kaspersky

Kaspersky Endpoint Security для Mac

Подготовительные процедуры и руководство по эксплуатации

Версия программы: 12.0.0.325

kaspersky

Уважаемый пользователь!

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

Дата изменения документа: 30.11.2023

Обозначение документа: 643.46856491.00053-05 90 01

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

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

kaspersky

Содержание

kaspersky

Об этом документе

Настоящий документ представляет собой подготовительные процедуры и руководство по эксплуатации программного изделия «Kaspersky Endpoint Security для Mac» (далее также «Kaspersky Endpoint Security», «приложение»).

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

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

В документе также содержатся разделы с дополнительной информацией о приложении.

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

kaspersky

Источники информации о приложении

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

Страница Kaspersky Endpoint Security на сайте "Лаборатории Касперского"

На странице Kaspersky Endpoint Security на сайте "Лаборатории Касперского" (https://www.kaspersky.ru/business-security/endpoint-mac) 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 (https://support.kaspersky.ru/kes11mac?page=kb) 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 с другими пользователями на нашем Форуме (https://community.kaspersky.com/produkty-kaspersky-dlya-biznesa-31).

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

Переход на Форум из меню "Справка"

3. Выберите **Справка** > **Поддержка**.
4. Нажмите на кнопку **Сообщество пользователей**.

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 "Лаборатории Касперского" (см. раздел "Способы получения технической поддержки" на странице 171).

kaspersky

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

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.

kaspersky

О программе

Программное изделие «Kaspersky Endpoint Security для Mac» представляет собой средство антивирусной защиты типа «Б» второго класса защиты и предназначено для применения на серверах информационных систем.

Основными угрозами, для противостояния которым используется программное изделие, являются угрозы, связанные с внедрением в информационные системы из информационно-телекоммуникационных сетей, в том числе сетей международного информационного обмена (сетей связи общего пользования) и / или съемных машинных носителей информации, вредоносных компьютерных программ (вирусов) (КВ).

В программном изделии реализованы следующие функции безопасности:

- разграничение доступа к управлению приложением;
- управление работой приложения;
- управление параметрами приложения;
- управление установкой обновлений (актуализации) базы данных признаков вредоносных компьютерных программ (вирусов) (БД ПКВ);
- аудит безопасности приложения;
- выполнение проверок объектов воздействия;
- обработка объектов воздействия;
- сигнализация приложения;
- контроль доступа к веб-ресурсам;
- контроль целостности компонентов приложения.

kaspersky

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.

kaspersky

Таблица 1. Сравнение функций Kaspersky Endpoint Security

Функция	Kaspersky Security Center		
	Консоль администрирования	Web Console	Cloud Console
Продвинутая защита			
Kaspersky Security Network	✓	✓	✓
Базовая защита			
Защита от файловых угроз	✓	✓	✓
Защита от веб-угроз	✓	✓	✓
Защита от сетевых угроз	✓	✓	✓
Контроль безопасности			
Веб-Контроль	✓	✓	✓
Шифрование данных			
Шифрование дисков с помощью FileVault®	✓	✓	✓
Ключ восстановления	✓	✓	✓
Detection and Response			
Managed Detection and Response	✓	✓	✓
Endpoint Detection and Response (KATA)	✓	✓	✓
Задачи			
Добавление ключа	✓	✓	✓
Обновление	✓	✓	✓
Откат обновления	✓	✓	✓
Проверка	✓	✓	✓

kaspersky

Требования

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

В этом разделе

Указания по эксплуатации и требования к среде

1. Установка, конфигурирование и управление программой должны осуществляться в соответствии с эксплуатационной документацией.
2. Программа должна эксплуатироваться на компьютерах, отвечающих минимальным требованиям, приведенным в разделе "Аппаратные и программные требования".
3. Перед установкой и началом эксплуатации программы необходимо установить все доступные обновления для используемых версий ПО среды функционирования.
4. Должен быть обеспечен доступ программы ко всем объектам информационной системы, которые необходимы программе для реализации своих функциональных возможностей (к контролируемым объектам информационной системы).
5. Должна быть обеспечена совместимость программы с контролируемыми ресурсами информационной системы.
6. Должна быть обеспечена возможность корректной совместной работы программы со средствами антивирусной защиты других производителей в случае их совместного использования в информационной системе.
7. Должна быть обеспечена физическая защита элементов информационной системы, на которых установлена программа.
8. Должна быть обеспечена синхронизация по времени между компонентами программы, а также между программой и средой ее функционирования.
9. Персонал, ответственный за функционирование программы, должен обеспечивать надлежащее функционирование программы, руководствуясь эксплуатационной документацией.
10. Должна быть обеспечена доверенная связь между программой и уполномоченными субъектами информационной системы (администраторами безопасности).
11. Функционирование программы должно осуществляться в среде функционирования, предоставляющей механизмы аутентификации и идентификации администраторов безопасности программы.
12. Должен быть обеспечен доверенный канал получения обновлений БД ПКВ.
13. Должна быть обеспечена защищенная область для выполнения функций безопасности программы.
14. Управление атрибутами безопасности, связанными с доступом к функциям и данным программы, должно предоставляться только уполномоченным ролям (администраторам программы и информационной системы).

15. Администратор должен установить в среде ИТ максимальное число попыток неуспешных попыток аутентификации с момента последней успешной попытки аутентификации пользователя с последующей блокировкой попыток аутентификации при превышении установленного значения.
16. Администратор должен задать метрику качества паролей, включающую требования к длине паролей, требования по запрещению использования определенных комбинаций символов, а также требования к категории используемых символов.
17. Должна быть обеспечена синхронизация по времени с другими компонентами Kaspersky Endpoint Detection and Response, а также программы и ее средой функционирования.

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® 12, 13 или 14;
- доступ в интернет.

Поддерживаемые браузеры:

- Safari®;
- Chrome™;
- Firefox™.

Kaspersky Endpoint Security совместим со следующими средствами виртуализации:

- Parallels Desktop 16 для Mac Business Edition;
- VMware Fusion™ 11.5 Professional;
- VMware Fusion 12 Professional.

Профили MDM могут быть развернуты на серверах Jamf и Apple. Если вы используете другие серверы, см. статью на сайте Службы технической поддержки https://support.kaspersky.com/15647#block2 (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 13 или более поздней версии:

- Kaspersky Security Center 13
- Kaspersky Security Center 13.1;
- Kaspersky Security Center 13.2;
- Kaspersky Security Center 14;
- Kaspersky Security Center 14.1;
- Kaspersky Security Center 14.2;
- Kaspersky Security Center Linux 14.2;
- Kaspersky Security Center Linux 15.

Для управления Kaspersky Endpoint Security для Mac 12 через Kaspersky Security Center вам нужно установить Агент администрирования версии 15 на удаленные компьютеры.

kaspersky

Установка и удаление приложения

В этом разделе

Подготовка к установке приложения

Перед установкой приложения на компьютер рекомендуется выполнить следующие действия:

- Убедитесь, что ваш компьютер соответствует аппаратным и программным требованиям (на странице 15).
- Удалите с компьютера Kaspersky Internet Security для Mac или другие антивирусные программы, чтобы избежать возникновения системных конфликтов и снижения быстродействия операционной системы.

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 https://support.kaspersky.com/15647.

Установка Kaspersky Endpoint Security

Специалисты "Лаборатории Касперского" рекомендуют устанавливать Kaspersky Endpoint Security только способами, описанными в этом руководстве.

- 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 (см. раздел "Установка и удаление Kaspersky Endpoint Security" на странице 99).
- 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 https://support.kaspersky.ru/KSC/14.2/ru-RU/5022.htm. Подробную информацию о развертывании приложений "Лаборатории Касперского" с помощью Kaspersky Security Center Cloud Console вы можете найти в справке Kaspersky Security Center Cloud Console https://support.kaspersky.ru/KSC/CloudConsole/ru-RU/5022.htm.

- Удаленно из файла формата PKG с помощью JAMF.

  Подробную информацию об установке Kaspersky Endpoint Security из файла формата PKG с помощью JAMF см. в статье на сайте Службы технической поддержки (https://support.kaspersky.com/15951) (База знаний).

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 https://support.kaspersky.com/15647.

► *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.

► *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**, 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 https://support.apple.com/ru-ru/remote-desktop.
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.

► *Установка Kaspersky Endpoint Security из файла формата PKG с помощью JAMF*

1. Создайте установщик формата PKG для Kaspersky Endpoint Security с помощью JAMF Composer.
2. Загрузите установщик формата PKG на сервер распространения пакетов (JAMF Share).
3. Создайте политики для установки Kaspersky Endpoint Security на управляемые устройства с помощью JAMF Pro.

Подробную информацию об установке Kaspersky Endpoint Security из файла формата PKG с помощью JAMF см. в статье на сайте Службы технической поддержки (https://support.kaspersky.com/15951) (База знаний).

Подготовка приложения к работе

После установки Kaspersky Endpoint Security вам нужно выполнить следующие действия:

- Активировать Kaspersky Endpoint Security (на странице 40). 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.
- Если компонент Endpoint Detection and Response не поддерживается вашей текущей лицензией, вам необходимо активировать Kaspersky Endpoint Detection and Response отдельно.
- Проверить состояние защиты компьютера (см. раздел "Просмотр сведений о состоянии защиты компьютера" на странице 45).
- Обновить Kaspersky Endpoint Security (см. раздел "Обновление баз приложения" на странице 50).

- Проверить компьютер на вредоносные программы (см. раздел "Запуск задач проверки" на странице 49).

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.

kaspersky

Процедура приемки

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

В этом разделе

Безопасное состояние

Программа находится в безопасном состоянии (сертифицированной конфигурации), если соблюдены следующие условия:

- Программа активирована (см. раздел «Активация Kaspersky Endpoint Security» на стр. 40)
- Параметры программы находятся в рамках допустимых значений, приведенных в приложении к этому документу (см. раздел «Приложения. Сертифицированное состояние программы: параметры и их значения» на стр. 181).
- Базы программы находятся в актуальном состоянии (см. раздел «Обновление баз программы» на стр. 50).

Проверка работоспособности приложения

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

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

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

Вы можете загрузить тестовый файл EICAR со страницы веб-сайта организации EICAR https://www.eicar.org/download-anti-malware-testfile/.

► *Чтобы проверить работоспособность программы:*

1. Отключите защиту компьютера (см. раздел «Выключение и возобновление защиты компьютера» на стр. 46).
2. Сохраните тестовый файл EICAR на компьютере.

3. Запустите выборочную проверку папки, в которой вы сохранили тестовый файл EICAR (см. раздел «Запуск задач проверки» на стр. 49).
4. Откройте отчет о выполнении задач проверки (см. инструкцию на стр. 52).
5. Убедитесь, что в отчете отображается правильная информация об обнаружении тестового файла EICAR.

По завершении проверки работоспособности программы рекомендуется незамедлительно включить защиту компьютера.

kaspersky

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 (на странице 40).

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 приложение Kaspersky Endpoint Security контролировало опасную активность файлов и процессы, запускаемые на вашем Mac, установите системное расширение. Для этого нажмите на кнопку **Установить** рядом с элементом **Системное расширение** и следуйте инструкциям на экране.
   - Если вы хотите, чтобы Защита от веб-угроз проверяла сетевые пакеты до того, как они нанесут вред вашему Mac, 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.

   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.

Разделение доступа к функциям программы по пользовательским ролям

По правам пользователи делятся на следующие группы:

- администратор Kaspersky Security Center (администратор безопасности);
- пользователь Mac с правами администратора компьютера (администратор сервера);
- пользователь Mac без прав администратора компьютера (пользователь).

Администратору Kaspersky Security Center доступны все функции программы. С помощью политик администратор Kaspersky Security Center определяет, какие функции программы доступны пользователю Mac с правами администратора компьютера. Пользователь Mac без прав администратора компьютера может запускать задачи антивирусной проверки и обновления баз, а также просматривать настройки и отчеты программы.

kaspersky

Интерфейс приложения Kaspersky Endpoint Security

В этом разделе

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 (см. раздел "Использование Центра защиты" на странице 48).
Безопасность	Нажмите, чтобы просмотреть рабочее состояние установленных компонентов. Узнать больше (см. раздел "Просмотр рабочего состояния установленных компонентов" на странице 45).
Проверка	Нажмите, чтобы управлять задачами сканирования. Узнать больше (см. раздел "Проверка" на странице 65).

Обновление	Нажмите, чтобы управлять задачами обновления. Узнать больше (см. раздел "Задачи обновления" на странице 69).
Лицензия	Нажмите, чтобы активировать приложение или просмотреть информацию о вашей лицензии.

Элементы управления на странице Мониторинг**.**

Страница **Мониторинг** отображает индикатор состояния защиты (см. раздел "Просмотр сведений о состоянии защиты компьютера" на странице 45), предоставляет информацию о том, что Kaspersky Endpoint Security делает для защиты вашего компьютера, а также содержит следующие элементы управления.

Центр защиты	Сообщает о проблемах с защитой компьютера. Узнать больше (см. раздел "Использование Центра защиты" на странице 48).
Отчеты	Позволяет просматривать события, произошедшие в процессе работы приложения, отдельных компонентов и задач. Узнать больше (см. раздел "Отчеты" на странице 73).
Резервное хранилище	Позволяет просмотреть список сохраненных копий зараженных файлов, удаленных приложением. Узнать больше. Узнать больше (см. раздел "Резервное хранилище" на странице 71).
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 в контекстном меню значка приложения пункт **Настройки**.

   Откроется окно настройки приложения.

2. На закладке **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 в контекстном меню значка приложения 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 закладки, расположенные в верхней части окна настройки приложения:

- **Базовая**. На этой закладке 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 закладке вы можете настроить параметры задач проверки и запуск проверки по расписанию.
- **Угрозы**. На этой закладке вы можете выбрать категории обнаруживаемых объектов, сформировать Доверенную зону и настроить параметры резервного хранилища.
- **Дополнительно**. На этой закладке вы можете присоединиться к участию в Kaspersky Security Network или отказаться от участия.

- **Обновление**. На этой закладке вы можете настроить параметры обновления приложения или вернуться к использованию предыдущей версии баз.
- **Интерфейс**. На этой закладке 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**.

kaspersky

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 в контекстном меню значка приложения пункт **Настройки**.

   Откроется окно настройки приложения.

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

► *Включение записи некритических событий*

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

   Откроется окно настройки приложения.

2. На закладке **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 (см. раздел "Отчеты" на странице 73) 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 в контекстном меню значка приложения пункт **Настройки**.

   Откроется окно настройки приложения.

2. На закладке **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.

kaspersky

Лицензирование приложения Kaspersky Endpoint Security

В этом разделе

О Лицензионном соглашении

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

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 обычно 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.

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.

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

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

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" (https://keyfile.kaspersky.com/ru/) 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

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 действующей 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; 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: 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; 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 действующей 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; дата и время запуска компонента мониторинг активности; версия компонента ПО; идентификатор обновления ПО; дата и время установки ПО; тип установленного 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 проверяемых объектах и действиях: 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 и URL-адресов: 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 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 в контекстном меню значка приложения 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 программы и ее модулей;
- информацию о подписке (тип подписки, регион);
- информацию о языке интерфейса, идентификатор программы, кастомизацию программы, версию программы, уникальный идентификатор установки программы, 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 программ (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.

Файлы трассировки могут содержать конфиденциальные данные. Отправляя файлы отчетов 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

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

Активация приложения заключается в добавлении ключа в приложение.

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

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.

   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**.

   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.

   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.

При устаревании баз вредоносного ПО риск заражения вашего компьютера возрастает.

► *Продление срока действия лицензии*

1. На боковой панели главного окна приложения (на странице 23) нажмите на кнопку **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 **Посетить 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  .

kaspersky

Решение типовых задач

В этом разделе

Запуск и остановка приложения

Сразу после установки приложение запускается автоматически, и в строке меню появляется значок приложения (см. раздел "Значок Kaspersky Endpoint Security" на странице 24).

► *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.

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

kaspersky

Просмотр сведений о состоянии защиты компьютера

Индикатор состояния защиты, имеющий форму щита и расположенный в главном окне приложения (на странице 23), информирует вас о проблемах с защитой компьютера. 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 (на странице 23).
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.

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.

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 (см. раздел "Значок Kaspersky Endpoint Security" на странице 24) 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.

Выключение или приостановка работы компонентов защиты не оказывает влияния на выполнение задач проверки (см. раздел "Проверка" на странице 65) и задачи обновления (ст. раздел "Задачи обновления" на странице 69).

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 в контекстном меню значка приложения пункт **Настройки**.

   Откроется окно настройки приложения.

2. На закладке **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**.

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 в контекстном меню значка приложения пункт **Настройки**.

   Откроется окно настройки приложения.

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

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 в контекстном меню значка приложения пункт **Настройки**.

   Откроется окно настройки приложения.

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

Также вы можете включить защиту компьютера или компоненты защиты в Центре защиты (см. раздел "Использование Центра защиты" на странице 48). 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 (на странице 23) нажмите на кнопку **Центр защиты**.

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

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.

kaspersky

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 (на странице 23) нажмите на кнопку **Проверка**.

   Откроется окно **Проверка**.

2. Нажмите на кнопку **Запустить Полную проверку**.

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 (на странице 23) нажмите на кнопку **Проверка**.

   Откроется окно **Проверка**.

2. Нажмите на кнопку **Запустить Быструю проверку**.

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 (см. раздел "Значок Kaspersky Endpoint Security" на странице 24) в панели Dock.
- Перетащите выбранный объект в окно **Проверка**.

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

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 (на странице 23) нажмите на кнопку **Проверка**.

   Откроется окно **Проверка**.

2. Нажмите на кнопку  .

   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 **ОК**.

► *Настройка расписания запуска задачи проверки из окна настройки приложения*

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

   Откроется окно настройки приложения.

2. На закладке **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 **ОК**, 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.

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 (на странице 23) нажмите на кнопку **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*

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

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 (см. раздел "Область защиты компьютера" на странице 54).

kaspersky

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.

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 закладке **Обработанные объекты**. Системные события отображаются на закладке **Системные события**. Дополнительно, подробный отчет формируется для каждого компонента приложения: Защиты от файловых угроз (на странице 57), Защиты от веб-угроз (на странице 60), Защиты от сетевых угроз (на странице 62), задач проверки (на странице 65) и обновления (на странице 69).

► *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".

kaspersky

Расширенная настройка приложения

В этом разделе

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 в контекстном меню значка приложения пункт **Настройки**.

   Откроется окно настройки приложения.

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

   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 (на странице 57), защиты от веб-угроз (на странице 60) и при выполнении задач проверки (см. раздел "Проверка" на странице 65).

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.

Если в настройках политики администратор запрещает изменение параметров Доверенной зоны, пользователи не могут открыть параметры Доверенной зоны.

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

   Откроется окно настройки приложения.

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

   Откроется окно настройки Доверенной зоны.

3. На закладке **Доверенные файлы и папки** отредактируйте 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 **OK**.

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

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

   Откроется окно настройки приложения.
2. На закладке **Угрозы** в блоке **Исключения** нажмите на кнопку **Доверенная зона**.

   Откроется окно настройки Доверенной зоны.
3. На закладке **Доверенные веб-адреса** отредактируйте 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.

► *Включение контроля доверенных веб-адресов*

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

   Откроется окно настройки приложения.
2. На закладке **Угрозы** в блоке **Исключения** нажмите на кнопку **Доверенная зона**.

   Откроется окно настройки Доверенной зоны.

3. На закладке **Доверенные веб-адреса** снимите флажок рядом с веб-адресом, который приложение Kaspersky Endpoint Security должно контролировать.
4. Нажмите **OK**.

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 в контекстном меню значка приложения пункт **Настройки**.

   Откроется окно настройки приложения.
2. На закладке **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 (см. раздел "Использование Центра защиты" на странице 48). 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 в контекстном меню значка приложения пункт **Настройки**.

   Откроется окно настройки приложения.
2. На закладке **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.

   > 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"**.

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 в контекстном меню значка приложения пункт **Настройки**.

Откроется окно настройки приложения.

2. На закладке **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.

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"**.

   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 в контекстном меню значка приложения пункт **Настройки**.

   Откроется окно настройки приложения.

2. На закладке **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.

   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 в контекстном меню значка приложения пункт **Настройки**.

   Откроется окно настройки приложения.

2. На закладке **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.

   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"**.

   В целях безопасности оптимизация может быть выключена.

4. Нажмите на кнопку **Сохранить**.

Когда вы или программа 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 в контекстном меню значка приложения пункт **Настройки**.

   Откроется окно настройки приложения.

2. На закладке **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.

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 (см. раздел "Обращение в Службу технической поддержки" на странице 169).

► *Просмотр отчета о работе компонента Защита от файловых угроз*

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

   Откроется окно **Отчеты**.

2. Откройте закладку **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.

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 в контекстном меню значка приложения пункт **Настройки**.

   Откроется окно настройки приложения.

2. На закладке **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 (см. раздел "Использование Центра защиты" на странице 48). Выключение защиты или компонентов защиты значительно повышает риск заражения компьютера, поэтому информация о выключении защиты отображается в Центре защиты.

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 (см. раздел "Участие в Kaspersky Security Network" на странице 78).

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 (см. раздел "Участие в Kaspersky Security Network" на странице 78).

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 в контекстном меню значка приложения пункт **Настройки**.

   Откроется окно настройки приложения.

2. На закладке **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.

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 (см. раздел "Обращение в Службу технической поддержки" на странице 169).

► *Просмотр отчета о работе защиты от веб-угроз*

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

   Откроется окно **Отчеты**.

2. Откройте закладку **Защита от веб-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 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 в контекстном меню значка приложения пункт **Настройки**.

   Откроется окно настройки приложения.

2. На закладке **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 (см. раздел "Использование Центра защиты" на странице 48). Выключение защиты или компонентов защиты значительно повышает риск заражения компьютера, поэтому информация о выключении защиты отображается в Центре защиты.

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 в контекстном меню значка приложения пункт **Настройки**.

   Откроется окно настройки приложения.

2. На закладке **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 закладку **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 в контекстном меню значка приложения пункт **Настройки**.

   Откроется окно настройки приложения.
2. На закладке **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 закладку **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.

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 (см. раздел "Обращение в Службу технической поддержки" на странице 169).

► *Просмотр отчета о работе защиты от сетевых угроз*

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

   Откроется окно **Отчеты**.

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

Проверка

Компоненты Защита от файловых угроз (на странице 57) и Защита от веб-угроз (на странице 60) обеспечивают постоянную защиту компьютера. Также мы рекомендуем регулярно проверять компьютер на вредоносное ПО 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).

Каждая задача проверки выполняется в заданной области проверки и запускается вручную. Для распознавания вредоносных объектов Kaspersky Endpoint Security использует сигнатурный анализ, а также эвристический анализ и другие технологии проверки.

► *Запуск задач полной проверки и быстрой проверки*

1. На боковой панели главного окна приложения (на странице 23) нажмите на кнопку **Проверка**.

   Откроется окно **Проверка**.

2. В окне **Проверка** нажмите на кнопку **Запустить Полную проверку** или **Запустить Быструю проверку**.

Запустится задача проверки.

► *Запуск задачи выборочной проверки*

1. На боковой панели главного окна приложения (на странице 23) нажмите на кнопку **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 (на странице 23) нажмите на кнопку **Проверка**.

   Откроется окно **Проверка**.
2. В окне **Проверка** нажмите на кнопку **Остановить** 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 (на странице 23) нажмите на кнопку **Проверка**.

   Откроется окно **Проверка**.
2. Нажмите на кнопку  .

   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 в контекстном меню значка приложения пункт **Настройки**.

   Откроется окно настройки приложения.
2. На закладке **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.

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.

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.

► *Включение и выключение проверки системного тома "только для чтения"*

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

   Откроется окно настройки приложения.
2. На закладке **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"**.

   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 в контекстном меню значка приложения пункт **Настройки**.

   Откроется окно настройки приложения.
2. На закладке **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 в контекстном меню значка приложения пункт **Настройки**.

   Откроется окно настройки приложения.

2. На закладке **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 в контекстном меню значка приложения пункт **Настройки**.

   Откроется окно настройки приложения.

2. На закладке **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 в контекстном меню значка приложения пункт **Настройки**.

   Откроется окно настройки приложения.

2. На закладке **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.

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 закладку **Проверка**.

Информация о ходе выполнения каждой задачи проверки (процент выполнения и оставшееся до завершения время) отображается в окне **Проверка**.

Задачи обновления

Своевременное обновление баз приложения – залог безопасности вашего компьютера. Защита от файловых угроз (на странице 57), защита от веб-угроз (на странице 60) и задачи проверки (см. раздел "Проверка" на странице 65) 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.

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 в контекстном меню значка приложения пункт **Настройки**.

   Откроется окно настройки приложения.

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

► *Проверка наличия обновлений баз Kaspersky Endpoint Security*

1. На боковой панели главного окна приложения (на странице 23) нажмите на кнопку **Обновление**.

   Откроется окно **Обновление**.

2. Нажмите на кнопку **Обновить**.

Запустится обновление баз программы.

Также вы можете запустить задачу обновления одним из следующих способов:

- Нажмите на значок программы 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 в контекстном меню значка приложения пункт **Настройки**.

   Откроется окно настройки приложения.

2. Выберите закладку **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.

При повреждении баз Kaspersky Endpoint Security рекомендуется запустить обновление (см. раздел "Обновление баз приложения" на странице 50), чтобы загрузить и установить последнюю версию баз приложения.

► *Откат последнего обновления*

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

   Откроется окно настройки приложения.
2. Выберите закладку **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. Откройте закладку **Обновление**.

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.

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 в контекстном меню значка приложения пункт **Настройки**.

   Откроется окно настройки приложения.

2. На закладке **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.

kaspersky

Отчеты

Вы можете просмотреть отчет Kaspersky Endpoint Security со списком всех обнаруженных объектов на закладке **Обработанные объекты**. Системные события отображаются на закладке **Системные события**. Дополнительно, подробный отчет формируется для каждого компонента приложения: Защиты от файловых угроз (на странице 57), Защиты от веб-угроз (на странице 60), Защиты от сетевых угроз (на странице 62), задач проверки (на странице 65) и обновления (на странице 69).

► *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 закладку 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 в контекстном меню значка приложения пункт **Настройки**.

   Откроется окно настройки приложения.
2. На закладке **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 недоступен в сертифицированной конфигурации.

kaspersky

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 можно найти в *справке Kaspersky Anti Targeted Attack Platform* https://support.kaspersky.com/KATA/6.0/ru-RU/246841.htm.

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 4.1 или более поздней версии.
- Kaspersky Security Center 13.2 или более поздней версии.
- Интеграцию с Endpoint Detection and Response можно настроить в Консоли администрирования Kaspersky Security Center (MMC), Web Console или Cloud Console.

Интеграция с Kaspersky Endpoint Detection and Response (KATA)

Для интеграции с Kaspersky Endpoint Detection and Response (KATA), выполните следующие действия:

a. **Установите компонент Endpoint Detection and Response**

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

b. **Активируйте 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**.

c. **Подключитесь 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 можно найти в *справке Kaspersky Anti Targeted Attack Platform* https://support.kaspersky.com/KATA/6.0/ru-RU/247872.htm.

   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 можно найти в *справке Kaspersky Anti Targeted Attack Platform* https://support.kaspersky.com/KATA/6.0/ru-RU/247877.htm.

   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 закладку **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 для криптоконтейнера 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.
3. Откроется окно свойств политики.
4. Выберите закладку **Параметры программы**.
5. Выберите **Detection and Response** > **Endpoint Detection and Response (KATA)**.
6. Включите переключатель **Endpoint Detection and Response (KATA)**.
7. Нажмите на кнопку **Параметры подключения к серверам**.
8. 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 для криптоконтейнера в поле **Пароль от криптоконтейнера**.

9. Нажмите **OK**.
10. Чтобы добавить сервер KATA, нажмите на кнопку **Добавить**.
11. В открывшемся окне укажите адрес и порт сервера и нажмите на кнопку **OK**.
12. Сохраните внесенные изменения.

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

Шифрование дисков с помощью FileVault

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 запустится только после ввода пользователем своих учетных данных и перезагрузки компьютера.

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.

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 от учетной записи пользователя и нажмите на кнопку **OK**.
6. Нажмите на кнопку **Продолжить**.

Пользователь может получить доступ к зашифрованному диску.

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 (см. раздел "Получение ключа восстановления для зашифрованного диска" на странице 142)

Как получить ключ восстановления с помощью Kaspersky Security Center Web Console и Cloud Console (см. раздел "Получение ключа восстановления для зашифрованного диска" на странице 157)

kaspersky

Участие в Kaspersky Security Network

В сертифицированной конфигурации Kaspersky Endpoint Security используется только Локальный KSN (KPSN), использование Глобального KSN не допускается.

Если вы принимаете участие в Kaspersky Security Network, приложение Kaspersky Endpoint Security автоматически отправляет статистическую информацию в "Лабораторию Касперского", чтобы улучшить защиту вашего Mac.

"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 в контекстном меню значка приложения пункт **Настройки**.

   Откроется окно настройки приложения.
2. На закладке **Дополнительно** в блоке **Улучшенная защита** 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**.

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 действующей 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; 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: 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; 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 действующей 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; дата и время запуска компонента мониторинг активности; версия компонента ПО; идентификатор обновления ПО; дата и время установки ПО; тип установленного 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 проверяемых объектах и действиях: 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 и URL-адресов: 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 о работе компонента Веб-Контроль: версия компонента, причина категоризации, дополнительная информация о причине категоризации, категоризированный URL-адрес, IP-адрес хоста заблокированного/категоризированного объекта.

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 https://support.kaspersky.ru/KSC/14.2/ru-RU/5022.htm.

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 https://support.kaspersky.com/KSC/14.2/ru-RU/5022.htm.

kaspersky

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. Эта утиита 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 integrity_checker (/Library/Application Support/Kaspersky Lab/KAV/Binaries).

Для запуска утилиты integrity_checker требуются права учетной записи пользователя Root.

Проверка целостности может быть выполнена с помощью утилиты, установленного 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 отобразить справку по настройкам утилиты, выполните следующую команду:*

```
--help
```

Результат проверки каждого файла манифеста отображается рядом с именем файла манифеста в следующем формате:

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`)

kaspersky

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 https://support.kaspersky.ru/KSC/14.2/ru-RU/5022.htm.

Также вы можете управлять работой Kaspersky Endpoint Security с помощью графического пользовательского интерфейса приложения (см. раздел "Расширенная настройка приложения" на странице 54), через Kaspersky Security Center Web Console и Cloud Console (см. раздел "Удаленное управление приложением через Kaspersky Security Center Web Console и Cloud Console" на странице 144) и из командной строки (см. раздел "Управление приложением из командной строки" на странице 158).

В этом разделе

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 (см. раздел "Установка плагина управления Kaspersky Endpoint Security" на странице 88).

   Плагин управления – специализированный компонент, предоставляющий интерфейс для управления работой приложений "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 (см. раздел "Локальная установка Агента администрирования" на странице 88)
   - Удаленно с помощью Apple Remote Desktop (см. раздел "Установка Агента администрирования с помощью Apple Remote Desktop" на странице 89)
   - Удаленно через Kaspersky Security Center (см. раздел "Установка Агента администрирования через Kaspersky Security Center" на странице 90)
   - Удаленно с помощью SSH-протокола (см. раздел "Установка Агента администрирования с использованием SSH-протокола" на странице 93)

   Для управления Kaspersky Endpoint Security для Mac 12 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 (см. раздел "Установка Kaspersky Endpoint Security" на странице 15)
   - Удаленно с помощью Apple Remote Desktop (см. раздел "Установка Kaspersky Endpoint Security" на странице 15)
   - Удаленно с помощью SSH-протокола (см. раздел "Установка приложения с использованием SSH-протокола" на странице 99)
   - Удаленно через Kaspersky Security Center (см. раздел "Установка приложения через Kaspersky Security Center" на странице 100)

   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 https://support.kaspersky.ru/KSC/14.2/ru-RU/5022.htm.

kaspersky

Обновление Kaspersky Endpoint Security 11.1 или более поздней версии до версии 12

Для управления Kaspersky Endpoint Security для Mac 12 через Kaspersky Security Center вам нужно установить Агент администрирования версии 15 на удаленные компьютеры.

Вы можете обновить Kaspersky Endpoint Security 11.1 или более поздней версии под управлением Kaspersky Security Center до версии 12 одним из следующих способов:

- Одновременно обновить и Kaspersky Endpoint Security до версии 12, 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.

При обновлении приложения до более новой версии учитывайте следующее:

- Для обновления Kaspersky Endpoint Security до версии 12 требуется macOS 12 или более поздняя версия.
- Необходимо загрузить архив KES_for_macOS11_and_later.zip с сайта Службы технической поддержки https://support.kaspersky.com/15647, чтобы применить новый конфигурационный профиль.
- После обновления Kaspersky Endpoint Security до версии 12 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, вам необходимо удалить приложение и обновить macOS до версии 12 или более поздней. Затем вы можете установить Kaspersky Endpoint Security версии 12.

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.

kaspersky

В этом разделе

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.

Установка плагина управления Kaspersky Endpoint Security начнется.

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 https://support.apple.com/ru-ru/remote-desktop.
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.

    > 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 программы 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**.

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 14**.
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 **ОК**.

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 https://support.kaspersky.ru/KSC/14.2/ru-RU/5022.htm.

► *Установка Агента администрирования с использованием SSH-протокола*

1. На рабочем месте администратора запустите SSH-клиент.
2. Соединитесь с удаленным компьютером Mac.
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/<klnagent_package_folder>
   ```

   где <klnagent_package_folder> – папка, в которой расположен инсталляционный пакет Агента администрирования.

   ```
   sudo ./install.sh --accept_eula [-r <server>] [-p <port number>] [-s
   use_ssl 0|1] [-l <SSL port number>] [-x use_proxy 0|1] [-a <proxy>]
   [-n <proxy login>] [-w <proxy password>]
   ```

   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", то 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).
   - <proxy> – IP-адрес или DNS-имя прокси-сервера.
   - <proxy_login> – имя пользователя для соединения с прокси-сервером.
   - <proxy_password> – пароль для соединения с прокси-сервером.

   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 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 **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 использованием утилиты klmover и проверить соединение удаленного компьютера с Сервером администрирования посредством утилиты klnagchk.

Вы можете удалить Агент администрирования.

В этом разделе

kaspersky

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
```

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 приложения) 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]
```

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]
```

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.

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 этом руководстве 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.

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:

```
cd /Library/Application\ Support/Kaspersky\ Lab/klnagent/Binaries/
```

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 (см. раздел "Установка и удаление приложения" на странице 15) или через Kaspersky Security Center Web Console https://support.kaspersky.ru/KSC/14.2/ru-RU/5022.htm или Kaspersky Security Center Cloud Console https://support.kaspersky.ru/KSC/CloudConsole/ru-RU/5022.htm.

В этом разделе

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 Mac.
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.

   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 (см. раздел "Создание инсталляционного пакета" на странице 103) 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 https://support.kaspersky.ru/KSC/14.2/ru-RU/5022.htm.

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**.

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 14**.
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 инсталляционного пакета (см. раздел "Создание инсталляционного пакета" на странице 103).

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.

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.

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 программы 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** снимите флажки рядом с названиями компонентов приложения, 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**.

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**.

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 14**.
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 14**.

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 (12.0)**.
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 закладку **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 (12.0)** и выполните одно из следующих действий:
    - Если вы хотите запустить программу, выберите пункт **Запустить**.
    - Если вы хотите остановить программу, выберите пункт **Остановить**.

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:

- Проверка
- Обновление
- Откат обновления
- Добавление ключа

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 https://support.kaspersky.ru/KSC/14.2/ru-RU/5022.htm.

kaspersky

В этом разделе

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 закладку **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 закладку **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 https://support.kaspersky.ru/KSC/14.2/ru-RU/5022.htm.

► *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**.

Вид кнопок может отличаться в зависимости от используемой версии Windows.

Шаг 1. Выбор программы и типа задачи

1. В окне **Выбор типа задачи** разверните узел **Kaspersky Endpoint Security для Mac (12.0)**.
2. Выберите тип задачи, которую вы хотите создать:
   - Если вы хотите создать задачу добавления ключа, выберите **Добавление ключа**.
   - Если вы хотите создать задачу отката обновления, выберите **Откат обновления**.
   - Если вы хотите создать задачу проверки, 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.

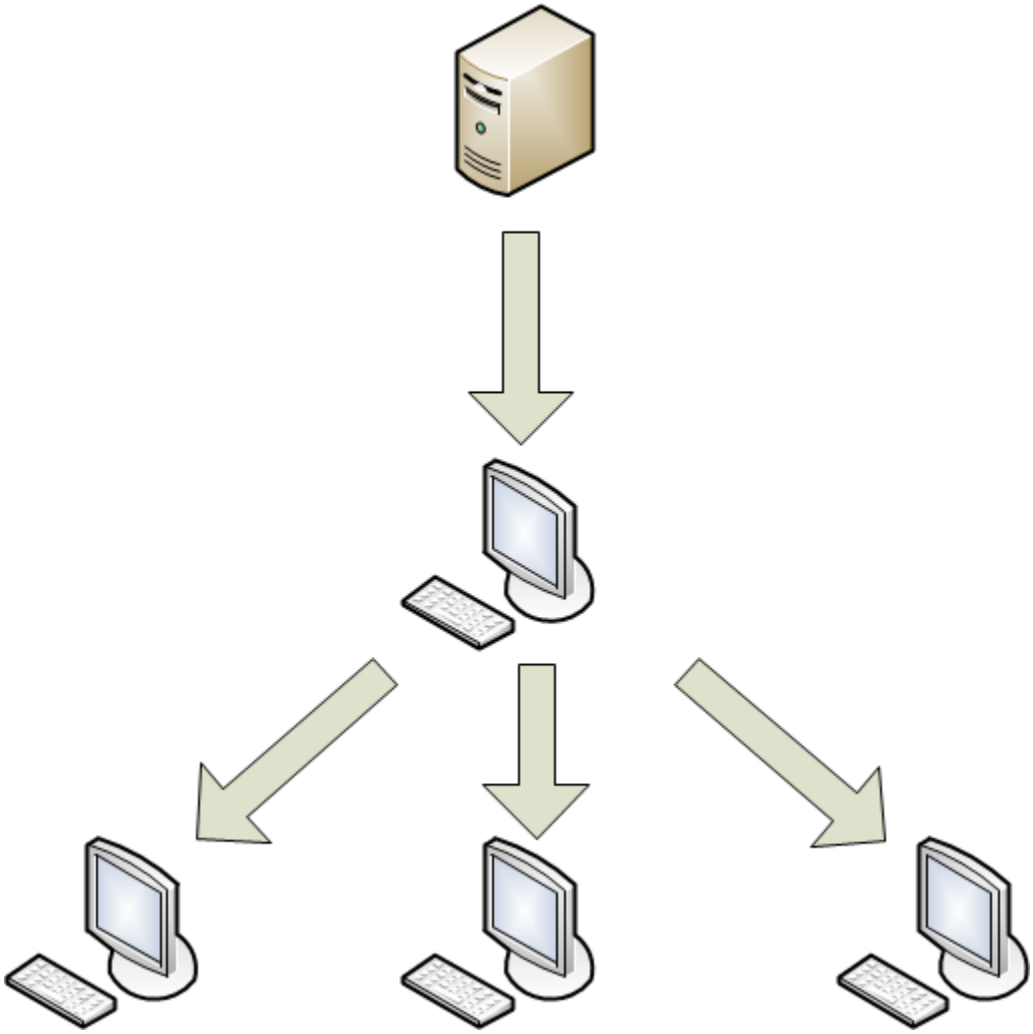
Вы можете поместить полученные обновления в локальную папку для обновления баз и модулей Kaspersky Endpoint Security на других компьютерах сети организации для уменьшения интернет-трафика.

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.

   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.



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 **OK**.

   b. Нажмите на кнопку **OK**, чтобы сохранить изменения и закрыть окно **Параметры: Обновление**.

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.

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

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

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.

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 закладку **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 закладку **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 закладку **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 закладку **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 https://support.kaspersky.ru/KSC/14.2/ru-RU/5022.htm.

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 **ОК**.
   - 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**.

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.

   > 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 **OK**, 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 закладке **Основные** в блоке **Типы файлов** выберите типы файлов, которые Kaspersky Endpoint Security проверяет при выполнении задачи проверки.

     c. На закладке **Основные** в блоке **Оптимизация** настройте параметры, которые определяют производительность проверки.

     d. На закладке **Основные** в блоке **Составные файлы** выберите, какие составные файлы Kaspersky Endpoint Security анализирует на присутствие обнаруживаемых объектов.

     e. На закладке **Дополнительно** в блоке **Дополнительные параметры** настройте использование технологии iSwift и запись информации об обнаруженных объектах в статистику программы.

f. На закладке **Дополнительно** в блоке **Эвристический анализатор** настройте использование эвристического анализатора и выберите уровень защиты, который эвристический анализатор применяет при выполнении задач проверки.

g. Нажмите на кнопку **OK**, 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 другие файлы или папки, нажмите на кнопку **Добавить** и укажите файл, папку или маску имени файла или папки.
   f. Нажмите на кнопку **OK**, 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 **OK**, 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 закладке **Основные** в блоке **Типы файлов** выберите типы файлов, которые Kaspersky Endpoint Security проверяет при открытии, исполнении и сохранении.
     b. На закладке **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 закладке **Основные** в блоке **Составные файлы** выберите, какие составные файлы нужно проверять на присутствие обнаруживаемых объектов и установите ограничение на проверку больших объектов.
     d. На закладке **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 закладке **Дополнительно** в блоке **Режим проверки** выберите режим работы защиты от файловых угроз.

f. На закладке **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 закладке **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 закладке **Основные** в блоке **Режим проверки** включите или выключите проверку веб-адресов по базе вредоносных веб-адресов.

     b. На закладке **Основные** в блоке **Параметры антифишинга** включите или выключите проверку веб-адресов по базе фишинговых веб-адресов.

     c. На закладке **Основные** в блоке **Параметры антифишинга** включите или выключите использование эвристического анализатора для обнаружения фишинговых ссылок.

d. На закладке **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 закладке **Основные** в блоке **Типы файлов** выберите типы файлов, которые Kaspersky Endpoint Security проверяет.

     b. На закладке **Основные** в блоке **Оптимизация** настройте параметры, которые определяют производительность проверки.

     c. На закладке **Основные** в блоке **Составные файлы** выберите, какие составные файлы Kaspersky Endpoint Security проверяет.

     d. На закладке **Дополнительно** в блоке **Дополнительные параметры** настройте использование технологии iSwift и запись информации об обнаруженных объектах в статистику приложения.

     e. На закладке **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: 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 закладке **Основные** в блоке **Типы файлов** выберите типы файлов, которые Kaspersky Endpoint Security проверяет.
     b. На закладке **Основные** в блоке **Оптимизация** настройте параметры, которые определяют производительность проверки.
     c. На закладке **Основные** в блоке **Составные файлы** выберите, какие составные файлы Kaspersky Endpoint Security проверяет.
     d. На закладке **Дополнительно** в блоке **Дополнительные параметры** настройте использование технологии iSwift и запись информации об обнаруженных объектах в статистику приложения.
     e. На закладке **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 **ОК**, 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 **ОК**, 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 закладке **Основные** в блоке **Типы файлов** выберите типы файлов, которые Kaspersky Endpoint Security проверяет.
     b. На закладке **Основные** в блоке **Оптимизация** настройте параметры, которые определяют производительность проверки.
     c. На закладке **Основные** в блоке **Составные файлы** выберите, какие составные файлы Kaspersky Endpoint Security проверяет.
     d. На закладке **Дополнительно** в блоке **Дополнительные параметры** настройте использование технологии iSwift и запись информации об обнаруженных объектах в статистику приложения.
     e. На закладке **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:
  - 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 программы и доступ к настройке программы, установленной на компьютерах группы администрирования. Для каждой программы требуется создать свою политику. Вы можете создать несколько различных политик для программ, установленных на компьютерах в каждой группе администрирования, но в пределах группы администрирования только одна политика может применяться единовременно к каждой программе.

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 https://support.kaspersky.ru/KSC/14.2/ru-RU/5022.htm.

В этом разделе

kaspersky

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 закладку **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**.

Вид кнопок может отличаться в зависимости от используемой версии Windows.

Шаг 1. Выбор программы

В окне **Выбор программы для создания групповой политики** в списке приложений выберите **Kaspersky Endpoint Security для Mac (12.0)**.

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.

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 **KSN** 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.

> 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 https://support.kaspersky.ru/KSC/14.2/ru-RU/5022.htm.

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.

> "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 действующей 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; 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: 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; 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 действующей 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; дата и время запуска компонента мониторинг активности; версия компонента ПО; идентификатор обновления ПО; дата и время установки ПО; тип установленного 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 проверяемых объектах и действиях: 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 и URL-адресов: 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 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.
- 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.

  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 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.

- Измените, удалите или измените порядок выполнения созданных правил.

  Порядок, в котором расположены правила, определяет приоритет их применения программой Kaspersky Endpoint Security.

Шаг 14. 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 15. 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 16. 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.

   > В группе администрирования для одной программы 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 https://support.kaspersky.ru/KSC/14.2/ru-RU/5022.htm.
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 закладке **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 программ, установленных на компьютерах в каждой группе администрирования, но в пределах группы администрирования только одна политика может применяться единовременно к каждой программе.

► *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 закладку **Политики**.

   Отобразится список политик.

Настройка параметров политики

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 (см. раздел "Настройка параметров, зависящих от задачи" на странице 115).

► *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 закладку **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 программа 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 программа выполнит при обнаружении опасного объекта веб-трафика.

     Настройте следующие параметры защита от сетевых угроз
     - Включите или выключите защиту от сетевых угроз.
     - Настройте параметры защиты сетевых угроз.
     - Укажите IP-адреса компьютеров, сетевая активность которых не будет блокироваться.

   - 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.

> 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 https://support.kaspersky.ru/KSC/14.2/ru-RU/5022.htm.

- В разделе **Контроль безопасности**

  Настройте следующие параметры Веб-Контроля

  - Включите или выключите Веб-Контроль.
  - Добавьте новое правило Веб-Контроля, нажав на кнопку **Добавить**.
  - Измените, удалите или измените порядок выполнения созданных правил.

- 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 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 **Обновление**

  Настройте следующие параметры обновления

  - Включите или выключите обновление модулей программы.
  - 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.
  - 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 программы 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.

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 закладку **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 **OK**, чтобы сохранить внесенные изменения и закрыть окно **Свойства: <Имя политики>**.

Экспорт политики в klp-файл

Вы можете экспортировать параметры политики в файл, чтобы использовать эту политику для другого Сервера администрирования.

► *Экспорт политики в klp-файл*

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 закладку **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 klp-файла

Вы можете импортировать уже существующую политику с предустановленными параметрами из файла.

► *Импорт политики из klp-файла*

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 закладку **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 закладку **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.

     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 закладку **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.

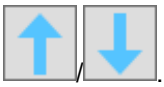
► *Изменение профиля политики*

1. В дереве консоли выберите группу администрирования, для которой вы хотите изменить профиль политики.
2. В рабочей области выберите закладку **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 закладку **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 закладку **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 https://support.kaspersky.ru/KSC/14.2/ru-RU/5022.htm.

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 закладку **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 https://support.kaspersky.ru/KSC/14.2/ru-RU/5022.htm.

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.

kaspersky

Удаленное управление приложением через Kaspersky Security Center Web Console и Cloud Console

В сертифицированной конфигурации управление приложением через Kaspersky Security Center Cloud Console недоступно.

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 https://support.kaspersky.ru/KSC/14.2/ru-RU/5022.htm.

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 https://support.kaspersky.ru/KSC/CloudConsole/ru-RU/5022.htm.

Также вы можете управлять Kaspersky Endpoint Security с помощью графического пользовательского интерфейса приложения (см. раздел "Расширенная настройка приложения" на странице 54), Консоли администрирования Kaspersky Security Center (см. раздел "Управление приложением через Консоль администрирования Kaspersky Security Center" на странице 85) и из командной строки (см. раздел "Управление приложением из командной строки" на странице 158).

В этом разделе

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 программы и доступ к настройке программы, установленной на компьютерах группы администрирования. Для каждой программы требуется создать свою политику. Вы можете создать несколько различных политик для программ, установленных на компьютерах в каждой группе администрирования, но в пределах группы администрирования только одна политика может применяться единовременно к каждой программе.

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 программу, для которой вы хотите создать политику, и нажмите на кнопку **Далее**.

   Откроется окно **Новая политика**.
4. На закладке **Общие** укажите имя политики, выберите состояние политики и настройте опции наследования параметров политики.
5. На закладке **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 https://support.kaspersky.ru/KSC/14.2/ru-RU/5022.htm.

Подробную информацию о политиках Kaspersky Security Center Cloud Console вы можете найти в справке Kaspersky Security Center Cloud Console https://support.kaspersky.ru/KSC/CloudConsole/ru-RU/5022.htm.

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.

kaspersky

В этом разделе

Настройка параметров продвинутой защиты

В разделе **Продвинутая защита** вы можете выбрать, участвует ли Kaspersky Endpoint Security на клиентских компьютерах в Kaspersky Security Network 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**.

  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 https://support.kaspersky.ru/KSC/14.2/ru-RU/5022.htm.

- 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.

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 https://support.kaspersky.ru/KSC/14.2/ru-RU/5022.htm.
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.

"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 действующей 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; 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: 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; 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 действующей 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; дата и время запуска компонента мониторинг активности; версия компонента ПО; идентификатор обновления ПО; дата и время установки ПО; тип установленного 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 проверяемых объектах и действиях: 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 и URL-адресов: 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 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".

kaspersky

Настройка параметров базовой защиты

Если требуется, в разделе **Базовая защита** вы можете настроить параметры работы следующих компонентов:

- Защита от файловых угроз (см. раздел "Настройка параметров защиты от файловых угроз" на странице 151)
- Защита от веб-угроз (см. раздел "Настройка параметров защиты от веб-угроз" на странице 151)
- Защита от сетевых угроз (см. раздел "Настройка параметров защиты от сетевых угроз" на странице 151)

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 программа 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.

  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 программа 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.

  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.
- Измените, удалите или измените порядок выполнения созданных правил.

  Порядок, в котором расположены правила, определяет приоритет их применения программой 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 (см. раздел "Настройка параметров Managed Detection and Response" на странице 153)
- Endpoint Detection and Response (KATA) (см. раздел "Настройка параметров Managed Detection and Response (KATA)" на странице 153)

Вы можете открыть окно настройки параметров работы компонента, нажав на соответствующую ссылку.

kaspersky

Настройка параметров Managed Detection and Response

Включение компонента Managed Detection and Response ведет к выводу программного изделия из сертифицированной конфигурации.

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 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 программы.
- Добавьте или удалите источники обновлений, которые Kaspersky Endpoint Security будет использовать.

kaspersky

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.
- 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 элемент **Kaspersky Endpoint Security для Mac (12.0)**.
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**.

> 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 https://support.kaspersky.ru/KSC/14.2/ru-RU/5022.htm.

Подробную информацию о задачах Kaspersky Security Center Cloud Console вы можете найти в справке Kaspersky Security Center Cloud Console https://support.kaspersky.ru/KSC/CloudConsole/ru-RU/5022.htm.

В этом разделе

Настройка параметров задачи Проверка

На закладке **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 закладку **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.

Настройка параметров задачи Добавление ключа

На закладке **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 закладку **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 закладке **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 закладку **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 https://support.kaspersky.ru/KSC/14.2/ru-RU/5022.htm.

Если необходимо, выполните следующие действия:

- Включите или выключите обновление модулей программы.
- 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 **OK**.
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.

kaspersky

Управление приложением из командной строки

Вы можете работать с приложением Kaspersky Endpoint Security посредством командной строки.

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.

В этом разделе

Просмотр справки командной строки

Чтобы просмотреть информацию по синтаксису командной строки, используйте следующую команду:

```
kav -? | help
```

kaspersky

Запуск задач поиска вредоносного ПО

Синтаксис команды:

```
kav scan <область проверки> <действие> <типы файлов> <исключения>
<параметры отчета> <дополнительные параметры>
```

Чтобы запустить задачу поиска вредоносного ПО, вы также можете использовать задачи, созданные в приложении, запуская их из командной строки (см. раздел "Запуск и остановка компонента или задачи" на странице 162). 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.

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.

  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 приложения.

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
```

kaspersky

Откат последнего обновления

Синтаксис команды:

```
kav rollback <параметры отчета>
```

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>
```

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.

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.

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

`<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.

Если вы запускаете команду status без параметра <название компонента или задачи>, то выводится статус всех задач и компонентов приложения. 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

<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.

<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
```

kaspersky

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
```

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
```

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
```

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
```

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
```

Для удаления приложения требуются права администратора.

Обновление баз вредоносного ПО в ручном режиме

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

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

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

kaspersky

Устранение уязвимостей и установка критических обновлений в приложении

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

Порядок получения критических обновлений изложен в формуляре.

Лицо, ответственное за эксплуатацию программы, должно периодически (не реже одного раза в три месяца) проверять отсутствие обнаруженных уязвимостей в программе, используя веб-сайт "Лаборатории Касперского" (https://support.kaspersky.ru/vulnerability), банк данных угроз безопасности информации ФСТЭК России (http://www.bdu.fstec.ru) и иные общедоступные источники.

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

Через веб-форму на веб-сайте Службы технической поддержки (https://support.kaspersky.ru/vulnerability.aspx?el=12429).

По адресу электронной почты vulnerability@kaspersky.com.

В сообществе пользователей "Лаборатории Касперского".

Действия после сбоя или неустранимой ошибки в работе приложения

Приложение автоматически восстанавливает свою работу после сбоев, участие пользователя не требуется. В случае, когда приложение не может восстановить свою работу, вам требуется переустановить программу или ее компонент. Вы также можете обратиться за помощью в Службу технической поддержки (см. стр. 171).

kaspersky

Обращение в Службу технической поддержки

В этом разделе описывается, как получить техническую поддержку и на каких условиях она доступна.

В этом разделе

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.

«Лаборатория Касперского» предоставляет поддержку Kaspersky Endpoint Security в течение всего жизненного цикла приложения (см. страницу жизненного цикла приложений (https://support.kaspersky.com/corporate/lifecycle)). Перед обращением в Службу технической поддержки ознакомьтесь с правилами предоставления технической поддержки (https://support.kaspersky.ru/support/rules#ru_ru).

Вы можете связаться со специалистами Службы технической поддержки одним из следующих способов:

- посетить сайт Службы технической поддержки (https://support.kaspersky.ru/b2b/ru);
- отправить запрос в Службу технической поддержки "Лаборатории Касперского" с портала Kaspersky CompanyAccount (https://companyaccount.kaspersky.com).

Техническая поддержка через Kaspersky CompanyAccount

Kaspersky CompanyAccount (https://companyaccount.kaspersky.com) – 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 (https://support.kaspersky.ru/faq/companyaccount_help).

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 в контекстном меню значка приложения пункт **Настройки**.

   Откроется окно настройки приложения.

2. На закладке **Интерфейс** в блоке **Трассировка** установите флажок **Включить трассировку**.

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 в контекстном меню значка приложения пункт **Настройки**.

   Откроется окно настройки приложения.

2. На закладке **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 программы и ее модулей;
- информацию о подписке (тип подписки, регион);
- информацию о языке интерфейса, идентификатор программы, кастомизацию программы, версию программы, уникальный идентификатор установки программы, 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 программ (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.

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

kaspersky

Приложения

Этот раздел содержит информацию, которая дополняет основной текст документа.

В этом разделе

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.apple.WebKit.Networking.xpc/Contents/MacOS/com.apple.WebKit.Networking`
    - `/System/Library/Frameworks/WebKit.framework/Versions/A/XPCServices/com.apple.WebKit.WebContent.xpc/Contents/MacOS/com.apple.WebKit.WebContent`
    - `/System/Library/PrivateFrameworks/SafariShared.framework/Versions/A/XPCServices/com.apple.Safari.SearchHelper.xpc/Contents/MacOS/com.apple.Safari.SearchHelper`
    - `/System/Library/Frameworks/webkit2.framework/versions/a/xpcservices/com.apple.webkit.networking.xpc/contents/macos/com.apple.webkit.networking`

- 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.
- Приложения, которым требуется Rosetta®, могут быть не установлены, если запущен Kaspersky Endpoint Security. Чтобы решить проблему, завершите работу Kaspersky Endpoint Security и попробуйте переустановить приложение.

Список объектов, проверяемых по расширению

Если при создании задачи поиска вредоносного ПО 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.

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.

Сертифицированное состояние программы: параметры и их значения

Этот раздел содержит перечень параметров программы, влияющих на безопасное состояние программы, и безопасные значения (диапазоны значений) параметров в сертифицированной конфигурации.

Изменение каких-либо из перечисленных параметров с их значений (диапазона значений) в сертифицированной конфигурации на другие значения выводит программу из безопасного состояния.

Таблица 1. Параметры и их безопасные значения для программы в сертифицированной конфигурации в локальном интерфейсе программы

Параметр	Краткое описание и диапазон значений	Значение параметра для программы в сертифицированном состоянии
Включить защиту	Настройки защиты. Общие.	***Флажок установлен.***
Обнаруживаемые объекты: **Вирусы, черви, троянские программы, вредоносные утилиты, рекламные программы и программы автодозвона**	Настройки защиты. Общие.	***Флажок установлен.***
Доверенная зона	Настройки защиты. Общие.	***Объекты не добавлены.*** Добавление некоторых объектов может вести к выходу из безопасного состояния. Для минимизации риска рекомендуется оставить значение по умолчанию.
Включить защиту от файловых угроз	Настройки защиты. Защита от файловых угроз.	***Флажок установлен.***
Действие приобнаружении угрозы	Настройки защиты. Защита от файловых угроз.	***Запрашивать действие***
Область защиты	Настройки защиты. Защита от файловых угроз.	***Все съемные диски, Все внутренние диски, Все сетевые диски.***
Включить защиту от веб-угроз	Настройки защиты. Защита от веб-угроз.	***Флажок установлен.***
Действие приобнаружении угрозы	Настройки защиты. Защита от веб-угроз.	***Запрашивать действие***
Проверять защищенные соединения (HTTPS)	Настройки защиты. Общие.	***Флажок установлен.***
Включить защиту от сетевых угроз	Настройки защиты. Защита от сетевых угроз.	***Флажок установлен.***
Доверенные компьютеры	Настройки защиты. Защита от сетевых угроз.	***Пустой список IP-адресов.*** Добавление некоторых исключений может вести к выходу из безопасного состояния. Для минимизации риска рекомендуется оставить значения по умолчанию.

Параметр	Краткое описание и диапазон значений	Значение параметра для программы в сертифицированном состоянии
Загружать обновления автоматически	Настройки обновления.	***Флажок установлен.***
Уведомлять о событиях	Настройки уведомлений.	***Флажок установлен.***
Воспроизводить звуковое уведомление при обнаружении вредоносных программ	Настройки уведомлений.	***Флажок установлен.***
Участвовать в Kaspersky Security Network	KSN.	***Флажок снят.*** Допускается включить переключатель только при использовании Локального KSN (Kaspersky Private Security Network – KPSN).

Таблица 2. Параметры и их безопасные значения для программы в сертифицированной конфигурации в интерфейсе Kaspersky Security Center

Параметр	Краткое описание и диапазон значений	Значение параметра для программы в сертифицированном состоянии
Включить защиту	Настройки защиты. Общие.	***Флажок установлен.***
Запускать приложение при включении компьютера	Настройки защиты. Общие.	***Флажок установлен.***
Обнаруживаемые объекты: **Вирусы, черви, троянские программы, вредоносные утилиты, рекламные программы и программы автодозвона**	Настройки защиты. Общие.	***Флажок установлен.***
Не запускать задачи по расписанию при работе от аккумулятора	Настройки защиты. Общие.	***Флажок снят.***
Доверенная зона	Настройки защиты. Общие.	***Объекты не добавлены.*** Добавление некоторых объектов может вести к выходу из безопасного состояния. Для минимизации риска рекомендуется оставить значение по умолчанию.
Включить защиту от файловых угроз	Настройки защиты. Защита от файловых угроз.	***Флажок установлен.***

Параметр	Краткое описание и диапазон значений	Значение параметра для программы в сертифицированном состоянии
Если обнаружен вредоносный объект	Настройки защиты. Защита от файловых угроз.	***Запрашивать действие***
Уровень безопасности	Настройки защиты. Защита от файловых угроз.	***Максимальная защита*** или ***Рекомендованный***.
Область защиты	Настройки защиты. Защита от файловых угроз.	***Все съемные диски, Все внутренние диски, Все сетевые диски.***
Включить защиту от веб-угроз	Настройки защиты. Защита от веб-угроз.	***Флажок установлен.***
Если обнаружен вредоносный объект	Настройки защиты. Защита от веб-угроз.	***Запрашивать действие***
Уровень безопасности	Настройки защиты. Защита от веб-угроз.	***Максимальная защита*** или ***Рекомендованный***.
Проверять защищенные соединения (HTTPS)	Настройки защиты. Защита от веб-угроз.	***Флажок установлен.***
Включить защиту от сетевых угроз	Настройки защиты. Защита от сетевых угроз.	***Флажок установлен.***
Блокировать атакующие компьютеры на N минут	Настройки защиты. Защита от сетевых угроз.	***Флажок установлен.*** ***Время блокирования – 60 мин.***
Исключения	Настройки защиты. Защита от сетевых угроз.	***Пустой список IP-адресов.*** Добавление некоторых исключений может вести к выходу из безопасного состояния. Для минимизации риска рекомендуется оставить значения по умолчанию.
Пропускать, если проверка длится более 30 сек.	Настройки проверок.	***Флажок снят.***
Пропускать, если размер файла больше 100 МБ	Настройки проверок.	***Флажок снят.***
Типы файлов: **Проверять все файлы**	Настройки проверок.	***Флажок установлен.***
Проверять архивы	Настройки проверок.	***Флажок установлен.***
Проверять вложенные OLE-объекты	Настройки проверок.	***Флажок установлен.***

Параметр	Краткое описание и диапазон значений	Значение параметра для программы в сертифицированном состоянии
Проверять файлы почтовых форматов	Настройки проверок.	***Флажок установлен.***
Использовать эвристический анализатор	Настройки проверок.	***Флажок установлен.***
Обновлять модули приложения	Настройки обновления.	***Флажок снят.***
Уведомления о событиях: Показывать уведомления	Настройки уведомлений.	***Флажок установлен.***
Я принимаю условия использования Kaspersky Security Network	KSN.	***Флажок снят.*** Допускается включить переключатель только при использовании Локального KSN (Kaspersky Private Security Network – KPSN).

kaspersky

Информация о стороннем коде

Информация о стороннем коде содержится в файле legal_notices.txt, расположенном в папке установки программы.

kaspersky

Уведомления о товарных знаках

Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.

App Store, Apple, Apple Remote Desktop, FileVault, Mac, Mac Pro, macOS, Rosetta, Safari и Xcode – товарные знаки Apple Inc.

IOS является зарегистрированным товарным знаком или товарным знаком Cisco Systems, Inc. и/или ее аффилированных компаний в США и в определенных других странах.

Android, Chrome, Chromium, Google и Google Chrome – товарные знаки Google LLC.

Intel – товарный знак Intel Corporation, зарегистрированный в Соединенных Штатах Америки и в других странах.

Linux – товарный знак Linus Torvalds, зарегистрированный в США и в других странах.

Excel, IIS, Internet Explorer, Microsoft, Microsoft Edge, Windows, Windows Installer, Windows Phone и WMI являются товарными знаками группы компаний Microsoft.

Firefox и Mozilla являются товарными знаками Mozilla Foundation в США и других странах.

Java и JavaScript – зарегистрированные товарные знаки компании Oracle и/или ее аффилированных компаний.

Parallels, логотип Parallels и Coherence являются товарными знаками или зарегистрированными товарными знаками Parallels International GmbH.

VMware и VMware Fusion – товарные знаки VMware, Inc. или зарегистрированные в США или других юрисдикциях товарные знаки VMware, Inc.

JAMF и Composer являются зарегистрированными или охраняемыми нормами общего права товарными знаками компании JAMF SOFTWARE, LLC в США и других странах.