнаружения стороннего ПО компонентом мониторинг активности; контрольная сумма (MD5) обрабатываемого объекта; результат проверки подписи модуля, целостность которого проверяется ПО; имя обрабатываемого объекта; тип сработавшей записи в антивирусных базах ПО; путь к обрабатываемому объекту; имя проверяемого объекта; дата и время проверки; URL-адрес и Referrer, по которому он был загружен; размер проверяемых файлов и пути к ним; признак нахождения в архиве; дата и время создания файла; имя, размер и контрольные суммы (MD5, SHA2-256) упаковщика (если файл был упакован); энтропия файла; тип файла; код типа файла; признак исполняемого файла, идентификатор исполняемого файла и формат исполняемого файла; контрольная сумма объекта (MD5, SHA2-256); тип и значение дополнительной контрольной суммы объекта; данные о ЭЦП (сертификате) объекта: данные об издателе сертификата, количество запусков объекта с момента последней отправки статистики, идентификатор задачи проверки, способ получения информации о репутации объекта, значение фильтра target, технические характеристики по применяемым технологиям обнаружения; путь к обрабатываемому объекту; код каталога файлов.

- Для исполняемых файлов: энтропия разделов файла, признак проверки репутации или подписи файла, название, тип, идентификатор типа, контрольная сумма (MD5) и размер приложения, загруженного проверяемым объектом, путь к приложению и пути к шаблонам, признак нахождения в списке автозапуска, дата записи, список атрибутов, название упаковщика, информация о цифровой подписи приложения: издатель сертификата, название отправляемого файла в формате MIME, дата и время сборки файла.

- Информация о запускаемых программах и их модулях: контрольные суммы запускаемых файлов (MD5, SHA2-256), размер, атрибуты, дата создания, имя упаковщика (если файл был упакован), имена файлов, данные о запущенных в системе процессах (идентификатор процесса в системе (PID), имя процесса, данные об учетной записи, от которой запущен процесс, приложении и команде, запустившей процесс, полный путь к файлам процесса и командная

строка запуска, описание приложения, к которому относится процесс (название приложения и данные об издателе), а также данные об используемых цифровых сертификатах и информация, необходимая для проверки подлинности этих сертификатов, или данные об отсутствии цифровой подписи файла), также информация о загружаемых в процессы модулях: их имена, размер, типы, даты создания, атрибуты, контрольные суммы (MD5, SHA2-256, SHA1), пути к ним, информация заголовка PE-файлов, имена упаковщиков (если файл был упакован), информация о наличии и валидности данных этой статистики, идентификатор условия формирования передаваемой статистики.

- В случае обнаружения угрозы или уязвимости, дополнительно к информации об обнаруженном объекте предоставляется информация об идентификаторе, версии и типе записи в антивирусных базах, название угрозы согласно классификации Правообладателя, дата и время последнего обновления антивирусных баз, имя исполняемого файла, контрольная сумма (MD5) файла приложения, запросившего URL-адрес, в котором произошло обнаружение, IP-адрес (IPv4 или IPv6) обнаруженной угрозы, идентификатор уязвимости и класс ее опасности, URL-адрес и Referrer страницы обнаружения уязвимости.

- В случае обнаружения потенциально вредоносного объекта предоставляется информация о данных в памяти процессов.

- Информация о сетевой атаке: IP-адрес атакующего компьютера и номер порта компьютера пользователя, на который была направлена сетевая атака, идентификатор протокола, по которому выполнялась атака, название и тип атаки.

- Информация о сетевых соединениях: версия и контрольные суммы (MD5, SHA2-256, SHA1) файла процесса, открывшего порт, путь к файлу процесса и его цифровая подпись, локальный и удаленный IP-адреса, номера локального и удаленного портов соединения, состояние соединения, время открытия порта.

- URL и IP-адрес веб-страницы, на которой был обнаружен вредоносный или подозрительный контент, имя, размер и контрольная сумма файла, запросившего данный URL, идентификатор, вес и степень применимости правила, по которому был вынесен вердикт, цель атаки.

- Информация об обновлении установленной программы и антивирусных баз: статус завершения задачи обновления, тип ошибки, которая могла произойти при обновлении, число неуспешных завершений обновления, идентификатор компонента программы, который выполняет обновление.

- Информация об использовании Kaspersky Security Network (далее "KSN"): идентификатор KSN, идентификатор ПО, полная версия ПО, обезличенный IP-адрес устройства пользователя, показатели качества выполнения запросов к KSN, показатели качества обработки пакетов для KSN, показатели количества

запросов в KSN и информация о типах запросов в KSN, дата и время начала передачи статистики, дата и время окончания передачи статистики, информация об обновлениях конфигурации KSN: идентификатор активной конфигурации, идентификатор полученной конфигурации, код ошибки при обновлении конфигурации.

- Информация о событиях в системных журналах: время события, название журнала, в котором обнаружено событие, тип и категория события, название источника события и его описание.

- Информация для определения репутации файлов, URL-адресов и сертификатов: URL-адрес, для которого запрашивается репутация и Referrer, тип протокола соединения, внутренний идентификатор типа программы, номер используемого порта, идентификатор пользователя, контрольная сумма проверяемого файла (MD5), тип обнаруженной угрозы, информация о записи, которая была использована для обнаружения угрозы (идентификатор записи в антивирусной базе, время создания и тип записи); публичный ключ сертификата; отпечаток цифрового сертификата проверяемого объекта и алгоритм хеширования.

- Данные о территориальной распространенности программы: дата установки и дата активации программы, идентификатор партнера, предоставившего лицензию для активации программы, идентификатор программы, идентификатор языковой локализации программы, серийный номер лицензии, по которой программа активирована, признак участия в KSN.

- Информация об используемой лицензии: тип лицензии и срок ее действия, количество дней до истечения срока действия лицензии, идентификатор партнера, у которого приобретена лицензия, идентификатор регионального центра активации, контрольная сумма кода активации, хеш-сумма тела тикета, рассчитанная по алгоритму SHA1, дата и время создания лицензионного тикета, идентификатор информации о лицензии, идентификатор лицензионного тикета, идентификатор последовательности лицензионного тикета, уникальный идентификатор компьютера пользователя, дата начала и окончания периода валидности лицензионного тикета, текущее состояние лицензионного тикета, версия заголовка тикета, версия лицензии, идентификатор сертификата подписи заголовка тикета, контрольная сумма файла ключа, серийный номер подписчика заголовка тикета, токен авторизации.

- Информация об установленном на компьютере аппаратном обеспечении: тип, название, модель, версия прошивки, характеристики встроенных и подключенных устройств.

- Информация об устройстве: идентификатор устройства.

- Информация о работе компонента "Веб-Контроль":

версия компонента, причина категоризации, дополнительная информация о причине категоризации, категоризированный URL-адрес, IP-адрес хоста заблокированного/категоризированного объекта.

Облачный режим

Переключатель **Облачный режим** включает/выключает режим работы приложения, в котором Kaspersky Endpoint Security использует облегченную версию баз вредоносного ПО. Этот режим доступен только в том случае, если включено участие в Kaspersky Security Network. Облегченная версия баз вредоносного ПО позволяет снизить нагрузку на оперативную память компьютера примерно в два раза. Если вы не участвуете в Kaspersky Security Network или облачный режим выключен, Kaspersky Endpoint Security загружает полную версию баз вредоносного ПО с серверов "Лаборатории Касперского".

Если переключатель включен, то Kaspersky Endpoint Security использует облегченную версию баз вредоносного ПО, за счет чего снижается нагрузка на ресурсы операционной системы.

Примечание. Kaspersky Endpoint Security загружает облегченную версию баз вредоносного ПО в ходе ближайшего обновления после того, как флажок был установлен.

Если переключатель выключен, то Kaspersky Endpoint Security использует полную версию баз вредоносного ПО.

Примечание. Kaspersky Endpoint Security загружает полную версию баз вредоносного ПО в ходе ближайшего обновления после того, как флажок был снят.

Положение о KSN

При нажатии на ссылку открывается окно, в котором вы можете прочитать Положение о Kaspersky Security Network и принять условия участия в Kaspersky Security Network.

Примечание. Если вы управляете Kaspersky Endpoint Security через Kaspersky Security Center Web Console и в зависимости от настроек Kaspersky Security Center, вы можете участвовать в Kaspersky Private Security Network вместо Kaspersky Security Network. Если вы управляете Kaspersky Endpoint Security через Kaspersky Security Center Cloud Console, участие в Kaspersky Private Security Network невозможно. Подробную информацию об участии в Kaspersky Private Security Network вы можете найти в справке Kaspersky Security Center.

В блоке **Параметры KSN-прокси** вы можете настроить параметры использования KSN-прокси.

Использовать KSN-прокси

Флажок включает/выключает использование прокси-сервера при подключении к Kaspersky Security Network.

Если флажок установлен, Kaspersky Endpoint Security использует прокси-сервер при подключении к Kaspersky Security Network.

Если флажок снят, Kaspersky Endpoint Security подключается напрямую к Kaspersky Security Network.

Этот флажок по умолчанию снят.

Использовать серверы «Лаборатории Касперского», если KSN-прокси недоступен

Флажок включает/выключает использование серверов "Лаборатории Касперского", если KSN-прокси недоступен.

Если флажок установлен, Kaspersky Endpoint Security использует серверы "Лаборатории Касперского", если KSN-прокси недоступен.

Если флажок снят, Kaspersky Endpoint Security не использует серверы "Лаборатории Касперского", если KSN-прокси недоступен.

Этот флажок по умолчанию снят.

Флажок доступен, если установлен флажок **Использовать KSN-прокси**.

Принудительно

Если переключатель **Принудительно** включен, Kaspersky Endpoint Security запрещает изменение значений в параметрах задач, параметрах приложения, в политиках вложенных групп и подчиненных Серверов администрирования.

Если переключатель **Принудительно** выключен, Kaspersky Endpoint Security разрешает изменение значений в параметрах задач, параметрах приложения, в политиках вложенных групп и подчиненных Серверов администрирования.

Окно Участие в Kaspersky Security Network/Kaspersky Private Security Network

Развернуть всё | Свернуть всё

Подробнее

При нажатии на ссылку открывается окно браузера, в котором вы можете прочитать текст Положения о Kaspersky Security Network или Положения о Kaspersky Private Security Network.

Я принимаю условия участия в Kaspersky Security Network/Kaspersky Private Security Network

Компьютеры, к которым применена политика, участвуют в Kaspersky Security Network/Kaspersky Private Security Network.

Я не принимаю условия участия в Kaspersky Security Network/Kaspersky Private Security Network

Компьютеры, к которым применена политика, не участвуют в Kaspersky Security Network/Kaspersky Private Security Network.

Примечание. Если вы управляете Kaspersky Endpoint Security через Kaspersky Security Center Cloud Console, участие в Kaspersky Private Security Network невозможно. Подробную информацию об участии в Kaspersky Private Security Network вы можете найти в справке Kaspersky Security Center .

Диалог Предоставление доступа

Развернуть всё | Свернуть всё

Получить ключ восстановления

При нажатии на кнопку создается ключ восстановления, который нужен для получения доступа к зашифрованному диску на клиентском компьютере.

Управление приложением из командной строки

Вы можете работать с приложением Kaspersky Endpoint Security посредством командной строки.

Примечание. После установки обновлений модулей Kaspersky Endpoint Security версия клиента приложения в командной строке может отличаться от установленной версии приложения.

Синтаксис командной строки:

```
kav <команда> <параметры>
```

Каждая команда имеет свой набор параметров.

Просмотр справки командной строки

Чтобы просмотреть информацию по синтаксису командной строки, используйте следующую команду:

```
kav -? | help
```

Запуск задач поиска вредоносного ПО

Синтаксис команды:

```
kav scan <область проверки> <действие> <типы файлов> <исключения> <параметры отчета> <дополнительные параметры>
```

Примечание. Чтобы запустить задачу поиска вредоносного ПО, вы также можете использовать задачи, созданные в приложении, запуская их из командной строки. При этом задача выполняется с параметрами, установленными в интерфейсе Kaspersky Endpoint Security.

Описание параметров

`<область проверки>` – перечень объектов, которые проверяются на наличие вредоносного кода. Вы можете указать несколько параметров, разделив их пробелом.

Примечание. Kaspersky Endpoint Security не проверяет файлы, расположенные в хранилищах OneDrive, iCloud и других облачных хранилищах. Исключите эти файлы из области проверки. В противном случае задача проверки может завершиться с ошибкой *Зараженный файл не удален*.

Возможны следующие значения:

- `<файлы>` – список путей к файлам и папкам для проверки. Вы можете указать как абсолютный, так и относительный путь к файлам. Элементы списка должны быть разделены пробелом.

  Примечание. Если имя объекта или путь к нему содержит пробел или специальные символы (например, $, &, @ и пр.), необходимо заключить его в одинарные кавычки (' '), либо экранировать исключаемый символ, добавив непосредственно перед ним обратную косую черту (\). Если указана конкретная папка, проверяются все файлы и папки, содержащиеся в ней.

- `-all` – полная проверка компьютера.
- `-remdrives` – все съемные диски.
- `-fixdrives` – все локальные диски.
- `-netdrives` – все сетевые диски.
- `-@:<filelist.lst>` – путь к файлу со списком объектов и папок, входящих в область проверки. Файл должен быть в текстовом формате; каждый объект проверки необходимо указывать с новой строки. Допускается ввод только абсолютного пути к файлу.

`<действие>` – указывает действие над вредоносными объектами, обнаруженными в ходе проверки. Если параметр не задан, по умолчанию выполняется действие, соответствующее значению `-i8`.

Возможны следующие значения:

- `-i0` – не выполнять никаких действий, только сохранять информацию об объекте в отчете;
- `-i1` – лечить зараженные объекты; если лечение невозможно – пропускать;
- `-i2` – лечить зараженные объекты; если лечение невозможно – удалять; не удалять контейнеры, кроме контейнеров с исполняемым заголовком (SFX-архивов);
- `-i3` – лечить зараженные объекты; если лечение невозможно – удалять; удалять контейнеры полностью, если невозможно удалить вложенные зараженные файлы;
- `-i4` – удалять зараженные объекты; удалять контейнеры полностью, если невозможно удалить вложенные зараженные файлы;
- `-i8` – запрашивать действие у пользователя при обнаружении зараженного объекта (используется по умолчанию);
- `-i9` – запрашивать действие у пользователя по окончании проверки.

`<типы файлов>` – определяет типы файлов, которые проверяются при поиске вредоносного ПО. Если параметр не задан, по умолчанию проверяются только потенциально заражаемые файлы (по содержимому).

Возможны следующие значения:

- `-fe` – проверять только потенциально заражаемые файлы по расширению;
- `-fi` – проверять только потенциально заражаемые файлы по содержимому (это значение установлено по умолчанию);
- `-fa` – проверять все файлы.

`<исключения>` – определяет объекты, исключаемые из проверки. Вы можете указать несколько параметров, разделив их пробелом.

Возможны следующие значения:

- `-e:a` – не проверять архивы;
- `-e:b` – не проверять почтовые базы;

- `-e:m` – не проверять почтовые сообщения в текстовом формате;
- `-e:<маска>` – не проверять объекты по маске;
- `-e:<секунды>` – пропускать объекты, проверка которых занимает больше заданного времени (в секундах);
- `-es:<размер>` – пропускать объекты, размер которых превышает указанное значение (в мегабайтах).

`<параметры отчета>` – определяют формат отчета о результатах проверки. Вы можете указать как абсолютный, так и относительный путь к файлу отчета. Если параметр не задан, результаты проверки выводятся на экран и отображаются все события.

Возможны следующие значения:

- `-r:<файл отчета>` – записывать в указанный файл отчета только важные события;
- `-ra:<файл отчета>` – записывать в указанный файл отчета все события.

`<дополнительные параметры>` – параметры, определяющие использование технологий поиска вредоносного ПО и конфигурационных файлов:

- `-iSwift=<on|off>` – включить/отключить использование технологии iSwift;
- `-c:<конфигурационный файл>` – определяет путь к конфигурационному файлу, содержащему настройки приложения для выполнения задач поиска вредоносного ПО. Вы можете указать как абсолютный, так и относительный путь к файлу. Если параметр не задан, наряду со значениями, указанными в командной строке, используются значения, установленные в интерфейсе приложения.

Пример:

Запустить проверку папок ~/Documents, /Applications и файла my test.exe:

```
kav scan ~/Documents /Applications 'my test.exe'
```

Проверить объекты, список которых приведен в файле objects2scan.txt. Использовать для работы конфигурационный файл scan_settings.txt. По результатам проверки сформировать отчет, в котором зафиксировать все события:

```
kav scan -@:objects2scan.txt -c:scan_settings.txt -ra:scan.log
```

Пример конфигурационного файла:

```
-netdrives -@:objects2scan.txt -ra:scan.log
```

Обновление приложения

Синтаксис команды:

```
kav update <источник обновления> <параметры отчета> <дополнительные параметры>
```

Описание параметров

`<источник обновлений>` – HTTP-сервер либо сетевая или локальная папка, из которой загружаются обновления. Если путь не указан, источник обновлений будет взят из параметров обновления приложения.

`<параметры отчета>` – определяют формат отчета о результатах проверки. Вы можете указать как абсолютный, так и относительный путь к файлу отчета. Если параметр не задан, результаты проверки выводятся на экран и отображаются все события.

Возможны следующие значения:

- `-r:<файл отчета>` – записывать в указанный файл отчета только важные события;
- `-ra:<файл отчета>` – записывать в указанный файл отчета все события.

`<дополнительные параметры>` – параметр, определяющий использование конфигурационного файла.

`-c:<имя конфигурационного файла>` – определяет путь к конфигурационному файлу, содержащему настройки приложения для выполнения обновления. Вы можете указать как абсолютный, так и относительный путь к файлу. Если параметр не задан, используются значения, установленные в интерфейсе программы.

Пример:

Обновить базы программы из источника по умолчанию, зафиксировав все события в отчете:

```
kav update -ra:avbases_upd.txt
```

Обновить модули Kaspersky Endpoint Security, используя параметры конфигурационного файла updateapp.ini:

```
kav update -app=on -c:updateapp.ini
```

Откат последнего обновления

Синтаксис команды:

```
kav rollback <параметры отчета>
```

Важно! Для выполнения команды требуются права администратора.

Описание параметров

`<параметры отчета>` – определяет формат отчета о результатах отката обновления. Вы можете указать как абсолютный, так и относительный путь к файлу отчета. Если параметр не задан, результаты проверки выводятся на экран и отображаются все события.

Возможны следующие значения:

- `-r:<файл отчета>` – записывать в указанный файл отчета только важные события;
- `-ra:<файл отчета>` – записывать в указанный файл отчета все события.

Пример:

```
kav rollback -ra:rollback.txt
```

Запуск и остановка компонента или задачи

Синтаксис команды start:

```
kav start <имя задачи или компонента> <параметры отчета>
```

Синтаксис команды stop:

```
kav stop <имя задачи или компонента>
```

Важно! Для выполнения команды stop требуются права администратора.

Описание параметров

`<имя задачи или компонента>` – укажите одно из следующих значений:

- `fm` или `file_monitoring` – для Защиты от файловых угроз;
- `wm` или `web_monitoring` – для Защиты от веб-угроз;
- `ids` – для Защиты от сетевых угроз;
- `full` или `scan_my_computer` – для задачи Полная проверка;
- `scan_objects` – для задачи Выборочная проверка;
- `quick` или `scan_critical_areas` – для задачи Быстрая проверка;
- `updater` – для задачи обновления;
- `rollback` – для задачи отката обновления.

`<параметры отчета>` – параметры, определяющие формат отчета о результатах работы компонента или выполнении задачи. Вы можете указать как абсолютный, так и относительный путь к файлу отчета. Если параметр не задан, Kaspersky Endpoint Security отображает результаты в соответствии с настройками, заданными в графическом интерфейсе пользователя.

Примечание. Параметр `<параметры отчета>` доступен только для значений `scan_objects`, `updater` и `rollback`.

Возможны следующие значения:

- `-r:<файл отчета>` – записывать в указанный файл отчета только важные события;
- `-ra:<файл отчета>` – записывать в указанный файл отчета все события.

Примечание. Компоненты и задачи, запущенные из командной строки, выполняются с настройками, заданными в интерфейсе приложения.

Пример:

Чтобы включить компонент Защита от файловых угроз, введите в командной строке:

```
kav start fm
```

Чтобы остановить задачу полной проверки, введите в командной строке:

```
kav stop scan_my_computer
```

Просмотр статуса и статистики по компоненту или задаче

Синтаксис команды status:

```
kav status <название компонента или задачи>
```

Синтаксис команды statistics:

```
kav statistics <название компонента или задачи>
```

Описание параметров

`<название компонента или задачи>` – укажите одно из следующих значений:

- `fm` или `file_monitoring` – для Защиты от файловых угроз;
- `wm` или `web_monitoring` – для Защиты от веб-угроз;
- `ids` – для Защиты от сетевых угроз;
- `full` или `scan_my_computer` – для задачи Полная проверка;
- `scan_objects` – для задачи Выборочная проверка;
- `quick` или `scan_critical_areas` – для задачи Быстрая проверка;
- `updater` – для задачи обновления;
- `rollback` – для задачи отката обновления.

Примечание. Если вы запускаете команду status без параметра `<название компонента или задачи>`, то выводится статус всех задач и компонентов программы. Для команды statistics параметр `<название компонента или задачи>` является обязательным.

Экспорт настроек защиты

Синтаксис команды:

```
kav export <название компонента или задачи> <файл экспорта>
```

Описание параметров

`<название компонента или задачи>` – укажите одно из следующих значений:

- `fm` или `file_monitoring` – для Защиты от файловых угроз;
- `wm` или `web_monitoring` – для Защиты от веб-угроз;
- `ids` – для Защиты от сетевых угроз;
- `full` или `scan_my_computer` – для задачи Полная проверка;
- `scan_objects` – для задачи Выборочная проверка;
- `quick` или `scan_critical_areas` – для задачи Быстрая проверка;
- `updater` – для задачи обновления;
- `rollback` – для задачи отката обновления.

`<файл экспорта>` – путь к файлу, в который экспортируются настройки приложения. Вы можете указать как абсолютный, так и относительный путь к файлу.

Пример:

```
kav export fm fm_settings.txt
```

Активация приложения

Вы можете активировать Kaspersky Endpoint Security с помощью файла ключа.

Синтаксис команды:

```
kav license /add <файл ключа или код активации>
```

Описание параметров

`<файл ключа>` – файл ключа к приложению с расширением key.

`<код активации>` – код активации в формате XXXX-XXXX-XXXX-XXXX.

Пример:

```
kav license /add ./1AA111A1.key
kav license /add A11A1-11111-1A1AA-1A11A
```

Установка системного расширения

Синтаксис команды:

```
kav activatesystemextension /sysext
```

Примечание. Вам необходимо предоставить разрешения для Kaspersky Endpoint Security в разделе настроек **Конфиденциальность и безопасность** для завершения установки расширения.

Настройка соединения с сетью

Вы можете настроить параметры соединения с сетью для компонентов Защита от веб-угроз и Защита от сетевых угроз.

Синтаксис команды:

```
kav activatesystemextension /webav
```

Примечание. Вам необходимо разрешить Kaspersky Endpoint Security фильтровать сетевой трафик для завершения настройки.

Удаление лицензионных ключей

Вы можете удалить все лицензионные ключи, добавленные в приложение.

Синтаксис команды:

```
kav license /del
```

Важно! Для выполнения команды требуются права администратора.

Коды возврата командной строки

Общие коды могут быть возвращены любой командой командной строки. К кодам возврата задач относятся общие коды, а также коды конкретных задач.

Синтаксис команды получения кода возврата:

```
echo $?
```

Общие коды возврата:

- `0` – операция выполнена успешно;
- `1` – неверное значение параметра;
- `2` – неизвестная ошибка;
- `3` – ошибка выполнения задачи;
- `4` – задача отменена.

Коды возврата задач поиска вредоносного ПО:

- `101` – все вредоносные объекты обработаны;
- `102` – обнаружены вредоносные объекты.

Завершение работы приложения

Синтаксис команды:

```
kav exit
```

Важно! Для выполнения команды требуются права администратора.

Удаление приложения

Используйте следующую последовательность команд для удаления Kaspersky Endpoint Security с помощью командной строки:

```
sudo /Library/Application\ Support/Kaspersky\
Lab/klnagent/Binaries/UninstallScript
```

```
sudo /Library/Application\ Support/Kaspersky\
Lab/KAV/Binaries/UninstallScript
sudo rm -rf /Library/Application\ Support/Kaspersky\ Lab/
/Applications/Kaspersky
```

Важно! Для удаления приложения требуются права администратора.

Команды управления Detection and Response

Вы можете управлять встроенными функциями решения Detection and Response из командной строки. Вы можете управлять решениями Detection and Response, если управление через консоль Kaspersky Security Center невозможно.

Управление Запретом запуска

Вы можете просматривать параметры Запрета запуска на клиентском компьютере, а также выключать Запрет запуска на нем.

Синтаксис команды:

```
kav prevention </disable | /show>
```

Описание команд

`/disable` – команда выключения Запрета запуска на клиентском компьютере.

`/show` – команда для отображения текущих параметров Запрета запуска, включая режим работы и список правил запрета запуска.

Управление Сетевой изоляцией

Вы можете просматривать параметры Сетевой изоляции на узле, а также выключать Сетевую изоляцию на узле.

Синтаксис команды:

```
kav isolation </off | /status>
```

Описание команд

`/off` – команда выключения Сетевой изоляции.

Важно! Для выполнения команды требуются права администратора.

`/status` – команда для отображения статуса Сетевой изоляции и исключений.

Примечание. Эти команды необходимо запускать одновременно.

Обращение в Службу технической поддержки

В этом разделе описывается, как получить техническую поддержку и на каких условиях она доступна.

Способы получения технической поддержки

Если вы не нашли решения вашей проблемы в документации к Kaspersky Endpoint Security или в других источниках информации о Kaspersky Endpoint Security, обратитесь в Службу технической поддержки. Сотрудники Службы технической поддержки ответят на ваши вопросы об установке и использовании Kaspersky Endpoint Security.

Примечание. "Лаборатория Касперского" предоставляет поддержку Kaspersky Endpoint Security в течение всего жизненного цикла приложения (см. страницу жизненного цикла приложений). Перед обращением в Службу технической поддержки ознакомьтесь с правилами предоставления технической поддержки .

Вы можете связаться со специалистами Службы технической поддержки одним из следующих способов:

- посетить сайт Службы технической поддержки;
- отправить запрос в Службу технической поддержки "Лаборатории Касперского" с портала Kaspersky CompanyAccount .

Техническая поддержка через Kaspersky CompanyAccount

Kaspersky CompanyAccount – это портал для организаций, использующих приложения "Лаборатории Касперского". Портал Kaspersky CompanyAccount предназначен для взаимодействия пользователей со специалистами "Лаборатории Касперского" с помощью электронных запросов. На портале Kaspersky CompanyAccount вы можете отслеживать статус обработки электронных запросов специалистами "Лаборатории Касперского" и хранить историю электронных запросов.

Вы можете зарегистрировать всех сотрудников вашей организации в рамках одной учетной записи Kaspersky CompanyAccount. Одна учетная запись позволяет вам централизованно управлять электронными запросами от зарегистрированных сотрудников в "Лабораторию Касперского", а также управлять правами этих сотрудников в Kaspersky CompanyAccount.

Портал Kaspersky CompanyAccount доступен на следующих языках:

- английском;
- испанском;
- итальянском;
- немецком;
- польском;
- португальском;
- русском;
- французском;
- японском.

Вы можете узнать больше о Kaspersky CompanyAccount на сайте Службы технической поддержки .

Отправка информации для Службы технической поддержки

Для более эффективного оказания поддержки в случае возникновения вопросов по работе приложения специалисты Службы технической поддержки могут попросить вас в отладочных целях на время проведения работ по диагностике изменить параметры приложения. Для этого может потребоваться выполнение следующих действий:

- Активировать функциональность, предназначенную для получения расширенной диагностической информации.
- Выполнить более тонкую настройку работы отдельных компонентов приложения, недоступную через стандартные средства пользовательского интерфейса.
- Изменить параметры отправки полученной диагностической информации.

Вся необходимая для выполнения перечисленных действий информация, а также состав полученных в отладочных целях данных будут сообщены вам специалистами Службы технической поддержки. Полученная расширенная диагностическая информация сохраняется на компьютере пользователя. Автоматическая пересылка данных в "Лабораторию Касперского" не выполняется.

Использование файла трассировки

После того как вы сообщите специалистам Службы технической поддержки "Лаборатории Касперского" о возникшей проблеме, они могут попросить вас сформировать отчет с информацией о работе Kaspersky Endpoint Security и отправить его в Службу технической поддержки "Лаборатории Касперского". Также специалисты Службы технической поддержки "Лаборатории Касперского" могут попросить вас создать *файл трассировки*. Файл трассировки позволяет выполнить пошаговую проверку исполнения команд приложения и установить, когда возникает ошибка.

Создание файла трассировки

Трассировка является эффективным способом записи подробной информации о функционировании приложения. Специалисты Службы технической поддержки используют файлы трассировки для устранения неисправностей.

Создание файла трассировки

1. В строке меню нажмите на значок приложения и выберите пункт **Настройки**.

   Откроется окно настройки приложения.

2. На вкладке **Интерфейс** в блоке **Трассировка** установите флажок **Включить трассировку**.

Важно! Рекомендуется использовать трассировку только под руководством специалиста Службы технической поддержки "Лаборатории Касперского".

Для записи файлов трассировки может потребоваться много места на диске. Если файлы трассировки больше не нужны, выключите трассировку.

Выключение трассировки

1. В строке меню нажмите на значок приложения и выберите пункт **Настройки**.

   Откроется окно настройки приложения.

2. На вкладке **Интерфейс** в блоке **Трассировка** снимите флажок **Включить трассировку**.

Kaspersky Endpoint Security сохраняет в файле трассировки следующую информацию:

- информацию об устройстве и об установленной на нем операционной системе (уникальный идентификатор устройства, тип устройства, MAC-адреса сетевых устройств, тип операционной системы, версию операционной системы);
- информацию о работе приложения и его модулей;
- информацию о подписке (тип подписки, регион);
- информацию о языке интерфейса, идентификатор приложения, кастомизацию приложения, версию приложения, уникальный идентификатор установки приложения, уникальный идентификатор компьютера;
- информацию о состоянии защиты компьютера от вредоносного ПО, а также данные обо всех обработанных и обнаруженных объектах (название детектируемого объекта, дата и время обнаружения, веб-адрес, по которому он был загружен, названия и размер зараженных файлов и пути к ним, IP-адрес атакующего компьютера и номер порта компьютера Пользователя, на который была направлена сетевая атака, перечень активностей вредоносной программы, нежелательные веб-адреса) и соответствующих действиях и решениях ПО и пользователя по ним;
- информацию о загруженных пользователем программах (веб-адреса, атрибуты, размер файлов, сведения о процессе, который загрузил файл);
- информацию о запускаемых программах и их модулях (размер, атрибуты, дата создания, информация заголовка PE, регион, имя, расположение, упаковщики);
- информацию об ошибках и использовании пользовательского интерфейса установленного ПО "Лаборатории Касперского";
- информацию о сетевых соединениях: IP-адрес удаленного компьютера и компьютера Пользователя, номера портов, через которые устанавливалось соединение, сетевой протокол соединения;

- информацию о сетевых пакетах, получаемых и передаваемых компьютером по информационно-телекоммуникационным сетям;
- информацию об отправляемых и принимаемых сообщениях электронной почты и мгновенных сообщениях;
- информацию о посещаемых веб-адресах: данные о логине и пароле для сайта и содержимое файлов cookie (если соединение устанавливалось по открытому протоколу);
- публичный сертификат сервера.

Файлы трассировки содержат только данные, необходимые для устранения неполадок в работе приложения. "Лаборатория Касперского" использует файлы трассировки в целях расследования инцидентов, связанных с ошибками в работе приложения Kaspersky Endpoint Security.

По умолчанию создание файлов трассировки выключено. Вы можете включить создание файлов трассировки в настройках приложения.

Файлы трассировки можно отправить в "Лабораторию Касперского" только вручную. Приложение не отправляет автоматически файлы трассировки в "Лабораторию Касперского".

Вы можете выбрать способ отправки файлов трассировки в "Лабораторию Касперского".

Перед отправкой файлов трассировки в "Лабораторию Касперского" ознакомьтесь с данными, которые в них содержатся.

Важно! Файлы трассировки могут содержать конфиденциальные данные. Отправляя файлы трассировки в "Лабораторию Касперского", вы соглашаетесь с передачей данных, которые в них содержатся, а также выражаете согласие со способом их передачи.

Источники информации о приложении

Страница Kaspersky Endpoint Security на сайте "Лаборатории Касперского"

На странице Kaspersky Endpoint Security на сайте "Лаборатории Касперского" вы можете получить общую информацию о приложении, его возможностях и особенностях работы.

Страница Kaspersky Endpoint Security в Базе знаний

База знаний – это раздел сайта Службы технической поддержки "Лаборатории Касперского".

На странице Kaspersky Endpoint Security в Базе знаний вы найдете статьи, которые содержат полезную информацию, рекомендации и ответы на часто задаваемые вопросы о приобретении, установке и использовании приложения.

Статьи Базы знаний могут отвечать на вопросы, которые относятся не только к Kaspersky Endpoint Security, но и к другим приложениям "Лаборатории Касперского". Статьи Базы знаний также могут содержать новости Службы технической поддержки.

Переход в Базу знаний из меню "Справка"

1. Выберите **Справка** > **Поддержка**.
2. Нажмите **Служба технической поддержки**.

Обсуждение приложений "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.

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

Переход в Форум пользователей из меню "Справка"

1. Выберите **Справка** > **Поддержка**.
2. Нажмите на кнопку **Сообщество пользователей**.

Примечание. Для использования источников информации на сайте "Лаборатории Касперского" требуется подключение к интернету.

Если вы не можете решить свою проблему самостоятельно, обратитесь в Службу технической поддержки.

Электронная справка

Приложение содержит файлы полной и контекстной справки.

В полной справке вы можете найти информацию о настройке и использовании Kaspersky Endpoint Security.

В контекстной справке вы можете найти информацию об окнах Kaspersky Endpoint Security, описание параметров приложения и ссылки на описания задач, в которых используются эти параметры.

Справка может быть включена в состав приложения либо располагаться онлайн на сайте "Лаборатории Касперского". Для просмотра онлайн-справки требуется соединение с интернетом.

Онлайн-справка (эта справка)

В этой справке вы можете найти информацию для выполнения следующих задач:

- подготовка к установке приложения, установка и активация приложения;
- настройка и использование приложения;
- удаленное управление приложением через Kaspersky Security Center.

Приложения

Этот раздел содержит информацию, которая дополняет основной текст документа.

Известные ошибки и ограничения

Kaspersky Endpoint Security имеет следующие известные ошибки и ограничения:

- Если программа, которая осуществляет сбор информации и отправляет ее на обработку, установлена на вашем компьютере, приложение Kaspersky Endpoint Security может классифицировать эту программу, как вредоносную. Чтобы избежать этого, вы можете исключить эту программу из проверки, настроив параметры приложения Kaspersky Endpoint Security, как описано в этом документе.
- Параметры работы приложения можно изменить путем редактирования конфигурационных файлов.
- В Kaspersky Security Center локальные задачи могут дублироваться в свойствах управляемых устройств.
- Изменение источника обновлений в локальной задаче обновления приложения для отдельного клиентского компьютера приводит к отключению автоматического обновления.

- Если вы запускаете задачу перезагрузки компьютера через Консоль администрирования, и сообщение пользователю содержит точку с запятой (;), задача отображается как выполненная, но пользователю не предлагается перезагрузить свой Mac.

- Чтобы исключить из проверки Kaspersky Endpoint Security сетевой трафик Safari, вам нужно добавить в список исключений следующие пути:

  - `/System/Library/Frameworks/WebKit.framework/Versions/A/XPCServices/com.a`

  - `/System/Library/Frameworks/WebKit.framework/Versions/A/XPCServices/com.a`

  - `/System/Library/PrivateFrameworks/SafariShared.framework/Versions/A/XPCS`

  - `/System/Library/Frameworks/webkit2.framework/versions/a/xpcservices/com`

- Чтобы исключить из проверки Kaspersky Endpoint Security сетевой трафик Google Chrome, вам нужно добавить в список исключений следующий путь:

  - `/Applications/Google Chrome.app/Contents/Frameworks/Google Chrome Framework.framework/Versions/<VersionNumber>/Helpers/Google Chrome Helper.app/Contents/MacOS/Google Chrome Helper`

- После создания профиля политики для политики Kaspersky Endpoint Security с помощью Kaspersky Security Center Web Console или Cloud Console вам нужно проверить правильность применения настроек к клиентским компьютерам.

- Если шифрование диска FileVault включено в настройках политики, пользователи с правами администратора могут расшифровать загрузочный диск Mac из Системных настроек.

- Чтобы применить изменения в параметрах подключения к прокси-серверу, нужно перезапустить Kaspersky Endpoint Security.

- Safari может не подключиться к сайту с недоверенным сертификатом. Вам нужно добавить этот сайт в исключения или использовать другой браузер.

- После удаления Kaspersky Endpoint Security 11.2 или более поздней версии через Kaspersky Security Center одно из системных расширений приложения может остаться в памяти компьютера. В редких случаях это может привести к проблемам с разрешением на полный доступ к диску при установке Kaspersky Endpoint Security. В таком случае рекомендуется удалить приложение локально и переустановить его.

- Программы, которым требуется Rosetta, могут быть не установлены, если запущен Kaspersky Endpoint Security. Чтобы решить проблему, завершите работу Kaspersky Endpoint Security и попробуйте переустановить приложение.

- Детали алерта об угрозах, обнаруженных в составе составных объектов, содержат информацию только о самом обнаруженном объекте без графа цепочки развития угрозы.

- При сохранении пароля для Защиты паролем может возникнуть ошибка. В этом случае рекомендуется удалить и переустановить приложение.

- Kaspersky Endpoint Security не проверяет файлы, расположенные в хранилищах OneDrive, iCloud и других облачных хранилищах. Исключите эти файлы из области проверки. В противном случае задача проверки может завершиться с ошибкой *Зараженный файл не удален*.

Список объектов, проверяемых по расширению

Если при создании задачи проверки в Kaspersky Security Center, в параметрах задачи вы выбрали вариант **Проверять программы и документы по расширению**, Kaspersky Endpoint Security проверяет объекты без расширения и объекты с приведенными ниже расширениями.

Общие форматы:

- txt;
- csv;
- htm;
- html.

Мультимедийные (аудио/видео) файлы:

- flv;
- f4v;
- avi;
- 3gp;
- 3g2;
- 3gp2;
- 3p2;
- divx;

- mp4;
- mkv;
- mov;
- qt;
- asf;
- wmv;
- rm;
- rmvb;
- vob;
- dat;
- mpg;
- mpeg;
- bik;
- fcs;
- mp3;
- mpeg3;
- flac;
- ape;
- ogg;
- aac;
- m4a;
- wma;
- ac3;

- wav;
- mka;
- rm;
- ra;
- ravb;
- mid;
- midi;
- cda.

Файлы изображений:

- jpg;
- jpe;
- jpeg;
- jff;
- gif;
- png;
- bmp;
- tif;
- tiff;
- emf;
- wmf;
- eps;
- psd;
- cdr;

- swf.

Исполняемые и системные файлы:

- exe;
- dll;
- scr;
- ocx;
- com;
- sys;
- class;
- o;
- so;
- elf;
- prx;
- vb;
- vbs;
- js;
- bat;
- cmd;
- msi;
- deb;
- rpm;
- sh;
- pl;

- dylib.

Документы и шаблоны:

- doc;
- dot;
- docx;
- dotx;
- docm;
- dotm;
- xsl;
- xls;
- xlsx;
- xltx;
- xlsm;
- xltm;
- xlam;
- xlsb;
- ppt;
- pot;
- pps;
- pptx;
- potx;
- pptm;
- potm;

- ppsx;
- ppsm;
- rtf;
- pdf;
- msg;
- eml;
- vsd;
- vss;
- vst;
- vdx;
- vsx;
- vtx;
- xps;
- oxps;
- one;
- onepkg;
- xsn;
- odt;
- ods;
- odp;
- sxw;
- pub;
- mdb;

- accdb;
- accde;
- accdr;
- accdc;
- chm;
- mht.

Архивы:

- zip;
- 7z*;
- 7-z;
- rar;
- iso;
- cab;
- jar;
- bz;
- bz2;
- tbz;
- tbz2;
- gz;
- tgz;
- arj;
- dmg;
- smi;

- img;
- xar.

Примечание. Фактический формат файла может не совпадать с форматом, указанным в расширении файла.

Маски в путях к файлам и папкам

Маска имени файла или *папки* – это представление имени папки или имени и расширения файла общими символами.

Вы можете использовать эти символы при формировании области защиты, области проверки и Доверенной зоны:

- Символ тильда (`~`) заменяет `/Users/<user name>` в пути к файлу или папке. Например, путь `~/Desktop` означает, что в область защиты добавляются папки Desktop всех пользователей на компьютерах, для которых вы формируете область защиты.
- Символ звездочка (`*`) заменяет любой набор символов в имени файла или папки, кроме символов `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `/*/*.txt` будет включать все пути к файлам с расширением txt, расположенным в папках на внутреннем диске, но не в подпапках.
- Два введенных подряд символа звездочки (`**`) заменяют любой набор символов, в том числе пустой, в имени файла или папки, включая символы `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `/Folder/**/*.txt` будет включать все пути к файлам с расширением txt в папке Folder и вложенных папках. Маска должна включать хотя бы один уровень вложенности. Маска `/**/*.txt` не работает.
- Символ знака вопроса (`?`) заменяет любой один символ, кроме символов `\` и `/` (разделители имен файлов и папок в путях к файлам и папкам). Например, маска `/Folder/???.txt` будет включать пути ко всем расположенным в папке Folder файлам с расширением txt и именем, состоящим из трех символов.

Требования к IOC-файлам

При создании задач поиска IOC учитывайте следующие требования и ограничения, связанные с IOC-файлами:

- Приложение поддерживает IOC-файлы с расширением IOC, XML и JSON открытого стандарта описания индикаторов компрометации OpenIOC версий 1.0 и 1.1 или STIX версий 2.0 и 2.1.

- Если при создании задачи Поиск IOC из командной строки вы загрузите IOC-файлы, часть из которых не поддерживается, то при запуске задачи приложение будет использовать только поддерживаемые IOC-файлы. Если при создании задачи Поиск IOC из командной строки все загруженные вами IOC-файлы не поддерживаются, то задача может быть запущена, но в результате выполнения задачи не будут обнаружены индикаторы компрометации. Загрузить IOC-файлы, которые не поддерживаются, в Web Console или Cloud Console невозможно.

- Семантические ошибки и неподдерживаемые IOC-термины и теги в IOC-файлах не приводят к ошибкам выполнения задачи. На таких участках IOC-файлов приложение фиксирует отсутствие совпадения.

- Идентификаторы всех IOC-файлов, которые используются в одной задаче поиска IOC, должны быть уникальными. Наличие IOC-файлов с одинаковыми идентификаторами может повлиять на корректность результатов выполнения задачи.

- Размер одного IOC-файла не должен превышать 2 МБ. Использование файлов большего размера приводит к завершению задач поиска IOC с ошибкой. Суммарный размер всех добавляемых файлов в IOC-коллекции не должен превышать 10 МБ. Если размер всех файлов превышает 10 МБ, вам нужно разделить IOC-коллекцию и создать несколько задач Поиск IOC.

- Рекомендуется создавать на каждую угрозу по одному IOC-файлу. Это облегчает чтение результатов задачи Поиск IOC.

Особенности и ограничения поддержки IOC-файлов приложением приведены в следующей таблице.

Особенности и ограничения поддержки документов IOC.

Поддерживаемые условия	OpenIOC 1.0:
	`is`
	`isnot` (как исключение из множества)
	`contains`
	`containsnot` (как исключение из множества)
	OpenIOC 1.1:
	`is`
	`contains`
	`starts-with`

```
ends-with

matches

greater-than

less-than
```

STIX 2.0 и 2.1:

```
=

!=

>

<

=>

<=
```

Поддерживаемые интерпретаторы скриптов для Запрета запуска

Запрет запуска поддерживает следующие интерпретаторы скриптов:

- PkgUtil
- PkgInstaller
- /usr/bin/osascript
- /usr/bin/osacompile
- /usr/local/bin/python
- /usr/local/bin/python3
- /usr/bin/perl
- /usr/bin/ruby
- /bin/bash
- /bin/zsh
- /bin/sh

- /bin/dash
- /bin/csh
- /bin/ksh
- /bin/tcsh

Важно: Если скрипт, указанный в правиле запрета запуска, открывается уже запущенными интерпретаторами скриптов PkgUtil или PkgInstaller, выполнение этого скрипта не будет заблокировано.

Как добавить сертификат Kaspersky Endpoint Security в хранилище сертификатов Mozilla Firefox

Если браузер использует хранилище сертификатов Mozilla Firefox, вам необходимо экспортировать и добавить сертификат "Лаборатории Касперского" в это хранилище сертификатов вручную. В противном случае браузер не сможет открывать HTTPS-страницы.

Экспорт сертификата "Лаборатории Касперского"

1. Откройте **Launchpad** > **Other** > **Связка ключей** на вашем Mac.
2. На левой панели окна нажмите **Система** и откройте вкладку **Сертификаты**.
3. В списке сертификатов найдите **Kaspersky Web Anti-Virus Certification Authority**.
4. Щелкните этот сертификат правой кнопкой мыши и выберите **Экспортировать «Kaspersky Web Anti-Virus Certification Authority»**.
5. Выберите место для сохранения сертификата и нажмите на кнопку **Сохранить**.

Сертификат "Лаборатории Касперского" сохранен.

Добавление сертификата "Лаборатории Касперского" в хранилище сертификатов Mozilla Firefox

1. Откройте Mozilla Firefox.

2. В правом верхнем углу нажмите на кнопку меню и выберите **Параметры**.
3. На левой панели окна выберите **Конфиденциальность и безопасность**.
4. Прокрутите вниз до раздела **Сертификаты**.
5. Нажмите на **Просмотр сертификатов**.
6. В открывшемся окне нажмите на кнопку **Импортировать**.
7. Выберите файл сертификата "Лаборатории Касперского" и нажмите **Открыть**.
8. Установите флажки **Доверять этому CA для идентификации веб-сайтов** и **Доверять этому CA для идентификации пользователей электронной почты**. Нажмите **OK**.

   Сертификат "Лаборатории Касперского" импортируется в хранилище сертификатов Mozilla Firefox. Он отображается в списке сертификатов в окне **Диспетчера сертификатов**.

Важно! При каждой переустановке приложения Kaspersky Endpoint Security создается новый корневой сертификат "Лаборатории Касперского". Это означает, что вам необходимо выполнять эту процедуру после каждой переустановки приложения Kaspersky Endpoint Security.

Информация о стороннем коде

Информация о стороннем коде содержится в файле legal_notices.txt, расположенном в папке с установленным приложением.

Уведомления о товарных знаках

Окно Обнаружен архив, защищенный паролем

Если в процессе работы Защиты от файловых угроз или выполнения задач проверки Kaspersky Endpoint Security требуется проверить архив, защищенный паролем, на экране появляется окно уведомления.

Архив

Путь к архиву.

Пароль

Поле для ввода пароля.

Если вы введете пароль, Kaspersky Endpoint Security проверит архив на наличие вредоносного ПО и других программ, представляющих угрозу безопасности компьютера.

Пропускать защищенные архивы

При нажатии на кнопку приложение пропустит проверку текущего объекта и всех объектов такого же типа.

Пропустить

При нажатии на кнопку объект пропускается.

Диалог Необходима аутентификация на прокси-сервере

Имя

Поле для ввода имени пользователя для соединения с прокси-сервером.

Пароль

Поле для ввода пароля.

Запомнить пароль

Флажок включает/выключает использование указанных имени пользователя и пароля для авторизации на прокси-сервере в дальнейшем.

По умолчанию флажок снят.

Диалог Обнаружен объект

Когда Kaspersky Endpoint Security обнаруживает вирус или другую программу, представляющую угрозу безопасности компьютера, на экране появляется окно уведомления.

Обнаружено

Имя объекта согласно Вирусной энциклопедии "Лаборатории Касперского" .

Подробнее

При нажатии на кнопку открывается страница Вирусной энциклопедии "Лаборатории Касперского" с информацией об обнаруженном объекте.

Объект

Путь к папке, в которой хранится объект, или веб-адрес, по которому он был обнаружен.

Применить во всех подобных случаях

Флажок включает/выключает применение выбранного действия ко всем объектам этого типа в текущем сеансе работы Защиты от файловых угроз, Защиты от веб-угроз или задачи поиска вредоносного ПО.

По умолчанию флажок снят.

Сеансом работы Защиты от файловых угроз и Защиты от веб-угроз считается время с момента запуска компонента до его выключения или до перезапуска приложения. Сеансом выполнения задачи поиска вредоносного ПО считается время с момента запуска до завершения задачи поиска вредоносного ПО.

Кнопки с действиями, которые вы можете применить к обнаруженному объекту, изменяются в зависимости от типа обнаруженного объекта.

Вы можете выбрать одно из следующих действий:

- **Лечить**. Лечить объект. Перед лечением Kaspersky Endpoint Security создает резервную копию файла на случай, если потребуется восстановить исходный файл.
- **Удалить**. Удалить объект. Перед удалением Kaspersky Endpoint Security создает резервную копию файла на случай, если потребуется восстановить исходный файл.
- **Не блокировать**. Разрешить доступ к сайту, который Kaspersky Endpoint Security считает опасным объектом веб-трафика.

- **Блокировать**. Запретить доступ к сайту, который Kaspersky Endpoint Security считает опасным объектом веб-трафика.
- **Удалить архив**. Удалить архив, содержащий обнаруженный объект.
- **Пропускать защищенные архивы**. Не проверять защищенные паролем архивы при поиске вредоносного ПО.
- **Пропустить**. Заблокировать доступ к объекту, но не выполнять над ним никаких действий.

Окно Проверка

При нажатии на кнопку вы возвращаетесь к предыдущему окну Kaspersky Endpoint Security.

При нажатии на кнопку вы переходите к следующему окну Kaspersky Endpoint Security.

При нажатии на кнопку удаляются все записи обо всех задачах поиска вредоносного ПО в окне **Проверка**.

Расписание проверки

При нажатии на кнопку открывается окно, в котором вы можете настроить расписание запуска полной и быстрой проверки.

Быстрая проверка

При нажатии на кнопку запуска ( ) в этом разделе запускается задача быстрой проверки.

Полная проверка

При нажатии на кнопку запуска ( ) в этом разделе запускается задача полной проверки.

При нажатии на кнопку останавливается выполнение выбранной задачи поиска вредоносного ПО.

Кнопка отображается, если задача поиска вредоносного ПО запущена.

Настройки

При нажатии на эту кнопку открывается вкладка **Проверка**, на которой вы можете настроить параметры задач проверки.

Выбрать

При нажатии на кнопку открывается окно, в котором вы можете выбрать файл или папку для проверки.

В нижней части раздела **Файлы и папки** вы можете просмотреть записи обо всех задачах поиска вредоносного ПО, которые были выполнены для выбранных файлов или папок.

Подробнее

При нажатии на кнопку открывается окно отчета о выполнении задач поиска вредоносного ПО.

Эта кнопка появляется, если вы наводите указатель мыши на задачу проверки.

Очистить историю проверок

При нажатии на кнопку все записи обо всех задачах поиска вредоносного ПО удаляются.

Показать все

При нажатии на кнопку открывается окно **Обнаруженные объекты**, в котором вы можете просмотреть все объекты, обнаруженные программой.

Примечание. Kaspersky Endpoint Security не проверяет файлы, расположенные в хранилищах OneDrive, iCloud и других облачных хранилищах. Исключите эти файлы из области проверки. В противном случае задача проверки может завершиться с ошибкой *Зараженный файл не удален*.

Окно Обнаруженные объекты

В блоке **Обнаруженные объекты** перечислены вредоносные объекты, обнаруженные приложением.

Лечить все

При нажатии на кнопку запускается лечение всех обнаруженных вредоносных объектов.

Игнорировать все

При нажатии на кнопку все вредоносные объекты удаляются из списка вредоносных объектов в блоке **Обнаруженные объекты**.

•••

При нажатии на кнопку открывается всплывающее меню, в котором вы можете выбрать одно из следующих действий над вредоносным объектом:

- **Лечить**. Лечить объект. Перед лечением приложение Kaspersky Endpoint Security создает резервную копию файла на случай, если потребуется восстановить файл или появится возможность его вылечить без потери данных.
- **Игнорировать**. Удалить объект из списка обнаруженных объектов.

В блоке **Другие объекты** перечислены обнаруженные объекты, которые не являются вредоносными программами, но могут быть использованы злоумышленниками для нанесения вреда вашему компьютеру или данным.

Удалить все

При нажатии на кнопку все обнаруженные объекты удаляются с вашего компьютера.

Игнорировать все

При нажатии на кнопку все обнаруженные объекты удаляются из списка обнаруженных объектов в блоке **Другие объекты**.

•••

При нажатии на кнопку открывается всплывающее меню, в котором вы можете выбрать одно из следующих действий над обнаруженным объектом:

- **Удалить**. Удалить обнаруженный объект с компьютера.
- **Игнорировать**. Удалить объект из списка обнаруженных объектов.

В блоке **Резервное хранилище** содержатся резервные копии обнаруженных объектов.

Удалить все

При нажатии на кнопку все резервные копии обнаруженных объектов удаляются с вашего компьютера.

•••

При нажатии на кнопку открывается всплывающее меню, в котором вы можете выбрать одно из следующих действий над резервной копией обнаруженного объекта:

- **Удалить копию**. Удалить копию обнаруженного объекта, помещенную на резервное хранилище, с вашего компьютера.
- **Восстановить файл**. Восстановить выбранную в списке резервную копию файла в исходном местоположении с тем же именем, которое было у исходного файла до лечения или удаления. Если в исходном местоположении уже есть объект с таким именем (например, если приложение Kaspersky Endpoint Security создало копию исходного файла перед лечением или вылечило исходный файл), на экране появляется соответствующее предупреждение. Вы можете переименовать восстанавливаемый объект или изменить его местоположение.

Окно Лицензия

При нажатии на кнопку вы возвращаетесь к предыдущему окну Kaspersky Endpoint Security.

При нажатии на кнопку вы переходите к следующему окну Kaspersky Endpoint Security.

> **Примечание.** Вид этого окна зависит от того, активировано ли приложение Kaspersky Endpoint Security, а также от типа лицензии или подписки.

В окне может отображаться следующая информация:

- статус лицензии или подписки;
- активные ключи;
- резервные ключи (если они были добавлены);
- тип лицензии и количество компьютеров, на которых вы можете использовать приложение по действующей лицензии или подписке;
- функции приложения, доступные по текущей лицензии или подписке;
- дата и время окончания срока действия лицензии;
- количество дней до завершения срока действия лицензии.

В этом окне вы можете выполнить следующие действия:

- активировать приложение с помощью кода активации;
- перейти на сайт с информацией о приобретении лицензии в интернет-магазине "Лаборатории Касперского";
- открыть сайт поставщика Kaspersky Endpoint Security с информацией об обновлении подписки;
- обновить статус подписки.

Дополнительную информацию о лицензировании Kaspersky Endpoint Security вы можете получить у системного администратора вашей организации.

Вкладка Базовая

В блоке **Основное** вы можете включить или выключить защиту компьютера от вредоносных программ и других угроз компьютерной безопасности.

Включить защиту

Флажок включает/выключает постоянную защиту от вредоносных программ и других угроз компьютерной безопасности.

Этот флажок по умолчанию установлен.

Проверять защищенные соединения (HTTPS)

Флажок включает/выключает проверку защищенных соединений (HTTPS) и отображение уведомлений, когда Веб-Контроль блокирует пользователю доступ к опасным веб-ресурсам.

По умолчанию флажок снят.

Доверенная зона

При нажатии на эту кнопку открывается окно, в котором вы можете редактировать Доверенную зону, создав список объектов, которым вы доверяете и которые не хотите проверять на наличие вредоносного ПО.

Настройки

При нажатии на эту кнопку открывается окно, в котором вы можете управлять списком доверенных корневых сертификатов, а также выбрать хранилище сертификатов для проверки зашифрованного HTTPS-трафика в браузере Mozilla Firefox.

В блоке **Защита от файловых угроз** вы можете включить или выключить Защиту от файловых угроз и выбрать, какие действия Kaspersky Endpoint Security выполнит при обнаружении зараженного файла.

Включить Защиту от файловых угроз

Флажок включает/выключает Защиту от файловых угроз.

Этот флажок по умолчанию установлен.

Область защиты

При нажатии на кнопку открывается окно, в котором вы можете сформировать область защиты.

Лечить или удалять вредоносные объекты автоматически

Kaspersky Endpoint Security блокирует доступ к зараженному файлу и пытается его лечить, не запрашивая подтверждения пользователя. Перед лечением Kaspersky Endpoint Security помещает резервную копию файла в резервное хранилище. Если файл вылечен, Kaspersky Endpoint Security восстанавливает его в исходном месте под исходным именем. Если вылечить зараженный файл не удается, Kaspersky Endpoint Security оставляет его заблокированным в исходном месте. Информация об обнаруженном зараженном объекте сохраняется в отчете Обработанные объекты.

Запрашивать действие

Kaspersky Endpoint Security выводит на экран окно уведомления с информацией о том, каким вредоносным объектом заражен или возможно заражен файл, и предлагает выбрать действие, которое выполнит Kaspersky Endpoint Security. В зависимости от статуса объекта действия могут отличаться.

Этот вариант действия используется по умолчанию.

В блоке **Защита от веб-угроз** вы можете включить или выключить Защиту от веб-угроз и выбрать действие, которое Kaspersky Endpoint Security выполнит при обнаружении опасных объектов веб-трафика.

Включить Защиту от веб-угроз

Флажок включает/выключает Защиту от веб-угроз.

Этот флажок по умолчанию установлен.

Блокировать опасные объекты веб-трафика автоматически

Kaspersky Endpoint Security блокирует доступ к сайту, на котором обнаружен опасный объект веб-трафика, не запрашивая подтверждения пользователя.

Запрашивать действие

Kaspersky Endpoint Security выводит на экран окно уведомления с информацией об обнаруженном опасном объекте веб-трафика и предлагает выбрать действие, которое выполнит Kaspersky Endpoint Security. В зависимости от статуса объекта действия могут отличаться.

Этот вариант действия используется по умолчанию.

В блоке **Защита от почтовых угроз** можно включить или выключить Защиту от почтовых угроз и выбрать действие, которое Kaspersky Endpoint Security выполнит при обнаружении вредоносных объектов.

Включить Защиту от почтовых угроз

Флажок включает/выключает Защиту от почтовых угроз.

Этот флажок по умолчанию установлен.

Удалять вредоносные объекты автоматически

При обнаружении зараженного объекта в сообщении электронной почты Kaspersky Endpoint Security удаляет зараженный объект и заменяет содержимое объекта текстом "The requested file infected with <название вируса> has been deleted".

Блокировать вредоносные объекты автоматически

При обнаружении зараженного объекта в сообщении электронной почты Kaspersky Endpoint Security заменяет тему сообщения на "Message is infected: <первоначальная тема письма>". Замена темы сообщения электронной почты выполняется только для протокола POP3.

В блоке **Защита от сетевых угроз** вы можете включить или выключить защиту компьютера от сетевых атак.

Включить Защиту от сетевых угроз

Флажок включает/выключает Защиту от сетевых угроз.

Этот флажок по умолчанию установлен.

Настройки

При нажатии на кнопку открывается окно, в котором вы можете сформировать список доверенных компьютеров или просмотреть и изменить список заблокированных компьютеров.

При нажатии на кнопку пользователи, не имеющие прав администратора компьютера, лишаются возможности изменять настройки приложения Kaspersky Endpoint Security.

При нажатии на кнопку открывается окно запроса учетных данных администратора компьютера. После ввода учетных данных администратора компьютера у пользователя появляется возможность изменять настройки приложения.

Окно Область защиты

В блоке **Область защиты** вы можете просмотреть и изменить область защиты.

Все съемные диски

Флажок включает/выключает постоянную защиту всех съемных дисков.

Этот флажок по умолчанию установлен.

Все внутренние диски

Флажок включает/выключает постоянную защиту всех внутренних дисков.

Этот флажок по умолчанию установлен.

Все сетевые диски

Флажок включает/выключает постоянную защиту всех сетевых дисков.

Этот флажок по умолчанию установлен.

+

При нажатии на кнопку раскрывается список, в котором вы можете выбрать элементы для формирования области защиты:

- **Файлы и папки**. При выборе этого элемента открывается окно, в котором вы можете выбрать файл или папку, которые нужно добавить в область защиты.
- **Все диски**. При выборе этого элемента в область защиты добавляются все съемные, внутренние и сетевые диски компьютера.
- **Все съемные диски**. При выборе этого элемента в область защиты добавляются все съемные диски компьютера.
- **Все внутренние диски**. При выборе этого элемента в область защиты добавляются все внутренние диски компьютера.
- **Все сетевые диски**. При выборе этого элемента в область защиты добавляются все сетевые диски компьютера.
- **Память**. При выборе этого элемента в область защиты добавляется память компьютера.
- **Объекты автозапуска**. При выборе этого элемента в область защиты добавляются все исполняемые файлы, которые запускаются вместе с операционной системой. Проверка объектов автозапуска позволяет обнаружить руткиты.

Флажок рядом с элементом списка включает/выключает постоянную защиту объектов, относящихся к этому элементу.

–

При нажатии на кнопку выбранный элемент списка удаляется из области защиты.

Элементы, включенные в область защиты по умолчанию, невозможно удалить.

В секции **Оптимизация** вы можете настроить проверку системного тома "только для чтения".

Пропускать проверку системного тома «только для чтения»

Флажок включает/выключает проверку системного тома "только для чтения".

Этот флажок по умолчанию установлен.

Важно! В целях безопасности оптимизация может быть выключена.

Окно Настройки

На вкладке **Доверенные компьютеры** вы можете сформировать список доверенных компьютеров. Приложение Kaspersky Endpoint Security не блокирует IP-адреса этих компьютеров автоматически при обнаружении исходящей с них опасной сетевой активности.

По умолчанию список доверенных компьютеров пуст.

+

При нажатии на кнопку добавляется поле для ввода IP-адреса доверенного компьютера.

–

При нажатии на кнопку выбранный IP-адрес удаляется из списка доверенных компьютеров.

Изменить

При нажатии на кнопку выбранный IP-адрес становится доступным для редактирования.

На вкладке **Заблокированные компьютеры** вы можете просмотреть и изменить список заблокированных компьютеров.

При обнаружении опасной сетевой активности, исходящей с компьютера, приложение Kaspersky Endpoint Security блокирует его по IP-адресу на один час.

IP-адрес

В этой графе отображается IP-адрес заблокированного компьютера.

Время события

В этой графе отображаются дата и время обнаружения опасной сетевой активности компьютера.

Разблокировать

При нажатии на кнопку выбранный IP-адрес удаляется из списка заблокированных компьютеров.

Вкладка Проверка

Список задач поиска вредоносного ПО

Содержит встроенные задачи поиска вредоносного ПО:

- **Полная проверка**. Поиск вредоносного ПО в памяти компьютера, объектах автозапуска и всех внутренних дисках.

- **Быстрая проверка**. Поиск вредоносного ПО в важных областях компьютера: памяти, объектах автозапуска и системных папках.

- **Выборочная проверка**. Поиск вредоносного ПО в отдельном объекте (файле, папке, внутреннем или съемном диске).

- **Проверка внешних дисков**. Поиск вредоносного ПО на внешних дисках, который выполняется при подключении внешнего диска к компьютеру.

Примечание. Kaspersky Endpoint Security не проверяет файлы, расположенные в хранилищах OneDrive, iCloud и других облачных хранилищах. Исключите эти файлы из области проверки. В противном случае задача проверки может завершиться с ошибкой *Зараженный файл не удален*.

В блоке **Область проверки** вы можете просматривать и изменять область проверки для задачи быстрой проверки.

Изменить

При нажатии на кнопку открывается окно, в котором вы можете просмотреть и изменить область проверки.

Кнопка отображается, если в списке выбрана задача Быстрой проверки.

В блоке **Действие** вы можете выбрать действие, которое Kaspersky Endpoint Security выполнит при обнаружении зараженного файла, а также настроить расписание запуска задачи.

Лечить или удалять вредоносные объекты автоматически

Kaspersky Endpoint Security блокирует доступ к зараженному файлу и пытается его лечить, не запрашивая подтверждения пользователя. Перед лечением Kaspersky Endpoint Security помещает резервную копию файла в резервное хранилище. Если файл вылечен, Kaspersky Endpoint Security восстанавливает его в исходном месте под исходным именем. Если вылечить зараженный файл не удается, Kaspersky Endpoint Security оставляет его заблокированным в исходном месте. Информация об обнаруженном зараженном объекте сохраняется в отчете Обработанные объекты.

Запрашивать по окончании проверки

Kaspersky Endpoint Security откладывает обработку обнаруженных зараженных файлов до конца проверки. По окончании проверки Kaspersky Endpoint Security отображает окна уведомлений с информацией о каждом обнаруженном зараженном объекте и предлагает выбрать дальнейшее действие. В зависимости от статуса объекта действия могут отличаться.

Этот вариант действия используется по умолчанию.

В разделе **Если подключен внешний диск** на вкладке **Проверка внешних дисков** вы можете выбрать действие, которое Kaspersky Endpoint Security выполнит при подключении внешнего диска.

Проверка

Если выбран этот вариант, Kaspersky Endpoint Security выполнит поиск вредоносного ПО на подключенном внешнем диске.

Этот вариант выбран по умолчанию.

Никаких действий не требуется

Если выбран этот вариант, Kaspersky Endpoint Security не будет проверять подключенный внешний диск.

В блоке **Оптимизация** вы можете настроить, будет ли приложение Kaspersky Endpoint Security проверять системный том "только для чтения" при выполнении задач быстрой и полной проверки.

Пропускать проверку системного тома «только для чтения»

Флажок включает/выключает проверку системного тома "только для чтения".

По умолчанию флажок установлен в настройках быстрой проверки и снят в настройках полной проверки.

Важно! В целях безопасности оптимизация может быть выключена.

Загрузка CPU

При нажатии на кнопку открывается окно, в котором вы можете включить или выключить ограничение использования CPU на защищаемом устройстве для проверок в приложении. Если опция **Ограничить загрузку CPU для проверок до** включена, вы можете установить предельное значение использования CPU в соответствующем поле.

Примечание. Это совокупный лимит для всех ядер CPU. В приложении «Мониторинг системы» отображается сумма загрузки отдельных ядер CPU, которая может превышать 100%.

Включение этой опции может негативно сказаться на производительности Kaspersky Endpoint Security.

По умолчанию эта опция выключена.

Расписание

При нажатии на кнопку открывается окно, в котором вы можете настроить расписание запуска полной и быстрой проверки.

При нажатии на кнопку пользователи, не имеющие прав администратора компьютера, лишаются возможности изменять настройки приложения Kaspersky Endpoint Security.

При нажатии на кнопку открывается окно запроса учетных данных администратора компьютера. После ввода учетных данных администратора компьютера у пользователя появляется возможность изменять настройки приложения.

Окно Область проверки

В этом окне вы можете просматривать и изменять область проверки для задачи быстрой проверки.

Флажок рядом с объектом в списке включает объект в область проверки или исключает из нее.

+

При нажатии на кнопку раскрывается список, позволяющий сформировать область проверки:

- **Файлы и папки**. При выборе этого элемента открывается окно, в котором вы можете выбрать файл или папку, которые нужно добавить в область проверки.
- **Все диски**. При выборе этого элемента в область проверки добавляются все съемные, внутренние и сетевые диски компьютера.
- **Все внешние диски**. При выборе этого элемента в область проверки добавляются все съемные диски компьютера.
- **Все внутренние диски**. При выборе этого элемента в область проверки добавляются все внутренние диски компьютера.
- **Все сетевые диски**. При выборе этого элемента в область проверки добавляются все сетевые диски компьютера.
- **Память**. При выборе этого элемента в область проверки добавляется память компьютера.
- **Объекты автозапуска**. При выборе этого элемента в область проверки добавляются все исполняемые файлы, которые запускаются вместе с операционной системой. Проверка объектов автозапуска позволяет обнаружить руткиты.

–

При нажатии на кнопку выбранный элемент списка удаляется из области проверки.

Элементы, включенные в область проверки по умолчанию, невозможно удалить.

В блоке **Оптимизация** вы можете настроить, будет ли приложение Kaspersky Endpoint Security проверять системный том "только для чтения" при выполнении задач поиска вредоносного ПО.

Пропускать проверку системного тома «только для чтения»

Флажок включает/выключает проверку системного тома "только для чтения".

Если флажок установлен, Kaspersky Endpoint Security пропускает проверку системного тома "только для чтения". Время выполнения проверки значительно уменьшается.

Если флажок снят, Kaspersky Endpoint Security проверяет системный том "только для чтения".

Этот флажок установлен по умолчанию.

> **Примечание.** Kaspersky Endpoint Security не проверяет файлы, расположенные в хранилищах OneDrive, iCloud и других облачных хранилищах. Исключите эти файлы из области проверки. В противном случае задача проверки может завершиться с ошибкой *Зараженный файл не удален*.

Вкладка Угрозы

В блоке **Обнаруживаемые объекты** вы можете сформировать список обнаруживаемых объектов.

Вирусы, черви, троянские программы, вредоносные утилиты, рекламные программы и программы автодозвона

Эта категория включает в себя следующие типы программ:

- Все типы вредоносных программ.
- Программы, которые отображают рекламные материалы (например, баннеры) на вашем компьютере или заменяют результаты поиска в вашем браузере на рекламные сайты.
- Программы, которые незаметно устанавливают телефонные соединения через компьютерный модем.

Kaspersky Endpoint Security всегда контролирует программы этой категории.

Флажок всегда установлен, и его невозможно снять.

Легальные программы, которые могут быть использованы злоумышленником для нанесения вреда вашему компьютеру или данным

Флажок включает/выключает контроль легальных программ (например, программ удаленного администрирования), которые могут быть использованы злоумышленником для нанесения вреда компьютеру или вашим данным.

По умолчанию флажок снят.

В блоке **Резервное хранилище** вы можете установить максимальный срок хранения объектов в резервном хранилище.

Удалять объекты из резервного хранилища через <число> дней

Флажок включает/выключает удаление объектов из резервного хранилища по истечении указанного срока.

Если флажок установлен, приложение удаляет объекты из резервного хранилища по истечении срока, указанного в поле рядом с флажком. Если флажок снят, объекты хранятся в резервном хранилище бессрочно.

По умолчанию флажок установлен, и объекты хранятся в резервном хранилище в течение 30 дней.

В блоке **Исключения** вы можете сформировать список файлов, папок, приложений и сайтов, которым вы доверяете и которые не хотите проверять.

Доверенная зона

При нажатии на кнопку открывается окно, в котором вы можете сформировать Доверенную зону.

> **Примечание.** Когда в настройках политики администратор запрещает редактирование Доверенной зоны, пользователи не могут перейти к настройкам Доверенной зоны.

При нажатии на кнопку пользователи, не имеющие прав администратора компьютера, лишаются возможности изменять настройки приложения Kaspersky Endpoint Security.

При нажатии на кнопку открывается окно запроса учетных данных администратора компьютера. После ввода учетных данных администратора компьютера у пользователя появляется возможность изменять настройки приложения.

Окно установки пароля администратора

Пароль

Поле для ввода пароля для ограничения нежелательных действий на устройстве.

Подтвердите пароль

Поле для подтверждения пароля путем его повторного ввода.

Опции

Список действий, которые могут быть защищены паролем. Установите требуемые флажки для защиты соответствующих действий на устройстве. Вы должны установить хотя бы один флажок.

Отменить

При нажатии на эту кнопку окно закрывается без сохранения изменений.

OK

Нажатие на эту кнопку сохраняет настройки пароля администратора и закрывает окно. После сохранения изменений вам будет предложено ввести пароль при попытке выполнить нежелательное действие на устройстве.

Окно настройки защиты паролем

Пароль

Поле для ввода пароля для ограничения нежелательных действий на устройствах пользователей.

Нажмите на кнопку **Показать**, чтобы просмотреть введенные символы.

Подтвердите пароль

Поле для подтверждения пароля путем его повторного ввода.

Нажмите на кнопку **Показать**, чтобы просмотреть введенные символы.

Требовать пароль, чтобы

Список действий, которые могут быть защищены паролем. Установите требуемые флажки для защиты соответствующих действий на устройстве пользователя.

Вкладка Доверенные приложения

На вкладке **Доверенные приложения** вы можете сформировать список приложений, которые приложение Kaspersky Endpoint Security не будет контролировать.

По умолчанию список объектов Доверенной зоны пуст.

+

При нажатии на кнопку открывается окно, в котором вы можете ввести путь к приложению, указать требования к подписи кода и выбрать типы активности, которые Kaspersky Endpoint Security не будет контролировать.

–

При нажатии на кнопку выбранное приложение удаляется из Доверенной зоны.

Изменить

При нажатии на эту кнопку открывается окно, в котором вы можете изменить параметры доверенного приложения.

Окно Добавить доверенное приложение

Путь

Путь к приложению, активность которого Kaspersky Endpoint Security не контролирует.

> **Примечание.** Символьные ссылки не могут использоваться для указания путей в этом поле.

Выбрать

При нажатии на эту кнопку открывается окно, в котором вы можете выбрать приложение, активность которого не будет контролироваться Kaspersky Endpoint Security. В этом случае значения полей **Путь** и **Требование к подписи кода** вставляются автоматически.

Требование к подписи кода

Требования к подписи кода приложения, активность которого не будет отслеживаться Kaspersky Endpoint Security.

Это необязательный параметр.

В разделе **Опции** вы можете выбрать тип активности, который вы хотите, чтобы приложение Kaspersky Endpoint Security не отслеживало.

Не контролировать активность файлов

Флажок включает/выключает контроль операций приложения с файлами на клиентском компьютере.

Если флажок установлен, Kaspersky Endpoint Security не контролирует файловую активность приложения.

Если флажок снят, Kaspersky Endpoint Security контролирует файловую активность приложения.

Этот флажок установлен по умолчанию.

Не контролировать сетевую активность

Этот флажок включает/выключает контроль входящего и исходящего интернет-трафика приложения на клиентском компьютере.

Если флажок установлен, Kaspersky Endpoint Security не контролирует сетевую активность приложения.

Если флажок снят, Kaspersky Endpoint Security контролирует сетевую активность приложения.

Этот флажок установлен по умолчанию.

Отменить

При нажатии на эту кнопку окно закрывается без сохранения изменений.

ОК

Нажатие на эту кнопку сохраняет параметры доверенного приложения и закрывает окно.

Вкладка Доверенные файлы и папки

На вкладке **Файлы и папки** вы можете сформировать список файлов и папок, которые приложение Kaspersky Endpoint Security не будет проверять.

По умолчанию список объектов Доверенной зоны пуст.

+

При нажатии на кнопку открывается окно, в котором вы можете выбрать файл или папку.

–

При нажатии на кнопку выбранный объект удаляется из Доверенной зоны.

Вкладка Доверенные веб-адреса

На вкладке **Веб-адрес** вы можете сформировать список веб-адресов, которые приложение Kaspersky Endpoint Security не будет проверять.

По умолчанию список объектов Доверенной зоны пуст.

+

При нажатии на кнопку появляется поле для ввода веб-адреса.

При указании адреса веб-сайта можно использовать следующие символы:

- Символ звездочки (*) заменяет любой набор символов, за исключением символов \ и / .
- Два последовательных символа звездочки (**) заменяют любой набор символов (включая пустой набор), включая символы \ и / .
- Вопросительный знак (?) заменяет любой отдельный символ в имени файла или папки, за исключением символов \ и / .

–

При нажатии на кнопку выбранный веб-адрес удаляется из Доверенной зоны.

Вкладка Дополнительно

В блоке **KSN** вы можете прочитать Положение о Kaspersky Security Network и принять условия участия или отказаться от участия в Kaspersky Security Network.

Показать Положение о KSN

При нажатии на кнопку открывается окно с текстом Положения о Kaspersky Security Network.

Kaspersky Endpoint Security может использовать глобальный или локальный KSN. Если вы участвуете в Kaspersky Security Network, Kaspersky Endpoint Security использует информацию о репутации файлов, веб-ресурсов и программ, полученную из Kaspersky Security Network, и отправляет в Kaspersky Security Network данные, которые нужны для работы служб обнаружения.

Участвовать в Kaspersky Security Network

Флажок включает/выключает участие в Kaspersky Security Network.

Участвовать в Kaspersky Private Security Network

Флажок включает/выключает участие в Kaspersky Private Security Network. Дополнительную информацию об участии в Kaspersky Private Security Network вы можете получить у системного администратора вашей организации.

Включить расширенный режим работы KSN

Флажок включает/выключает отправку дополнительных данных Kaspersky Security Network. Эти данные нужны для улучшения защиты вашего компьютера и работы Kaspersky Endpoint Security. Вы можете найти перечень предоставляемых данных в Положении о Kaspersky Security Network и в справке Kaspersky Endpoint Security.

Этот флажок устанавливается автоматически, когда вы устанавливаете флажок **Участвовать в Kaspersky Security Network**, но вы можете его снять.

Включить облачный режим

Облачный режим – режим работы приложения, при котором Kaspersky Endpoint Security использует облегченную версию баз вредоносного ПО. Этот режим доступен только в том случае, если включено участие в Kaspersky Security Network. Облегченная версия баз вредоносного ПО позволяет снизить нагрузку на оперативную память компьютера примерно в два раза. Если вы не участвуете в Kaspersky Security Network или облачный режим выключен, Kaspersky Endpoint Security загружает полную версию баз вредоносного ПО с серверов "Лаборатории Касперского".

Если переключатель включен, то Kaspersky Endpoint Security использует облегченную версию баз вредоносного ПО, за счет чего снижается нагрузка на ресурсы операционной системы.

> **Примечание.** Kaspersky Endpoint Security загружает облегченную версию баз вредоносного ПО в ходе ближайшего обновления после того, как флажок был установлен.

Если переключатель выключен, то Kaspersky Endpoint Security использует полную версию баз вредоносного ПО.

> **Примечание.** Kaspersky Endpoint Security загружает полную версию баз вредоносного ПО в ходе ближайшего обновления после того, как флажок был снят.

В разделе **Анализ поведения** вы можете включить/выключить компонент Анализ поведения и выбрать действие, которое будет выполнено при обнаружении активности вредоносного ПО.

Включить Анализ поведения

Этот флажок включает/выключает компонент Анализ поведения, который получает информацию о действиях программ на вашем компьютере и предоставляет ее другим компонентам защиты для повышения их производительности.

Блокировать вредоносную активность

Если выбран этот вариант, Kaspersky Endpoint Security завершает работу программы при обнаружении вредоносной активности.

Удалять обнаруженный опасный объект

Если выбран этот вариант, Kaspersky Endpoint Security удаляет исполняемый файл вредоносной программы и создает резервную копию файла в Резервном хранилище при обнаружении вредоносной активности.

Запрашивать действие

Если выбран этот вариант, при обнаружении вредоносной активности приложение Kaspersky Endpoint Security отображает окно уведомления с информацией о вредоносном объекте и предлагает пользователю выбрать действие, которое выполнит приложение Kaspersky Endpoint Security. В зависимости от статуса объекта действия могут отличаться.

При нажатии на кнопку пользователи, не имеющие прав администратора компьютера, лишаются возможности изменять настройки приложения Kaspersky Endpoint Security.

При нажатии на кнопку открывается окно запроса учетных данных администратора компьютера. После ввода учетных данных администратора компьютера у пользователя появляется возможность изменять настройки приложения.

Вкладка Обновление

В блоке **Базы** вы можете настроить режим обновления баз Kaspersky Endpoint Security.

Загружать обновления автоматически

Флажок включает/выключает автоматическое обновление баз приложения.

Этот флажок по умолчанию установлен.

В блоке **Прокси** вы можете настроить использование прокси-сервера для обновления Kaspersky Endpoint Security.

Использовать прокси-сервер

Флажок включает/выключает использование прокси-сервера для выхода в интернет во время обновления баз вредоносного ПО и модулей приложения.

Этот флажок по умолчанию установлен.

Настройки

При нажатии на кнопку открывается окно, в котором вы можете настроить параметры подключения к прокси-серверу.

В блоке **Откат обновления** вы можете вернуться к использованию предыдущей версии баз приложения. Вам может потребоваться откатить обновления, например, если новая версия баз приложения содержит некорректную сигнатуру, из-за которой Kaspersky Endpoint Security блокирует безопасную программу.

Откатить обновление

При нажатии на кнопку запускается откат обновления баз приложения.

При нажатии на кнопку пользователи, не имеющие прав администратора компьютера, лишаются возможности изменять настройки приложения Kaspersky Endpoint Security.

При нажатии на кнопку открывается окно запроса учетных данных администратора компьютера. После ввода учетных данных администратора компьютера у пользователя появляется возможность изменять настройки приложения.

Окно Настройки прокси-сервера

Использовать системные настройки прокси-сервера

Kaspersky Endpoint Security использует параметры прокси-сервера, указанные в системных настройках вашего Mac.

Этот вариант действия используется по умолчанию.

Использовать указанные настройки прокси-сервера

Kaspersky Endpoint Security использует параметры прокси-сервера, указанные в этом окне.

Адрес

Поле для ввода IP-адреса или доменного имени прокси-сервера.

Поле доступно, если выбрана опция **Использовать указанные настройки прокси-сервера**.

Порт

Поле для ввода номера порта прокси-сервера, предназначенного для обновления Kaspersky Endpoint Security.

Поле доступно, если выбрана опция **Использовать указанные настройки прокси-сервера**.

По умолчанию установлено значение 8080.

Использовать аутентификацию

Аутентификация – это проверка имени пользователя и пароля при соединении с прокси-сервером.

Флажок включает/выключает аутентификацию при соединении с прокси-сервером.

По умолчанию флажок снят.

Имя

Поле для ввода имени пользователя для аутентификации при соединении с прокси-сервером.

Поле доступно, если установлен флажок **Использовать аутентификацию**.

Пароль

Поле для ввода пароля для аутентификации при соединении с прокси-сервером.

Поле доступно, если установлен флажок **Использовать аутентификацию**.

Если вы не указали имя пользователя и пароль или указанные имя пользователя и пароль не были приняты прокси-сервером, откроется окно, в котором вам нужно указать имя пользователя и пароль для аутентификации на прокси-сервере. Если аутентификация завершилась успешно и в окне запроса был установлен флажок **Запомнить пароль**, то указанные имя пользователя и пароль будут использоваться в дальнейшем. Если флажок **Запомнить пароль** в окне запроса имени пользователя и пароля снят, при следующем соединении с прокси-сервером имя пользователя и пароль будут запрошены повторно.

Не использовать прокси-сервер для локальных адресов

Флажок включает/выключает использование прокси-сервера при обновлении из локальной или сетевой папки.

Этот флажок по умолчанию установлен.

Вкладка Интерфейс

В блоке **Уведомления** вы можете настроить параметры уведомлений, которые Kaspersky Endpoint Security отображает, чтобы информировать вас о различных событиях.

Уведомлять о событиях

Флажок включает/выключает вывод уведомлений о событиях в работе приложения.

Этот флажок по умолчанию установлен.

Воспроизводить звуковое уведомление при обнаружении вредоносных программ

Флажок включает/выключает звуковое уведомление, когда Kaspersky Endpoint Security обнаруживает вредоносный объект.

Этот флажок по умолчанию установлен.

В блоке **Значок приложения** вы можете настроить отображение значка приложения в строке меню.

Отображать в строке меню

Флажок включает/выключает отображение значка приложения в строке меню.

В блоке **Отчеты** вы можете включить или выключить запись некритических событий в отчеты Kaspersky Endpoint Security.

Записывать некритические события

Флажок включает/выключает запись информационных событий в отчеты. Как правило, такие события не важны для обеспечения защиты компьютера.

В блоке **Трассировка** вы можете включить или выключить трассировку.

Трассировка – это процесс пошагового выполнения приложения, необходимый для получения подробной информации о работе приложения. Специалисты Службы технической поддержки "Лаборатории Касперского" используют файлы трассировки для устранения неисправностей. Вы можете включить запись событий для создания файлов трассировки и отправки этих файлов по запросу в Службу технической поддержки. По умолчанию запись событий приложения выключена.

Важно! Включайте трассировку только по просьбе специалиста Службы технической поддержки.

Включить трассировку

Флажок включает/выключает функцию сохранения файлов трассировки.

По умолчанию флажок снят.

В разделе **Защита паролем** вы можете включить защиту паролем от нежелательных действий на вашем компьютере.

Включить Защиту паролем

Этот флажок включает/выключает защиту паролем от нежелательных действий.

По умолчанию флажок снят.

Установка этого флажка открывает окно, в котором вы можете установить и настроить пароль администратора.

Настройки

При нажатии на кнопку открывается окно, в котором вы можете изменить параметры пароля администратора.

При нажатии на кнопку пользователи, не имеющие прав администратора компьютера, лишаются возможности изменять настройки приложения Kaspersky Endpoint Security.

При нажатии на кнопку открывается окно запроса учетных данных администратора компьютера. После ввода учетных данных администратора компьютера у пользователя появляется возможность изменять настройки приложения.

Окно настройки Защиты от почтовых угроз

Пропускать, если размер файла больше N МБ

Если флажок установлен, Защита от почтовых угроз исключает из проверки архивы, прикрепленные к электронным письмам, если их размер превышает указанное значение.

Если флажок снят, Защита от почтовых угроз проверяет архивы вложений электронной почты любого размера.

По умолчанию установлено значение 8 МБ.

Этот флажок по умолчанию установлен.

Ограничить время проверки архива до N сек.

Если этот флажок установлен, время, выделенное на проверку архивов, прикрепленных к электронным письмам, ограничено указанным периодом.

Если флажок снят, время, выделенное на проверку архивов, не ограничено.

По умолчанию установлено значение 5 секунд.

По умолчанию флажок установлен.

Окно Сетевое пакетное правило

Название правила

Имя сетевого пакетного правила.

В разделе **Действие** можно выбрать действие, которое Kaspersky Endpoint Security выполнит при обнаружении сетевой активности.

В разделе **Протокол** можно указать протокол, к которому применяется сетевое правило.

В разделе **Направление** можно указать направление отслеживаемой сетевой активности.

В разделе **TTL** можно задать срок жизни отслеживаемых сетевых пакетов.

В разделе **Сетевые адаптеры** можно указать сетевые адаптеры, к которым применяется сетевое правило.

В разделе **Удаленный адрес** можно указать сетевые адреса удаленных устройств, которые могут отправлять и получать сетевые пакеты.

В разделе **Локальный адрес** можно указать локальные сетевые адреса устройств, которые могут отправлять и получать сетевые пакеты.

Записывать в отчет

Этот флажок включает и выключает запись событий Сетевого экрана.

Если флажок установлен, Kaspersky Endpoint Security записывает события Сетевого экрана в отчет.

Если флажок снят, Kaspersky Endpoint Security не записывает события Сетевого экрана в отчет.

По умолчанию флажок снят.

Окно Сетевой адаптер

Имя адаптера

Имя сетевого адаптера.

Тип интерфейса

В выпадающем списке можно выбрать тип интерфейса сетевого адаптера.

IP-адреса

Список IP-адресов.

MAC-адреса

Список MAC-адресов.

Окно Сетевые адаптеры

Название

В этой графе отображается имя сетевого адаптера.

Тип интерфейса

В этой графе отображается тип интерфейса сетевого адаптера.

IP-адреса

В этой графе отображаются IP-адреса сетевого адаптера.

MAC-адреса

В этой графе отображаются MAC-адреса сетевого адаптера.

Окно Локальные адреса

Локальные адреса

В этой графе отображаются локальные адреса.

Окно Локальный адрес

Тип

Этот раскрывающийся список позволяет указать тип записи локального IP-адреса, к которой вы хотите применить сетевое правило.

IP-адрес

Поле ввода IP-адреса. Это поле доступно, только если вы выбрали **IP-адрес** в раскрывающемся списке **Тип**.

Начало диапазона

Поле для ввода начала диапазона IP-адресов. Это поле доступно, только если вы выбрали **Диапазон IP-адресов** в раскрывающемся списке **Тип**.

Конец диапазона

Поле ввода конца диапазона IP-адресов. Это поле доступно, только если вы выбрали **Диапазон IP-адресов** в раскрывающемся списке **Тип**.

Окно Удаленные адреса

Удаленные адреса

В этой графе отображаются удаленные адреса.

Окно Удаленный адрес

Тип

Этот раскрывающийся список позволяет указать тип записи удаленного адреса, к которой вы хотите применить сетевое правило.

Адрес

Поле ввода IP-адреса или DNS-имени. Это поле доступно, только если вы выбрали **IP-адрес или DNS-имя** в раскрывающемся списке **Тип**.

Начало диапазона

Поле для ввода диапазона IP-адресов. Это поле доступно, только если вы выбрали **Диапазон IP-адресов** в раскрывающемся списке **Тип**.

Конец диапазона

Поле ввода конца диапазона IP-адресов. Это поле доступно, только если вы выбрали **Диапазон IP-адресов** в раскрывающемся списке **Тип**.

Окно Шаблоны

Шаблоны сетевого правила

В этой графе отображаются шаблоны сетевых правил.

Окно Сетевое пакетное правило

Сетевая служба

Имя сетевого правила.

Действие

Действие, которые выполняет Сетевой экран при обнаружении типа сетевой активации.

Адрес

Сетевые адреса, к которым применяется сетевое правило.

Вкладка Доступные сети

Название

В этой графе отображается название сети.

Статус сети

В этой графе отображается статус сети.

IP-адрес

В этой графе отображаются сетевые IP-адреса.

Окно Доступная сеть

Имя сети

Имя сети.

Статус сети

Раскрывающийся список статуса сети.

IP-адрес

Сетевой IP-адрес.

Окно MAC-адрес

Тип

В этом раскрывающемся списке вы можете указать тип записи MAC адреса, к которой вы хотите применить сетевое правило.

MAC-адрес

Поле ввода MAC-адреса. Это поле доступно только в том случае, если вы выбрали **MAC-адрес** в раскрывающемся списке **Тип**.

Маска

Поле ввода маски MAC-адреса. Это поле доступно только в том случае, если вы выбрали **Маска MAC-адреса** в раскрывающемся списке **Тип**.

Начало диапазона

Поле для ввода начала диапазона MAC-адресов. Это поле доступно только в том случае, если вы выбрали **Диапазон MAC-адресов** в раскрывающемся списке **Тип**.

Конец диапазона

Поле ввода конца диапазона MAC адресов. Это поле доступно только в том случае, если вы выбрали **Диапазон MAC-адресов** в раскрывающемся списке **Тип**.

Отчет Системные события

В правой части окна представлен отчет о работе Kaspersky Endpoint Security.

Время

В этой графе отображается дата и время события.

Событие

В этой графе указан статус события.

Имя программы

В этой графе отображается название программы, в которой произошло событие.

Пользователь

В этой графе указан пользователь, который инициировал событие.

Тип пользователя

В этой графе указан тип пользователя, который инициировал событие.

При нажатии на кнопку открывается окно, из которого вы можете экспортировать отчет в файл в формате TXT.

Отчет Обработанные объекты

В правой части окна представлен список всех зараженных объектов, а также опасных объектов веб-трафика, которые обнаружило приложение Kaspersky Endpoint Security.

Время

В этой графе отображается время обнаружения объекта.

Объект

В этой графе отображается путь к местоположению, в котором был обнаружен объект или веб-адрес объекта.

Статус

В этой графе отображается действие, выполненное приложением при обнаружении объекта.

Обнаружено

В этой графе указан тип обнаруженного объекта согласно классификации Вирусной энциклопедии "Лаборатории Касперского".

Имя

В этой графе отображается имя обнаруженного объекта согласно классификации Вирусной энциклопедии "Лаборатории Касперского".

При нажатии на кнопку открывается окно, из которого вы можете экспортировать отчет в файл в формате TXT.

Отчет Обновление баз

В правой части окна представлены отчеты по задачам обновления, выполненным приложением.

Запущено

В этой графе отображается дата и время запуска каждой задачи обновления. Если список операций раскрыт, в этом столбце также перечислены операции, выполненные при обновлении приложения, и время, в течение которого они были выполнены.

Статус

В этой графе отображается статус задачи обновления.

Размер

В этой графе отображается размер загруженных файлов обновления.

Средняя скорость

В этой графе отображается скорость загрузки файлов обновления.

Окончание

В этой графе отображается время завершения задачи обновления.

При нажатии на кнопку раскрывается список операций, входящих в задачу обновления.

При нажатии на кнопку скрывается список операций, входящих в задачу обновления.

При нажатии на кнопку открывается окно, из которого вы можете экспортировать отчет в файл в формате TXT.

Отчет Проверка

В правой части окна представлены отчеты по задачам проверки, выполненным Kaspersky Endpoint Security.

Задача

В этой графе отображается имя задачи проверки.

Статус

В этой графе отображается текущий статус задачи проверки или статус проверяемых объектов.

Дата

В этом столбце отображается дата и время задачи проверки.

Инициатор

В этой графе отображается пользователь, программа или процесс, который запустил задачу проверки.

При нажатии на кнопку раскрывается список проверяемых объектов.

При нажатии на кнопку скрывается список проверяемых объектов.

При нажатии на кнопку открывается окно, из которого вы можете экспортировать отчет в файл в формате TXT.

Отчет Защита от файловых угроз

В правой части окна представлен отчет о работе Защиты от файловых угроз.

Дата

В этой графе отображается время и дата обращения программы к проверяемому объекту.

Путь

В этой графе указан путь к исходному местонахождению проверяемого объекта.

Статус

В этой графе указан статус, присвоенный проверяемому объекту.

Имя программы

В этой графе указано название программы, которая обращалась к проверяемому объекту.

При нажатии на кнопку открывается окно, из которого вы можете экспортировать отчет в файл в формате TXT.

Отчет Защита от веб-угроз

В правой части окна представлен отчет о работе Защиты от веб-угроз.

Дата

В этой графе отображается время и дата обнаружения опасного объекта веб-трафика.

URL

В этой графе отображаются опасные объекты веб-трафика, которые были обнаружены Защитой от веб-угроз. Для каждого обнаруженного объекта веб-трафика указан веб-адрес, по которому он был обнаружен.

Статус

В этой графе указан статус обнаруженного опасного объекта веб-трафика.

Имя программы

В этой графе указано название программы, которая обращалась к обнаруженному опасному объекту веб-трафика.

При нажатии на кнопку открывается окно, из которого вы можете экспортировать отчет в файл в формате TXT.

Отчет Защита от почтовых угроз

В правой части окна представлен отчет о работе Защиты от почтовых угроз.

Дата

В этой графе отображается дата и время обнаружения зараженного объекта в сообщении электронной почты.

Путь

В этой графе отображается информация о сообщении электронной почты, в котором был обнаружен зараженный объект.

Статус

В этой графе отображается действие, выполненное Kaspersky Endpoint Security при обнаружении зараженного объекта.

Имя программы

В этой графе отображается название почтового клиента.

При нажатии на кнопку открывается окно, из которого вы можете экспортировать отчет в файл в формате TXT.

Отчет Защита от сетевых угроз

В правой части окна представлен отчет о работе Защиты от сетевых угроз.

Дата

В этой графе отображаются дата и время обнаружения опасной сетевой активности компьютера.

IP-адрес

В этой графе отображается IP-адрес компьютера, от которого исходила опасная сетевая активность, обнаруженная Kaspersky Endpoint Security.

Статус

В этой графе отображается действие, выполненное Kaspersky Endpoint Security при обнаружении опасной сетевой активности.

Тип атаки

В этой графе отображается тип обнаруженной сетевой атаки.

Локальный порт

В этой графе отображается номер локального порта, через который была произведена попытка вторжения.

Протокол

В этой графе указан тип протокола, который был использован для сетевой атаки.

При нажатии на кнопку открывается окно, из которого вы можете экспортировать отчет в файл в формате TXT.

Отчет Endpoint Detection and Response

В правой части окна представлен отчет о работе Endpoint Detection and Response.

Дата

В этой графе отображается дата и время событий.

Событие

В этой графе указан статус событий.

При нажатии на кнопку открывается окно, из которого вы можете экспортировать отчет в файл в формате TXT.

Отчет Сетевой экран

В правой части окна представлен отчет о работе Сетевого экрана.

Дата

В этой графе отображается дата и время событий.

Событие

В этой графе указан статус событий.

При нажатии на кнопку открывается окно, из которого вы можете экспортировать отчет в файл в формате TXT.

Отчет Защита от эксплойтов

В правой части окна представлен отчет о работе Защиты от эксплойтов.

Дата

В этой графе отображается дата и время событий.

Событие

В этой графе указан статус событий.

При нажатии на кнопку открывается окно, из которого вы можете экспортировать отчет в файл в формате TXT.

Отчет Контроль устройств

В правой части окна представлен отчет о работе Контроля устройств.

Дата

В этой графе отображается дата и время событий.

Событие

В этой графе указан статус событий.

При нажатии на кнопку открывается окно, из которого вы можете экспортировать отчет в файл в формате TXT.

Отчет Мониторинг активности

В правой части окна представлен отчет о работе Мониторинга активности.

Дата

В этой графе отображается дата и время событий.

Событие

В этой графе указан статус событий.

При нажатии на кнопку открывается окно, из которого вы можете экспортировать отчет в файл в формате TXT.

Окно Техническая поддержка пользователей

В окне содержится следующая информация:

- версия Kaspersky Endpoint Security;
- дата выпуска антивирусных баз, используемых Kaspersky Endpoint Security;
- версия установленной на компьютере операционной системы.

Служба технической поддержки

При нажатии на кнопку открывается база знаний Службы технической поддержки, где вы найдете статьи о Kaspersky Endpoint Security, опубликованные специалистами Службы технической поддержки.

Сообщество пользователей

При нажатии на кнопку открывается страница сообщества, где вы можете обсудить Kaspersky Endpoint Security со специалистами "Лаборатории Касперского" и другими пользователями.

Закрыть

При нажатии на кнопку окно поддержки пользователей закрывается.

Окно Параметры сертификата

На вкладке **Основные** вы можете выбрать хранилище сертификатов для проверки зашифрованного HTTPS-трафика в браузере Mozilla Firefox:

- **Связка ключей для корневых системных сертификатов (рекомендовано)**
- **Хранилище сертификатов в настройках браузера Mozilla Firefox**

  В этом случае вам нужно вручную добавить сертификат Kaspersky Endpoint Security в хранилище сертификатов браузера Mozilla Firefox. Дополнительные сведения см. в разделе Как добавить сертификат Kaspersky Endpoint Security в хранилище сертификатов Mozilla Firefox.

На вкладке **Надежные сертификаты** вы можете создать список доверенных корневых сертификатов для подключения к соответствующим серверам без уведомлений.

Список доверенных корневых сертификатов по умолчанию пуст.

+

При нажатии на эту кнопку открывается диалоговое окно для добавления сертификата, который будет считаться доверенным.

–

При нажатии на кнопку выбранный сертификат удаляется из списка доверенных сертификатов.

Имя сертификата

В этом столбце отображаются имена доверенных корневых сертификатов.

Отменить

При нажатии на эту кнопку окно закрывается без сохранения изменений.

Сохранить

При нажатии на эту кнопку текущий список доверенных корневых сертификатов сохраняется, и окно закрывается.

Окно Проверка сертификата

Показать сертификат

При нажатии на эту кнопку открывается системное окно с информацией о сертификате.

Отмена

При нажатии на кнопку окно закрывается.

Добавить в доверенные

При нажатии на эту кнопку сертификат добавляется в список доверенных сертификатов. В результате вы сможете подключаться к соответствующему серверу без уведомлений.

Подключиться

При нажатии на эту кнопку вы подключаетесь к серверу.

> **Примечание.** Доступные кнопки могут отличаться в зависимости от типа сертификата.

Окно Выбор сертификата

Список доступных сертификатов

Установите флажок рядом с сертификатом, чтобы использовать его при подключении к серверу.

Показать сертификат

При нажатии на эту кнопку открывается системное окно с информацией о сертификате.

Отменить

При нажатии на кнопку окно закрывается.

Продолжить

При нажатии на эту кнопку вы подключаетесь к серверу с использованием выбранного