kaspersky

Kaspersky Endpoint Security для Android

Руководство по эксплуатации

Версия программы: 10

Уважаемый пользователь!

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

Дата редакции документа: 01.03.2024

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

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

Содержание

Kaspersky Endpoint Security для Android

Комплект поставки

Файл приложения Kaspersky Endpoint Security для Android

`kesandroid10<version><languages>.apk` – пакетный файл Android для приложения Kaspersky Endpoint Security для Android.

Комплект документации

- Руководство «Kaspersky Endpoint Security для Android».

О приложении Kaspersky Endpoint Security для Android

Kaspersky Endpoint Security для Android защищает мобильные устройства от веб-угроз, вирусов и других программ, представляющих угрозы.

Для активации всех функций приложения необходимо подключение к KSC.

Kaspersky Endpoint Security для Android включает следующие компоненты:

- **Защита от вредоносного ПО**. Позволяет обнаруживать и устранять угрозы на мобильном устройстве, используя базы вредоносного ПО приложения и дополнительно облачную службу Kaspersky Security Network. В состав Защиты от вредоносного ПО входят следующие компоненты:
- **Защита**. Позволяет обнаруживать угрозы в открытых файлах, а также проверять новые приложения и предотвращать заражение устройства в режиме реального времени.
- **Проверка**. Запускается по требованию для всей файловой системы, только для установленных приложений, выбранного файла или папки.
- **Обновление**. Позволяет загружать новые базы вредоносного ПО приложения.
- **Анти-Вор.** Защищает информацию на устройстве от несанкционированного доступа в случае потери или кражи устройства. Позволяет отправлять на устройство следующие команды:
- **Поиск**, чтобы получить координаты местоположения устройства.
- **Сигнал**, чтобы устройство издало громкий сигнал тревоги.

- **Фото**, чтобы устройство сделало фотоснимки на фронтальную камеру, если кто-то попытается его разблокировать.

- **Удаление корпоративных данных**, чтобы защитить конфиденциальную информацию компании.

- **Веб-Фильтр.** Позволяет блокировать вредоносные веб-сайты, цель которых – распространить вредоносный код. Веб-Фильтр также блокирует поддельные (фишинговые) веб-сайты, цель которых – украсть конфиденциальные данные пользователя (например, пароли от интернет-банка или платежных систем) и получить доступ к его финансовым счетам. Веб-Фильтр проверяет веб-сайты до открытия, используя облачную службу Kaspersky Security Network. По результатам проверки Веб-Фильтр разрешает загрузку веб-сайтов, признанных надежными, и блокирует веб-сайты, признанные вредоносными. Веб-Фильтр также поддерживает фильтрацию веб-сайтов по категориям, определенным в облачной службе Kaspersky Security Network. Это позволяет администратору ограничить доступ пользователей к некоторым категориям веб-страниц (например, к веб-страницам из категории "Азартные игры, лотереи, тотализаторы" или "Общение в сети").

- **Контроль приложений.** Позволяет вам устанавливать на устройство рекомендованные и обязательные приложения с помощью прямой ссылки на дистрибутив или ссылки на Google Play. С помощью Контроля приложений вы можете удалять запрещенные приложения, которые не удовлетворяют требованиям корпоративной безопасности.

- **Контроль соответствия.** Позволяет проверять управляемые устройства на соответствие требованиям корпоративной безопасности и накладывать ограничения на определенные функции несовместимых устройств.

  Приложение Kaspersky Endpoint Security для Android также можно установить в режиме device owner. Режим device owner обеспечивает полный контроль над корпоративными Android-устройствами и позволяет вам настроить множество функций устройства. В режиме device owner вы можете:

- Ограничить функции операционной системы Android.

- Задать настройки Google Chrome.

- Задать настройки запуска приложений в Контроле приложений.

- Ограничить набор приложений, доступных пользователю устройства в режиме киоска.

- Задать настройки Exchange ActiveSync для Gmail.

- Настроить подключение к NDES/SCEP-серверу.

- Установить корневые сертификаты на устройствах.

Аппаратные и программные требования к мобильному устройству пользователя для установки Kaspersky Endpoint Security для Android

Kaspersky Endpoint Security для Android имеет следующие аппаратные и программные требования:

- смартфон или планшет с разрешением экрана от 320x480 пикселей;
- 65 МБ свободного места в основной памяти устройства;
- Android 5.0 или выше (включая Android 12L, исключая Go Edition);
- архитектура процессора x86, x86-64, Arm5, Arm6, Arm7, Arm8.

Приложение устанавливается только в основную память устройства.

Известные проблемы и рекомендации

Следующие известные проблемы не являются критичными для работы решения.

Известные проблемы при установке программы

- Kaspersky Endpoint Security для Android устанавливается только в основную память устройства.
- На устройствах под управлением Android 7.0 при попытке выключить права администратора для Kaspersky Endpoint Security для Android в настройках устройства может произойти сбой, если для Kaspersky Endpoint Security для Android запрещено наложение поверх других окон. Проблема связана с известным дефектом в Android 7.
- Приложение Kaspersky Endpoint Security для Android на устройствах под управлением Android 7.0 и выше не поддерживает многооконный режим.
- Kaspersky Endpoint Security для Android не работает на Chromebook-устройствах под управлением операционной системы Chrome.
- Kaspersky Endpoint Security для Android не работает на устройствах с операционной системой Android версии Go Edition.
- При использовании приложения Kaspersky Endpoint Security для Android со сторонними EMM-системами (например, VMWare AirWatch) доступны только компоненты Защита от вредоносного ПО и Веб-Фильтр. Администратор может

настраивать параметры Защиты от вредоносного ПО и Веб-Фильтра в консоли EMM-системы. При этом уведомления о работе приложения доступны только в интерфейсе приложения Kaspersky Endpoint Security для Android (Отчеты).

Известные проблемы при обновлении версии приложения

- Вы можете обновить Kaspersky Endpoint Security для Android только до более новой версии приложения. Обновить Kaspersky Endpoint Security для Android до более старой версии невозможно.

- Для обновления Kaspersky Endpoint Security для Android с помощью автономного пакета установки на мобильном устройстве пользователя должна быть разрешена установка приложений из неизвестных источников.

- Обновление с помощью Google Play доступно, если Kaspersky Endpoint Security для Android установлен из Google Play. Если приложение установлено другим способом, обновление с помощью Google Play невозможно.

Известные проблемы в работе Защиты от вредоносного ПО

- Из-за технических ограничений Kaspersky Endpoint Security для Android не может проверять файлы размером 2 ГБ и более. Во время проверки приложение пропускает такие файлы и не уведомляет вас, если такие файлы были пропущены.

- Для дополнительной проверки устройства на новые угрозы, информация о которых еще не вошла в базы вредоносного ПО, требуется включить использование Kaspersky Security Network. *Kaspersky Security Network (KSN)* – инфраструктура облачных служб, предоставляющая доступ к оперативной базе знаний "Лаборатории Касперского" о репутации файлов, веб-ресурсов и программного обеспечения. Для использования KSN требуется подключение мобильного устройства к интернету.

- Иногда обновление баз вредоносного ПО с Сервера администрирования может завершиться ошибкой на мобильных устройствах. В этом случае запустите задачу обновления баз вредоносного ПО на Сервере администрирования.

- На некоторых устройствах Kaspersky Endpoint Security для Android не обнаруживает устройства, подключенные по USB OTG. Выполнить поиск вредоносного ПО на таких устройствах невозможно.

- На устройствах с операционной системой Android 11 или выше приложение Kaspersky Endpoint Security для Android не может сканировать папки Android/data и Android/obb и обнаруживать в них вредоносные программы из-за технических ограничений.

- На устройствах с операционной системой Android 11 и выше пользователю необходимо предоставить разрешение "Разрешить доступ на управление всеми файлами".

- На устройствах под управлением Android 7 и выше может некорректно отображаться окно настройки расписания запуска поиска вредоносного ПО (не отображаются элементы управления). Проблема связана с известным дефектом в Android 7.

- На устройствах под управлением Android 7.0 при выполнении задачи постоянной защиты в расширенном режиме не выполняется обнаружение угроз в файлах, хранящихся на внешней SD-карте.

- На устройствах под управлением Android 6 Kaspersky Endpoint Security для Android не обнаруживает загрузку вредоносного файла в память устройства. Вредоносный файл может быть обнаружен Защитой от вредоносного ПО при запуске файла или во время поиска вредоносного ПО на устройстве. Проблема связана с известным дефектом в Android 6. Для обеспечения безопасности устройства рекомендуется настроить запуск поиска вредоносного ПО по расписанию.

Известные проблемы в работе Веб-Фильтра

- Веб-Фильтр на Android-устройствах поддерживается только браузерами Google Chrome, HUAWEI Browser, Samsung Internet Browser и Яндекс Браузер.

- Функция Custom Tabs поддерживается браузерами Google Chrome, HUAWEI Browser и Samsung Internet Browser.

- В браузерах HUAWEI Browser, Samsung Internet Browser и Яндекс Браузер Веб-Фильтр не блокирует сайты на мобильном устройстве, если используется рабочий профиль и установлен флажок Включить Веб-Фильтр только в рабочем профиле.

- Kaspersky Endpoint Security в рабочем профиле проверяет только домен веб-сайта в HTTPS-трафике. Вредоносные и фишинговые веб-сайты могут оставаться разблокированными, если приложение установлено в рабочем профиле. Если домен является доверенным, Веб-Фильтр может пропустить угрозу (например, `https://trusted.domain.com/phishing/`). Если домен не является доверенным, Веб-Фильтр блокирует вредоносные и фишинговые веб-сайты.

- Для работы Веб-Фильтра требуется включить использование Kaspersky Security Network. Веб-Фильтр блокирует веб-сайты на основе данных о репутации и категории веб-сайтов, которые содержатся в KSN.

- На устройствах под управлением Android 6 с установленным браузером Google Chrome версии 51 или более ранних версий запрещенные веб-сайты могут не блокироваться Веб-Фильтром, если веб-сайт открыт следующими способами (проблема связана с известным дефектом в Google Chrome):

- из результатов поискового запроса;

- из списка закладок;
- из истории поисковых запросов;
- при использовании функции автозаполнения веб-адреса;
- при открытии веб-сайта на новой вкладке в Google Chrome.
- Запрещенные веб-сайты могут не блокироваться в браузере Google Chrome версии 50 или более ранних версий, если веб-сайт открыт из результатов поискового запроса Google и в настройках браузера включена функция **Объединить вкладки и приложения**. Проблема связана с известным дефектом в Google Chrome.
- Веб-сайты из запрещенных категорий могут не блокироваться в Google Chrome, если пользователь открывает их из сторонних приложений, например, из приложения IM-клиента. Проблема связана с особенностями работы службы Специальных возможностей с функцией Chrome Custom Tabs.
- Запрещенные веб-сайты могут не блокироваться в Samsung Internet Browser, если пользователь открывает их в фоновом режиме из контекстного меню или из сторонних приложений, например, из приложения IM-клиента.
- Для работы Веб-Фильтра Kaspersky Endpoint Security для Android должен быть установлен в качестве службы Специальных возможностей.
- На некоторых устройствах Xiaomi для работы Веб-Фильтра должны быть предоставлены разрешения "Отображать всплывающее окно" и "Отображать всплывающие окна во время работы в фоновом режиме".
- При вводе адреса веб-сайта в параметрах Веб-Фильтра соблюдайте следующие правила:
- Для Android-устройств указывайте адрес в формате регулярных выражений (например, `https://example.com.*`);
- Разрешенные веб-сайты могут блокироваться в Samsung Internet Browser в режиме Веб-Фильтра **Разрешить только перечисленные веб-сайты** при обновлении страницы. Веб-сайты блокируются, если регулярное выражение содержит дополнительные параметры (например, `^https?://example.com/pictures/`). Рекомендуется использовать регулярные выражения без дополнительных параметров (например, `^https?://example.com`).
- Если для Веб-Фильтра выбран режим **Запрещены все веб-сайты**, то Kaspersky Endpoint Security для Android не блокирует поиск в виджете Google Поиск. Вместо этого блокируется доступ к результатам поиска.
- Если в рабочем профиле для Веб-Фильтра выбран режим **Запрещены все веб-сайты**, то Kaspersky Endpoint Security для Android постоянно перезагружает

главную страницу Google Chrome, блокирует браузер и мешает работе устройства.

- Чтобы гарантировать, что приложение Kaspersky Endpoint Security для Android разрешает или ограничивает доступ к веб-сайту во всех поддерживаемых версиях Google Chrome, HUAWEI Browser, Samsung Internet Browser и Yandex Browser, добавьте один и тот же URL дважды: один раз – с указанием протокола HTTP (например, https://example.com), а другой раз – с указанием протокола HTTPS (например, https://example.com). В качестве альтернативы вы можете использовать регулярные выражения.

- В Яндекс Браузере и Samsung Internet Browser вредоносные и фишинговые сайты могут оставаться незаблокированными. Это связано с тем, что проверяется только домен веб-сайта, и, если он является доверенным, Веб-Фильтр может пропустить угрозу.

- Если Kaspersky Endpoint Security для Android не установлен в качестве службы Специальных возможностей, то Веб-Фильтр может блокировать разрешенный сайт при подгрузке на него элементов с сайта, домен которого не добавлен в список разрешенных.

Известные проблемы в работе Анти-Вора

- Для своевременной доставки команд на Android-устройства приложение использует сервис Firebase Cloud Messaging (FCM). Если FCM не настроен, команды будут доставлены на устройство только при синхронизации с Kaspersky Security Center по расписанию, заданному в политике, например, каждые 24 часа.

- Для блокирования устройства Kaspersky Endpoint Security для Android должен быть установлен в качестве администратора устройства.

- На устройствах под управлением операционной системы Android версии 7.0 и выше для блокирования устройства Kaspersky Endpoint Security для Android должен быть установлен в качестве службы Специальных возможностей.

- На некоторых устройствах команды Анти-Вора не могут быть выполнены, если на устройстве включен режим энергосбережения. Этот дефект подтвержден на Alcatel 5080X.

- Чтобы определить местоположение устройства с операционной системой Android 10 и выше, необходимо предоставить разрешение "Всегда" для доступа к местоположению устройства.

- Чтобы выполнить снимок с помощью устройства с операционной системой Android 11 и выше, необходимо предоставить разрешение "При использовании приложения" для доступа к камере.

Известные проблемы в работе Контроля приложений

- Для работы Контроля приложений Kaspersky Endpoint Security для Android должен быть установлен в качестве службы Специальных возможностей. Не применимо к режиму device owner.

- Для работы Контроля приложений (категории приложений) требуется включить использование Kaspersky Security Network. Контроль приложений определяет категорию приложения на основе данных, которые содержатся в KSN. Для использования KSN требуется подключение мобильного устройства к интернету. Для работы Контроля приложений вы можете добавить отдельные приложения в списки запрещенных и разрешенных приложений. В этом случае KSN не требуется.

- При настройке Контроля приложений рекомендуется снять флажок **Блокировать системные приложения**. Блокировка системных приложений может привести к сбоям в работе устройства.

- На некоторых личных устройствах HUAWEI и Honor приложения из разрешенных категорий могут быть заблокированы, а приложения из запрещенных категорий могут оставаться разблокированными. Это связано с тем, что категория для некоторых приложений из AppGallery не может быть определена правильно.

- На некоторых устройствах Samsung и Oppo после снятия флажка **Блокировать системные приложения** значки приложений могут остаться скрытыми на рабочем столе. Это связано с особенностями операционной системы Android.

Известные проблемы при настройке электронной почты

- Дистанционная настройка почтового ящика доступна только на следующих устройствах:

- Samsung-устройства (Exchange ActiveSync);

- Android-устройства с установленным почтовым клиентом TouchDown.

Известные проблемы при настройке надежности пароля разблокировки устройства

- На устройствах под управлением Android 10 и выше Kaspersky Endpoint Security приводит требования надежности пароля к одному из системных значений: средний или высокий.

  Если требуемая длина пароля составляет от 1 до 4 символов, приложение предлагает пользователю установить пароль средней надежности. Он должен быть либо цифровым (PIN-код) без повторяющихся или упорядоченных последовательностей (например, 1234), либо буквенно-цифровым. PIN-код или пароль должны состоять не менее чем из 4 символов.

  Если требуемая длина пароля составляет не менее 5 символов, приложение предлагает пользователю установить пароль высокой надежности. Он должен

быть либо цифровым (PIN-код) без повторяющихся или упорядоченных последовательностей, либо буквенно-цифровым (пароль). PIN-код должен состоять не менее чем из 8 цифр; пароль должен состоять не менее чем из 6 символов.

- На устройствах под управлением Android 10 и выше управлять использованием отпечатка пальца для разблокировки экрана можно только в рабочем профиле.

- На устройствах под управлением Android 7.1.1 при несоответствии пароля разблокировки требованиям корпоративной безопасности (Контроль соответствия) системное приложение Настройки может работать некорректно при попытке изменить пароль разблокировки из Kaspersky Endpoint Security для Android. Проблема связана с известным дефектом в Android 7.1.1. Для изменения пароля разблокировки в этом случае используйте только системное приложение Настройки.

- На некоторых устройствах под управлением Android 6 и выше может произойти сбой при вводе пароля разблокировки экрана, если данные на устройстве зашифрованы. Проблема связана с особенностями работы Службы специальных возможностей на устройствах с прошивкой MIUI.

- На некоторых устройствах HUAWEI появляется уведомление о слишком простом методе разблокировки устройства. В этом случае пользователь должен установить PIN-код, соответствующий требованиям политики. Дополнительные сведения о настройке правильного PIN-кода на устройствах HUAWEI смотрите в разделе Настройка надежного пароля разблокировки для устройства Android.

Известные проблемы при настройке Wi-Fi

- На устройствах с операционной системой Android версии 8.0 или выше настроить параметры прокси-сервера для сети Wi-Fi с помощью политики невозможно. Вы можете настроить параметры прокси-сервера для сети Wi-Fi на мобильном устройстве вручную.

Известные проблемы при работе с сетевым экраном

- Использование сетевого экрана доступно только на Samsung-устройствах.

Известные проблемы при настройке VPN

- Дистанционная настройка VPN доступна только на следующих устройствах:

- Samsung-устройства.

- При настройке VPN-соединения для избранных доменов в Safari, если изменить значение опции **Подключаться автоматически**, изменения не будут применены на устройстве. По умолчанию флажок **Подключаться автоматически**

установлен, и его не рекомендуется снимать, если вы хотите автоматически включать VPN для указанных доменов.

Известные проблемы, связанные с защитой от удаления приложения

- Kaspersky Endpoint Security для Android должен быть установлен в качестве администратора устройства.
- На устройствах под управлением операционной системы Android версии 7.0 и выше для защиты приложения от удаления Kaspersky Endpoint Security для Android должен быть установлен в качестве службы Специальных возможностей.
- На некоторых устройствах Xiaomi и HUAWEI защита Kaspersky Endpoint Security для Android от удаления не работает. Проблема связана с особенностями прошивки MIUI 7 и 8 на Xiaomi и прошивки EMUI на HUAWEI.

Известные проблемы при настройке ограничений устройства

- На устройствах под управлением Android 10 и выше запрет на использование сетей Wi-Fi не поддерживается.
- На устройствах с операционной системой Android 11 и выше Kaspersky Endpoint Security для Android должен быть установлен в качестве службы Специальных возможностей. Kaspersky Endpoint Security для Android предлагает пользователю установить приложение в качестве службы Специальных возможностей во время работы мастера первоначальной настройки. Пользователь может пропустить этот шаг или выключить службу в параметрах устройства позднее. В этом случае не удастся ограничить использование камеры.

Известные проблемы при отправке команд на мобильные устройства

- На устройствах с операционной системой Android 12 и выше, если пользователю предоставлено разрешение "Использовать приблизительное местоположение", Kaspersky Endpoint Security для Android сначала пытается определить точное местоположение устройства. Если это не удалось, определяется приблизительное местоположение устройства, но только в том случае, если данные о нем были получены не более 30 минут назад. В противном случае команда **Определить местоположение устройства** завершится с ошибкой.
- Если на устройстве Android отключена служба Google "Точность местоположения", команда **Определить местоположение устройства** работать не будет. Обращаем внимание, что не на всех устройствах Android есть эта служба.

Известные проблемы, связанные с рабочим профилем Android

- Если вы создаете рабочий профиль Android с помощью политики, пользователь должен предоставить разрешение "Разрешить доступ на управление всеми файлами" программе Kaspersky Endpoint Security для Android, установленной на устройствах под управлением Android 11 или более поздней версии и связанной с рабочим профилем.

- Функция рабочего профиля Android **Запретить включать режим отладки по USB** не работает на устройствах под управлением Android 13. Это связано с проблемой в Android 13.

- На некоторых устройствах Xiaomi рабочий профиль Android можно разблокировать с помощью отпечатка пальца только в том случае, если значение параметра **Период неактивности без блокировки экрана устройства** будет установлено после установки отпечатка пальца в качестве метода разблокировки экрана.

- При выборе действия **Отклонять разрешения автоматически** в параметре **Выдача дополнительных разрешений для работы приложений**, если после синхронизации устройства с Kaspersky Security Center пользователь настроил для приложения необходимые разрешения до того, как это приложение их запросило, то эти разрешения нельзя будет изменить без переустановки приложения или удаления его данных.

Известные проблемы, связанные с определенными моделями устройств

- На некоторых устройствах (например, HUAWEI, Meizu, Xiaomi) требуется предоставить приложению Kaspersky Endpoint Security для Android разрешение на автоматический запуск или вручную добавить его в список приложений, запускаемых при загрузке операционной системы. Если приложение не добавлено в список, Kaspersky Endpoint Security для Android прекращает выполнять все свои функции после перезагрузки мобильного устройства. Также, если устройство было заблокировано, разблокировать устройство с помощью команды невозможно. Вы можете разблокировать устройство только с помощью одноразового кода разблокировки.

- На некоторых устройствах (например, Meizu, Asus) под управлением Android 6 и выше после шифрования данных и перезагрузки устройства Android требует ввести цифровой пароль для разблокировки устройства. Если пользователь использует графический пароль для разблокировки, требуется перевести графический пароль в цифровой. Подробнее о переводе графического пароля в цифровой см. на сайте Службы технической поддержки компании-производителя мобильного устройства. Проблема связана с особенностями работы службы Специальных возможностей.

- На некоторых устройствах HUAWEI под управлением Android 5.X после установки Kaspersky Endpoint Security для Android в качестве службы Специальных возможностей отображается неверное сообщение об отсутствии соответствующих прав. Чтобы скрыть это сообщение, включите приложение как защищенное в настройках устройства.

- На некоторых устройствах HUAWEI под управлением Android 5.X или 6 при включенном режиме энергосбережения для Kaspersky Endpoint Security для Android пользователь может самостоятельно завершить работу приложения. При этом устройство пользователя не защищено. Проблема связана с особенностями программного обеспечения HUAWEI. Чтобы восстановить защиту устройства, запустите Kaspersky Endpoint Security для Android вручную. Рекомендуется отключить режим энергосбережения для приложения Kaspersky Endpoint Security для Android в настройках устройства.

- На устройствах HUAWEI с прошивкой EMUI под управлением Android 7 пользователь может скрыть уведомление о статусе защиты Kaspersky Endpoint Security для Android. Проблема связана с особенностями программного обеспечения HUAWEI.

- На некоторых Xiaomi-устройствах пользователь может использовать Диспетчер задач ОС, чтобы остановить работу Kaspersky Endpoint Security для Android в фоновом режиме. Проблема связана с особенностями программного обеспечения Xiaomi.

- На некоторых Xiaomi-устройствах при установке в политике длины пароля больше 5 символов пользователю будет предложено изменить пароль разблокировки экрана, а не PIN-код. Установить PIN-код длиной более 5 символов невозможно. Проблема связана с особенностями программного обеспечения Xiaomi.

- На Xiaomi-устройствах с прошивкой MIUI под управлением Android 6 значок Kaspersky Endpoint Security для Android в строке состояния может быть скрыт. Проблема связана с особенностями программного обеспечения Xiaomi. Рекомендуется разрешить отображение значков уведомлений в настройках уведомлений.

- На некоторых Nexus-устройствах под управлением Android 6.0.1 во время работы мастера первоначальной настройки Kaspersky Endpoint Security для Android невозможно выдать необходимые права для корректной работы. Проблема связана с известным дефектом в Security Patch для Android от Google. Для корректной работы приложения требуется вручную выдать необходимые права в настройках устройства.

- На некоторых Samsung-устройствах под управлением операционной системы Android 7.0 и выше при попытке пользователя настроить неподдерживаемые способы разблокировки устройства (например, графический пароль) устройство может быть заблокировано, если выполнены следующие условия: включена защита Kaspersky Endpoint Security для Android от удаления и заданы требования к надежности пароля разблокировки экрана. Для разблокировки устройства требуется отправить на устройство специальную команду.

- На некоторых Samsung-устройствах невозможно запретить использование отпечатков пальцев для разблокировки экрана.

- На некоторых Samsung-устройствах не работает Веб-Фильтр, если устройство подключено к сети 3G/4G, на устройстве включен режим энергосбережения и

ограничены фоновые данные. Рекомендуется выключить функцию отключения фоновых процессов в настройках режима энергосбережения.

- Также на некоторых Samsung-устройствах при несоответствии пароля разблокировки требованиям корпоративной безопасности Kaspersky Endpoint Security для Android не запрещает использование отпечатков пальцев для разблокировки экрана.

- На некоторых Samsung-устройствах после выполнения команд Анти-Вора (поиск, блокирование, разблокирование и фотографирование) мобильный сертификат и VPN-сертификат могут удалиться. Для продолжения работы требуется заново установить сертификаты. Проблема связана со стандартом безопасности MDFPP (Mobile Device Fundamentals Protection Profile).

- На некоторых устройствах Honor и HUAWEI невозможно ограничить использование Bluetooth. При попытке приложения Kaspersky Endpoint Security для Android ограничить использование Bluetooth операционная система показывает уведомление с вариантами действий: отклонить или разрешить это ограничение. Таким образом, пользователь может отклонить ограничение и продолжить использование Bluetooth.

- На некоторых устройствах Samsung после установки или обновления Kaspersky Endpoint Security из автономного инсталляционного пакета активация профиля KNOX MDM недоступна.

- На устройствах Blackview пользователь может очистить память для приложения Kaspersky Endpoint Security для Android. В результате защита и управление устройством отключается, все заданные параметры становятся недействительными, а приложение Kaspersky Endpoint Security для Android удаляется из специальных возможностей. Это связано с тем, что устройства этого производителя предоставляют приложению "Недавние экраны" (Recent screens) расширенные права. Приложение может переопределять значения параметров Kaspersky Endpoint Security для Android, и его нельзя заменить, поскольку оно является частью операционной системы Android.

- На некоторых устройствах Google Pixel под управлением Android 11 и ниже сразу после запуска приложения Kaspersky Endpoint Security для Android происходит его сбой. Это связано с проблемой в Android.

- На некоторых устройствах TECNO и OnePlus пользователь может разблокировать устройство с помощью сканирования лица, даже если этот метод биометрической разблокировки запрещен политикой.

- На некоторых устройствах (например, Xiaomi, Tecno и Realme) под управлением Android 9 или выше после установки флажка **Запретить изменение языка** в режиме device owner пользователь по-прежнему может изменить язык, при этом предупреждающее сообщение не отобразится.

- На некоторых устройствах Xiaomi, если для развертывания приложения Kaspersky Endpoint Security для Android используется инсталляционный пакет из Kaspersky

Security Center, встроенный антивирус может предложить загрузку из проверенного источника, например, из Xiaomi GetApps. Это связано с тем, что сертификат подписи инсталляционного пакета отличается от указанного в магазине приложений. Если установить приложение из магазина приложений, его дальнейшее обновление может завершиться с ошибкой. Чтобы предотвратить это, пользователю следует нажать на кнопку **Игнорировать** в появившемся окне **Обнаружены угрозы безопасности**, чтобы продолжить установку.

- На некоторых устройствах HUAWEI разрешения службы Специальных возможностей могут быть сброшены после запуска встроенного приложения Digital Balance.

Известные проблемы при работе на Android 13

- На Android 13 пользователь может использовать Диспетчер задач ОС, чтобы остановить работу Kaspersky Endpoint Security в фоновом режиме. Это связано с известной проблемой в Android 13.

- На Android 13 разрешение на отправку уведомлений запрашивается в начале настройки приложения. Это связано с особенностями операционной системы Android 13.

Известные проблемы при добавлении веб-клипов

- Максимальное количество веб-клипов, которые можно добавить на Android-устройство, зависит от типа устройства. Когда это количество достигнуто, веб-клипы перестают добавляться на Android-устройство.

Известные проблемы в режиме device owner

- Некоторые опции режима device owner и функции управления могут работать некорректно на устройствах Xiaomi (включая Redmi и POCO) из-за особенностей устройств этих производителей.

- На устройствах Xiaomi, Redmi и POCO могут не работать следующие ограничения функций Android:

- **Запретить изменение приложений через Настройки**

- **Запретить удаление приложений**

- Прочие проблемы:

- При установке приложения Kaspersky Endpoint Security для Android в режиме device owner на устройствах Xiaomi под управлением Android 12 приложение не запускается автоматически после завершения настройки устройства. Пожалуйста, запустите приложение вручную.

- При настройке разрешений для приложения Kaspersky Endpoint Security для Android на устройствах Xiaomi MI A3 под управлением стандартной операционной системы Android 11 может потребоваться дважды выдать разрешение "Специальные возможности", чтобы настройки применились. После выбора опции **Разрешить** разрешение "Специальные возможности" может быть запрошено повторно. Переведите переключатель в положение **Выключено**, а затем снова в положение **Включено**, чтобы применить изменения и завершить настройку.

- Защита приложения Kaspersky Endpoint Security для Android от удаления может не работать на некоторых устройствах Xiaomi. Проблема вызвана особенностями прошивки MIUI 7 и 8 на устройствах Xiaomi.

- На некоторых устройствах под управлением Android 10 или ниже после установки флажка **Запретить изменение приложений через Настройки** при настройке ограничений для приложений и после применения политики пользователь по-прежнему может сбрасывать настройки приложений по умолчанию и останавливать приложения через настройки. Это связано с особенностями операционной системы Android.

- Управление настройками обновлений на мобильных устройствах является вендор-специфичным. На некоторых Android-устройствах ограничения на установку обновлений операционной системы вручную пользователем могут работать некорректно.

- Приложение Kaspersky Endpoint Security для Android невозможно установить в режиме device owner на следующие устройства: Honor 30i (Android 10), HUAWEI y8p, HUAWEI Y5 (Android 8.0), HUAWEI Mate 40 PRO (Android 10), Xiaomi Redmi 4X (Android 7.1), Honor 5c (Android 7.0, EMUI 5.0). Это связано со спецификой прошивки устройств: сканер QR-кода недоступен после сброса устройства до заводских настроек.

- На устройствах под управлением Android 10 при выдаче разрешения на определение местоположения автоматически устанавливается значение **Разрешить только во время использования приложения** вместо **Разрешить в любом режиме**. Это значение не может быть изменено администратором или пользователями. Проблема связана с известной ошибкой в Android 10.

- Ограничение **Запретить снимки экрана** не блокирует снимки экрана в настройках устройства.

- На некоторых устройствах Samsung и Xiaomi ограничение **Запретить передачу файлов через USB** не блокирует передачу файлов через Android Debug Bridge (ADB).

- На некоторых устройствах (например, Samsung, Oppo или Google Pixel), если после обнаружения несоответствия **Установлены запрещенные приложения** истекло время, выделенное пользователю устройства для устранения этого несоответствия, то выбранное действие может выполниться с задержкой или может потребовать синхронизации устройства с Kaspersky Security Center.

Известные проблемы, связанные с конфигурациями приложений

- Настройки **Настроить Безопасный режим для YouTube**, **Включить обязательное использование хотя бы Умеренного безопасного режима** и **Отключить обязательное использование Безопасного режима** не работают для Google Chrome. Проблема связана с известным дефектом в Google Chrome.

Развертывание

Этот раздел справки адресован специалистам, которые осуществляют установку Kaspersky Endpoint Security для Android, и специалистам технической поддержки организаций, использующих Kaspersky Endpoint Security для Android.

В этом разделе

Схемы развертывания Kaspersky Endpoint Security для Android

Разрешения

Для работы всех функций приложений Kaspersky Endpoint Security для Android запрашивает у пользователя необходимые разрешения. Kaspersky Endpoint Security для Android запрашивает обязательные разрешения во время прохождения мастера установки, а также после установки перед использованием отдельных функций приложений. Без предоставления обязательных разрешений Kaspersky Endpoint Security для Android установить невозможно.

На некоторых устройствах (например, HUAWEI, Meizu, Xiaomi) требуется в настройках устройства вручную добавить Kaspersky Endpoint Security для Android в список приложений, запускаемых при загрузке операционной системы. Если приложение не добавлено в список, Kaspersky Endpoint Security для Android прекращает выполнять все свои функции после перезагрузки мобильного устройства.

На устройствах с операционной системой Android 11 или выше, либо Android 6-10 (при использовании сервисов Google Play) необходимо выключить системную настройку **Удалять разрешения, если приложение не используется**. В противном случае, если приложение не используется в течение нескольких

месяцев, система автоматически сбрасывает разрешения, предоставленные приложению пользователем.

Разрешения, запрашиваемые Kaspersky Endpoint Security для Android

Разрешение	Функция приложения
Телефон (для Android 5.0 – 9)	Подключение к Kaspersky Security Center (идентификатор устройства)
Память (обязательно)	Защита от вредоносного ПО
Доступ на управление всеми файлами (для Android 11 или выше)	Защита от вредоносного ПО
Устройства Bluetooth поблизости (для Android 12 или выше)	Ограничение использования Bluetooth На некоторых устройствах Xiaomi и HUAWEI под управлением Android 12 Kaspersky Endpoint Security для Android не запрашивает у пользователя разрешение "**Устройства Bluetooth поблизости**". Проблема связана с особенностями прошивки MIUI на Xiaomi и прошивки EMUI на HUAWEI. Несмотря на отсутствие запроса на это разрешение, все функции, связанные с использованием Bluetooth, корректно работают на этих устройствах.
Игнорировать оптимизацию батареи (для Android 12 или выше)	Контроль приложений. Веб-Фильтр. Анти-Вор.
Уведомления (для Android 13)	Уведомление пользователя о проблемах безопасности и событиях приложения
Разрешение на работу в фоновом режиме (для Android 12 или выше. Для Android 11 и ниже разрешение не требуется)	Обеспечение непрерывной работы приложения. Если разрешение не предоставлено, приложение может быть выгружено из памяти и не сможет перезапуститься.

Администратор устройства (обязательно)	Анти-Вор – блокировка устройства (только для Android 5.0 – 6)
	Анти-Вор – выполнение снимка фронтальной камерой
	Анти-Вор – воспроизведение звукового сигнала
	Анти-Вор – сброс настроек до заводских
	Защита паролем
	Защита приложения от удаления
	Установка сертификатов безопасности
	Контроль приложений
	Управление KNOX (только для Samsung-устройств)
	настройка Wi-Fi;
	настройка Exchange ActiveSync;
	ограничение использования камеры, Bluetooth, Wi-Fi.
Камера	Анти-Вор – выполнение снимка фронтальной камерой
	На устройствах с операционной системой Android 11 или выше необходимо при появлении запроса предоставить разрешение "При использовании приложения".
Местоположение	Анти-Вор – определение местоположения устройства
	На устройствах с операционной системой Android 10 или выше необходимо при

	появлении запроса предоставить разрешение "Всегда".
Специальные возможности	Анти-Вор – блокировка устройства (только для Android 7.0 или выше) Веб-Фильтр Контроль приложений Защита приложения от удаления (только для Android 7.0 или выше) Отображение предупреждений Kaspersky Endpoint Security для Android (только для Android 10 или выше) Ограничение использования камеры (только для Android 11 или выше)
Отображать всплывающее окно (на некоторых устройствах Xiaomi)	Веб-Фильтр
Отображать всплывающие окна при работе в фоновом режиме (на некоторых устройствах Xiaomi)	Веб-Фильтр
Работа в фоновом режиме (для устройств Xiaomi с прошивкой MIUI под управлением Android 11 или ниже).	Контроль приложений. Веб-Фильтр. Анти-Вор.

Способы установки приложения

- **Загрузить приложение с веб-сайта "Лаборатории Касперского"**

  Выберите этот способ для мобильных устройств, которые имеют доступ в интернет, чтобы загрузить установочный файл APK с сайта "Лаборатории Касперского".

Обновление предыдущей версии программы

Обновление программы должно выполняться с учетом следующих требований:

- Соблюдайте версионность мобильного приложения Kaspersky Endpoint Security для Android.
- Используйте одну версию Kaspersky Endpoint Security для Android на всех мобильных устройствах организации.

Вы можете посмотреть версию и номер сборки приложения Kaspersky Endpoint Security для Android следующими способами:

- Если Kaspersky Endpoint Security для Android установлен с помощью автономного пакета установки, вы можете посмотреть версию и номер сборки приложения в свойствах пакета.

В этом разделе

Удаление Kaspersky Endpoint Security для Android

Удаление Kaspersky Endpoint Security для Android может быть выполнено следующими способами:

1. Удаление приложения пользователем

Пользователь самостоятельно удаляет Kaspersky Endpoint Security для Android, используя интерфейс приложения. Чтобы пользователи могли удалить приложение, в групповой политике, которая применена к устройству, должно быть разрешено удаление приложения.

Настройка доступа пользователей к веб-сайтам

В этом разделе содержатся инструкции по настройке доступа к веб-сайтам на Android устройствах.

В этом разделе

Настройка доступа к веб-сайтам на Android-устройствах

Вы можете настраивать доступ пользователей Android-устройств к веб-сайтам с помощью Веб-Фильтра. Веб-Фильтр поддерживает фильтрацию веб-сайтов по категориям, определенным в облачной службе Kaspersky Security Network. Фильтрация позволяет вам ограничить доступ пользователей к отдельным веб-сайтам или категориям веб-сайтов (например, к веб-сайтам из категории "Азартные игры, лотереи, тотализаторы" или "Общение в сети"). Веб-Фильтр также защищает персональные данные пользователей в интернете.

Для работы Веб-Фильтра необходимо выполнение следующих условий:

- Положение об обработке данных в целях использования Веб-Фильтра (Положение о Веб-Фильтре) должно быть принято. Kaspersky Endpoint Security использует Kaspersky Security Network (KSN) для проверки веб-сайтов. Положение о Веб-Фильтре содержит условия обмена данными с KSN.

  Вы можете принять Положение о Веб-Фильтре в Kaspersky Security Center. В этом случае пользователю не потребуется выполнять никаких действий.

  Если вы не приняли Положение о Веб-Фильтре и направили пользователю запрос на принятие Положения, пользователь должен прочитать и принять Положение о Веб-Фильтре в настройках приложения.

  Если вы не приняли Положение о Веб-Фильтре, Веб-Фильтр будет недоступен.

  Веб-Фильтр на Android-устройствах поддерживается только браузерами Google Chrome, HUAWEI Browser, Samsung Internet Browser и Яндекс Браузер.

  Если приложение Kaspersky Endpoint Security для Android в режиме device owner не установлено в качестве службы Специальных возможностей, Веб-Фильтр поддерживается только браузером Google Chrome и проверяет только домен сайта. Чтобы Веб-Фильтр поддерживался другими браузерами (Samsung Internet Browser, Яндекс Браузер и HUAWEI Browser), приложение Kaspersky Endpoint Security должно быть включено в качестве службы Специальных возможностей. Это также позволит использовать функцию Custom Tabs.

  Функция Custom Tabs поддерживается браузерами Google Chrome, HUAWEI Browser и Samsung Internet Browser.

В браузерах HUAWEI Browser, Samsung Internet Browser и Яндекс Браузер Веб-Фильтр не блокирует сайты на мобильном устройстве, если используется рабочий профиль и установлен флажок Включить Веб-Фильтр только в рабочем профиле.

По умолчанию Веб-Фильтр включен: ограничен доступ пользователя к веб-сайтам категорий **Фишинг** и **Вредоносное программное обеспечение**. На устройствах в режиме device owner, управляемых приложением Kaspersky Endpoint Security для Android, Веб-Фильтр поддерживается только браузером Google Chrome и

проверяет только домен сайта. Чтобы Веб-Фильтр поддерживался другими браузерами (Samsung Internet Browser, Яндекс Браузер и HUAWEI Browser), приложение Kaspersky Endpoint Security должно быть включено в качестве службы Специальных возможностей.

Контроль соответствия

В этом разделе приведены инструкции по контролю соблюдения корпоративных требований на устройствах и настройке правил контроля соответствия.

В этом разделе

Контроль соответствия Android-устройств требованиям корпоративной безопасности

Контроль соответствия Android-устройств требованиям корпоративной безопасности

Вы можете контролировать Android-устройства на соответствие требованиям корпоративной безопасности. Требования корпоративной безопасности регламентируют работу пользователя с устройством. Например, на устройстве должна быть включена постоянная защита, базы вредоносного ПО должны быть актуальны, пароль устройства должен быть достаточно сложным. Контроль соответствия работает на основе списка правил. Правило соответствия состоит из следующих компонентов:

- критерий проверки устройства (например, отсутствие на устройстве запрещенных приложений);
- время, выделенное пользователю устройства для устранения несоответствия (например, 24 часа);
- действия, которые будут выполнены с устройством, если пользователь не устранит несоответствие в течение указанного времени (например, блокирование устройства).

Если устройство находится в режиме энергосбережения, приложение может выполнить эту задачу позже, чем указано. Для своевременного реагирования KES-устройств под управлением Android на команды администратора, следует включить использование сервиса Google Firebase Cloud Messaging.

Контроль приложений

В этом разделе содержатся инструкции по настройке доступа пользователей к приложениям на мобильном устройстве.

В этом разделе

Контроль приложений на Android-устройствах

Компонент Контроль приложений позволяет управлять приложениями на Android-устройствах, чтобы обеспечивать безопасность этих устройств.

Вы можете установить ограничения при работе пользователя с устройством, на котором установлены запрещенные приложения или не установлены обязательные приложения (например, заблокировать устройство). Вы можете установить ограничения с помощью компонента Контроль соответствия. Для этого в параметрах правила проверки требуется выбрать критерий **Установлены запрещенные приложения**, **Установлены приложения запрещенных категорий** или **Не установлены все обязательные приложения**.

Для работы Контроля приложений Kaspersky Endpoint Security для Android должен быть установлен в качестве службы Специальных возможностей. Kaspersky Endpoint Security для Android предлагает пользователю установить приложение в качестве службы Специальных возможностей во время работы мастера первоначальной настройки. Пользователь может пропустить этот шаг или выключить службу в параметрах устройства позднее. В этом случае Контроль приложений не работает.

В режиме device owner вам доступен расширенный контроль над устройством. Контроль приложений работает, не уведомляя об этом пользователя устройства:

- Обязательные приложения устанавливаются автоматически в фоновом режиме. Для тихой установки приложений необходимо указать ссылку на APK-файл обязательного приложения в настройках политики.
- Запрещенные приложения можно удалять с устройства автоматически. Для тихого удаления приложений необходимо установить флажок **Автоматически удалять запрещенные приложения (только в режиме device owner)** в настройках политики.

Защита данных при потере или краже устройств

Этот раздел содержит информацию о настройке параметров защиты мобильного устройства от несанкционированного доступа в случае потери или кражи.

В этом разделе

Разблокировка мобильного устройства

Шифрование данных

Удаление данных на Android-устройствах после неудачных попыток ввода пароля

Отправка команд на утерянное или украденное мобильное устройство

Для защиты данных на мобильном устройстве в случае его потери или кражи вы можете отправить специальные команды.

Вы можете отправлять команды на следующие типы управляемых мобильных устройств:

- Android-устройства, управляемые через приложение Kaspersky Endpoint Security для Android;

Каждый тип устройств поддерживает свой набор команд (см. таблицу ниже).

Команды для Android-устройств

Команды для защиты данных при потере или краже Android-устройства

Команда	Результат выполнения команды
Заблокировать	Мобильное устройство заблокировано. Для получения доступа к данным необходимо разблокировать устройство.
Разблокировать	Мобильное устройство разблокировано.
	После разблокировки устройства под управлением операционной системы Android 5.0–6 пароль разблокировки экрана будет заменен на "1234". На устройствах под управлением операционной системы Android 7.0 и выше после разблокировки мобильного устройства пароль разблокировки экрана останется прежним.
Определить местоположение устройства	Получены координаты местоположения мобильного устройства.
	На устройствах с операционной системой Android 12 и выше, если пользователю предоставлено разрешение "Использовать приблизительное местоположение", Kaspersky Endpoint Security для Android сначала пытается определить точное местоположение устройства. Если это не удалось, определяется приблизительное

	местоположение устройства, но только в том случае, если данные о нем были получены не более 30 минут назад. В противном случае команда **Определить местоположение устройства** завершится с ошибкой. Если на устройстве Android отключена служба Google "Точность местоположения", команда **Определить местоположение устройства** работать не будет. Обращаем внимание, что не на всех устройствах Android есть эта служба.
Сфотографировать	Мобильное устройство заблокировано. Фотография выполнена фронтальной камерой устройства при попытке разблокировать устройство. На устройствах с выдвижной фронтальной камерой фотография будет черной, если камера закрыта.
	При попытке разблокировки устройства пользователь автоматически соглашается на фотографирование. Если разрешение на использование камеры было отозвано, на мобильном устройстве отображается уведомление, предлагающее предоставить это разрешение. Если разрешение на использование камеры было отозвано из панели быстрых настроек на мобильном устройстве под управлением Android 12 или более поздней версии, уведомление не отображается, но сделанная фотография будет черной.
Воспроизвести звуковой сигнал	Мобильное устройство воспроизводит звуковой сигнал. Звуковой сигнал воспроизводится 5 мин (при низком уровне заряда батареи – 1 мин).
Удалить данные приложения	Данные указанного приложения удалены с мобильного устройства.
	Действие применимо только к устройствам с Android 9 или выше в режиме device owner или с установленным рабочим профилем Android. Для выполнения действия необходимо указать имя пакета приложения, данные которого должны быть удалены. **Как получить имя пакета приложения** В результате выполнения команды приложение возвращается в состояние по умолчанию.

Данные системных приложений и приложений-администраторов не удаляются.

Чтобы получить имя пакета приложения:

Откройте Google Play.

Найдите нужное приложение и откройте его страницу.

URL приложения оканчивается именем пакета приложения (например, https://play.google.com/store/apps/details?id=**com.android.chrome**).

Чтобы получить имя пакета приложения, которое было добавлено в Kaspersky Security Center:

В дереве консоли Kaspersky Security Center выберите **Дополнительно** > **Удаленная установка** > **Инсталляционные пакеты**.

Нажмите на кнопку **Дополнительные действия** и в раскрывающемся списке выберите **Управление пакетами мобильных приложений**.

В открывшемся окне **Управление пакетами мобильных приложений** в столбце **Название приложения** отображаются идентификаторы управляемых приложений.

Если пакет приложения представлен файлом в формате .apk или .ipa, и необходимо узнать идентификатор приложения, можно добавить этот пакет приложения в окне **Управление пакетами мобильных приложений**, нажав на кнопку **Новый** и следуя инструкциям на экране.

Удалить данные всех приложений	Данные всех приложений удалены с мобильного устройства.

Действие применимо только к устройствам с Android 9 или выше в режиме device owner или с установленным рабочим профилем Android.

Если устройство работает в режиме device owner, данные всех приложений на устройстве удалены.

	Если на устройстве создан рабочий профиль Android, данные всех приложений в рабочем профиле удалены. В результате выполнения команды приложения возвращаются в состояние по умолчанию. Данные системных приложений и приложений-администраторов не удаляются.
Удалить корпоративные данные	Корпоративные данные удалены с устройства. Перечень удаленных данных зависит от режима работы устройства. На личном устройстве удалены KNOX-контейнер и почтовый сертификат. Если устройство работает в режиме device owner, удалены KNOX-контейнер и сертификаты, установленные приложением Kaspersky Endpoint Security для Android (почтовые и VPN-сертификаты, сертификаты, полученные через профили SCEP, кроме мобильных сертификатов). Дополнительно, если установлен рабочий профиль Android, удален рабочий профиль (содержимое, настройки и ограничения) и сертификаты, установленные в рабочем профиле (почтовые и VPN-сертификаты, сертификаты, полученные через профили SCEP, кроме мобильных сертификатов).
Сбросить настройки до заводских	Удалены все данные с мобильного устройства, настройки мобильного устройства сброшены до заводских. После выполнения этой команды устройство не сможет получать и выполнять последующие команды.
Получить историю местоположений устройства	Отображается история местоположений мобильного устройства за последние 14 дней. Эта команда работает только в том случае, если в базе Сервера администрирования хранится тип информационного события **История местоположений устройства**. События настраиваются в разделе **События** свойств политики. Дополнительная информация о событиях приведена в справке Kaspersky Security Center. Из-за технических ограничений на устройствах Android фактическое получение местоположения устройства может

происходить реже, чем указано в разделе **Синхронизация** свойств политики.

Для выполнения команд Kaspersky Endpoint Security для Android требуются специальные права и разрешения. Во время работы мастера первоначальной настройки Kaspersky Endpoint Security для Android предлагает пользователю предоставить приложению необходимые права и разрешения. Пользователь может пропустить эти шаги или выключить права в параметрах устройства позднее. В этом случае выполнение команд невозможно.

На устройствах с операционной системой Android 10 и выше необходимо предоставить разрешение "Всегда" для доступа к местоположению устройства. На устройствах с операционной системой Android 11 и выше необходимо также предоставить разрешение "При использовании приложения" для доступа к камере. В противном случае команды Анти-Вора работать не будут. Пользователю будет выведено уведомление об этом ограничении и будет предложено повторно предоставить требуемые разрешения. Если пользователь выбрал вариант "Только сейчас" для разрешения камеры, считается, что доступ предоставлен приложением. Рекомендуется связаться с пользователем напрямую при повторном запросе разрешения для камеры.

Полный список доступных команд приведен в разделе "Команды для мобильных устройств". Подробная информация об отправке команд из Консоли администрирования приведена в разделе "Отправка команд".

Разблокировка мобильного устройства

Вы можете разблокировать мобильное устройство следующими способами:

- Отправить команду разблокировки мобильного устройства.
- Ввести на мобильном устройстве одноразовый код разблокировки (только для Android-устройств).

На некоторых устройствах (например, HUAWEI, Meizu, Xiaomi) требуется вручную добавить Kaspersky Endpoint Security для Android в список приложений, запускаемых при загрузке операционной системы. Если приложение не добавлено в список, вы можете разблокировать устройство только с помощью одноразового кода разблокировки. Разблокировать устройство с помощью команд невозможно.

Подробная информация об отправке команд из списка мобильных устройств в Консоли администрирования приведена в разделе "Отправка команд".

Одноразовый код разблокировки – секретный код программы для разблокировки мобильного устройства. Одноразовый код создается программой и является уникальным для каждого мобильного устройства. Вы можете изменить длину одноразового кода (4, 8 или 16 цифр) в параметрах групповой политики в разделе **Анти-Вор**.

Чтобы разблокировать мобильное устройство с помощью одноразового кода, выполните следующие действия:

1. В дереве консоли выберите **Управление мобильными устройствами** → **Мобильные устройства**.
2. Выберите мобильное устройство, для которого вы хотите получить одноразовый код для разблокировки.
3. Откройте окно свойств мобильного устройства двойным щелчком мыши.
4. Выберите раздел **Приложения** → **Kaspersky Endpoint Security для Android**.
5. Откройте окно свойств приложения Kaspersky Endpoint Security двойным щелчком мыши.
6. Выберите раздел **Анти-Вор**.
7. В блоке **Одноразовый код разблокировки устройства** в поле **Одноразовый код** будет указан уникальный для выбранного устройства код.
8. Сообщите пользователю заблокированного мобильного устройства одноразовый код любым доступным способом (например, в сообщении электронной почты).
9. Пользователь вводит одноразовый код на экране устройства, заблокированном Kaspersky Endpoint Security для Android.

   Мобильное устройство разблокировано.

После разблокировки устройства под управлением операционной системы Android 5.0–6 пароль разблокировки экрана будет заменен на "1234". На устройствах под управлением операционной системы Android 7.0 и выше после разблокировки мобильного устройства пароль разблокировки экрана останется прежним.

Шифрование данных

Для защиты данных от несанкционированного доступа требуется включить шифрование всех данных на устройстве (например, учетных данных, внешних устройств и приложений, а также сообщений электронной почты, SMS-сообщений,

контактов, фотографий и других файлов). Для доступа к зашифрованным данным требуется задать специальный ключ – пароль для разблокировки устройства. Таким образом, если данные зашифрованы, доступ к ним можно получить, только когда устройство разблокировано.

Чтобы зашифровать все данные на Android-устройстве, выполните следующие действия:

1. Включите блокирование экрана на Android-устройстве (**Настройки** → **Безопасность** → **Блокирование экрана**).

2. Установите пароль разблокировки устройства, соответствующий требованиям корпоративной безопасности.

> Не рекомендуется использовать графический пароль для разблокировки устройства. На некоторых Android-устройствах под управлением Android 6 и выше после шифрования данных и перезагрузки устройства Android требует ввести цифровой пароль для разблокировки устройства вместо графического. Проблема связана с особенностями работы службы Специальных возможностей. Для разблокировки экрана устройства в этом случае переведите графический пароль в цифровой. Подробнее о переводе графического пароля в цифровой см. на сайте Службы технической поддержки компании-производителя мобильного устройства.

3. Включите шифрование всех данных устройства (**Настройки** → **Безопасность** → **Зашифровать данные**).

Удаление данных на Android-устройствах после неудачных попыток ввода пароля

Вы можете настроить удаление всех данных на Android-устройстве (то есть сброс настроек устройства до заводских) после того, как пользователь неправильно ввел пароль разблокировки экрана слишком много раз.

Эти настройки применимы для устройств, работающих в режиме device owner, и персональных устройств, на которых приложение Kaspersky Endpoint Security для Android включено в качестве администратора устройства.

Настройка надежности пароля разблокировки устройства

Для защиты доступа к мобильному устройству пользователя следует настроить пароль разблокировки устройства.

Этот раздел содержит информацию о настройке защиты паролем Android-устройств.

В этом разделе

Настройка надежности пароля разблокировки Android-устройства

Для обеспечения безопасности Android-устройства нужно настроить использование пароля, который запрашивается при выходе устройства из спящего режима.

Вы можете установить ограничения при работе пользователя с устройством, если пароль разблокировки недостаточно сложный (например, заблокировать устройство). Вы можете установить ограничения с помощью компонента Контроль соответствия. Для этого в параметрах правила проверки требуется выбрать критерий **Пароль разблокировки не соответствует требованиям безопасности**.

На некоторых Samsung-устройствах под управлением операционной системы Android 7.0 и выше при попытке пользователя настроить неподдерживаемые способы разблокировки устройства (например, графический пароль) устройство может быть заблокировано, если выполнены следующие условия: включена защита Kaspersky Endpoint Security для Android от удаления и заданы требования к надежности пароля разблокировки экрана. Для разблокировки устройства требуется отправить на устройство специальную команду.

Защита Kaspersky Endpoint Security для Android от удаления

Для защиты мобильного устройства и выполнения требований корпоративной безопасности вы можете включить защиту Kaspersky Endpoint Security для Android от удаления. В этом случае пользователю недоступно удаление приложения с помощью интерфейса Kaspersky Endpoint Security для Android. При удалении приложения с помощью инструментов операционной системы Android появится запрос на выключение прав администратора для Kaspersky Endpoint Security для Android. После выключения прав мобильное устройство будет заблокировано.

На некоторых Samsung-устройствах под управлением операционной системы Android 7.0 и выше при попытке пользователя настроить неподдерживаемые способы разблокировки устройства (например, графический пароль) устройство может быть заблокировано, если выполнены следующие условия: включена защита Kaspersky Endpoint Security для Android от удаления и заданы требования к надежности пароля разблокировки экрана. Для разблокировки устройства требуется отправить на устройство специальную команду.

Обнаружение взлома устройства (получение root-прав)

Kaspersky Endpoint Security для Android позволяет обнаруживать взлом устройства (получение root-прав). На взломанном устройстве системные файлы не защищены и доступны для изменения. Также на взломанном устройстве доступна установка сторонних приложений из неизвестных источников. После обнаружения взлома рекомендуется восстановить нормальную работу устройства.

Kaspersky Endpoint Security для Android использует следующие службы для обнаружения получения пользователем root-прав:

- *Встроенная служба Kaspersky Endpoint Security для Android*. Служба "Лаборатории Касперского", которая проверяет получение root-прав пользователем мобильного устройства (Kaspersky Mobile Security SDK).

  При взломе устройства вы получите уведомление. Вы можете просмотреть уведомления о взломе в рабочей области Сервера администрирования на закладке **Мониторинг**. Вы также можете выключить уведомление о взломе в параметрах уведомлений о событиях.

  На устройствах под управлением операционной системы Android вы можете установить ограничения при работе пользователя с устройством в случае взлома (например, заблокировать устройство). Вы можете установить ограничения с помощью компонента Контроль соответствия. Для этого в параметрах правила соответствия требуется выбрать критерий **На устройстве получены root-права**.

Настройка уведомлений Kaspersky Endpoint Security для Android

Если вы хотите, чтобы пользователь мобильного устройства не отвлекался на уведомления Kaspersky Endpoint Security для Android, вы можете выключить некоторые уведомления.

В Kaspersky Endpoint Security используются следующие средства для отображения статуса защиты устройства:

- **Уведомление о состоянии защиты**. Уведомление закреплено в панели уведомлений. Уведомление о состоянии защиты нельзя удалить. В уведомлении отображается статус защиты устройства (например, ) и количество проблем, если они имеются. Чтобы посмотреть список проблем в приложении, выберите статус защиты устройства.

- **Уведомления приложения**. Уведомления информируют пользователя устройства о приложении (например, об обнаружении угрозы).

- **Всплывающие сообщения**. Всплывающие сообщения требуют внимания со стороны пользователя устройства (например, действия, предпринимаемые при обнаружении угрозы).

  По умолчанию все уведомления Kaspersky Endpoint Security для Android включены.

На Android 13 пользователь устройства должен предоставить разрешение на отправку уведомлений во время работы Мастера начальной настройки или позже.

Пользователь Android-устройства может выключить все уведомления от Kaspersky Endpoint Security для Android в настройках панели уведомлений. Если уведомления выключены, пользователь не контролирует работу приложения и может пропустить важную информацию (например, о сбоях при синхронизации устройства с Kaspersky Security Center). Чтобы пользователь узнал статус работы приложения, ему необходимо открыть Kaspersky Endpoint Security для Android.

Участие в Kaspersky Security Network

В сертифицированной версии программы использование Глобального KSN не допускается, так как приводит к выходу программы из сертифицированного состояния.

Чтобы повысить эффективность защиты мобильных устройств, Kaspersky Endpoint Security для Android использует данные, полученные от пользователей со всего мира. Для обработки этих данных предназначена сеть *Kaspersky Security Network*.

Kaspersky Security Network (KSN) – инфраструктура облачных служб, предоставляющая доступ к оперативной базе знаний "Лаборатории Касперского" о репутации файлов, веб-ресурсов и программного обеспечения. Использование данных Kaspersky Security Network обеспечивает более высокую скорость реакции программ "Лаборатории Касперского" на угрозы, повышает эффективность работы некоторых компонентов защиты, а также снижает вероятность ложных срабатываний.

Ваше участие в Kaspersky Security Network позволяет "Лаборатории Касперского" оперативно получать информацию о типах и источниках новых угроз, разрабатывать способы их нейтрализации, уменьшать количество ложных срабатываний Kaspersky Endpoint Security для Android. Кроме того, участие в Kaspersky Security Network обеспечивает доступ к данным о репутации программ и веб-сайтов.

Когда вы участвуете в Kaspersky Security Network, статистика, полученная в результате работы Kaspersky Endpoint Security для Android, автоматически отправляется в "Лабораторию Касперского". Эта информация позволяет отслеживать угрозы в режиме реального времени. Также для дополнительной

проверки в "Лабораторию Касперского" могут отправляться файлы (или их части), в отношении которых существует риск использования их злоумышленником для нанесения вреда компьютеру или данным пользователя.

Использование Kaspersky Security Network необходимо для работы Kaspersky Endpoint Security для Android. KSN используется для работы основных компонентов приложения: Защита от вредоносного ПО, Веб-Фильтр и Контроль приложений. Отказ от участия в KSN снижает уровень защиты устройства, что может привести к заражению устройства и потере информации. Чтобы начать использование Kaspersky Security Network, вы должны принять условия Лицензионного соглашения при установке приложения. В Лицензионном соглашении вы можете ознакомиться с тем, какие данные Kaspersky Endpoint Security для Android передает в Kaspersky Security Network.

Для повышения качества работы приложения вы можете дополнительно отправлять в Kaspersky Security Network статистические данные. Участие в Kaspersky Security Network для обработки статистических данных является добровольным. Чтобы начать использование Kaspersky Security Network, вы должны принять условия специального соглашения – *Положения о Kaspersky Security Network*. Вы можете в любой момент отказаться от участия в Kaspersky Security Network. В Положении о Kaspersky Security Network вы можете прочитать о том, какие данные Kaspersky Endpoint Security для Android передает в Kaspersky Security Network.

В этом разделе

Обмен информацией с Kaspersky Security Network

Для повышения уровня оперативной защиты Kaspersky Secure Mobility Management использует облачную службу Kaspersky Security Network в работе следующих компонентов:

- **Защита от вредоносного ПО.** Приложение получает доступ к оперативной базе знаний "Лаборатории Касперского" о репутации файлов и приложений. Проверка производится на угрозы, информация о которых еще не вошла в базы вредоносного ПО, но уже содержится в KSN. Облачная служба Kaspersky Security Network обеспечивает полноценную работу Защиты от вредоносного ПО и снижает вероятность ложных срабатываний.

- **Веб-Фильтр.** Приложение выполняет проверку веб-сайтов до их открытия с учетом данных, полученных от KSN. Также приложение определяет категорию

веб-сайта для контроля доступа пользователей в интернет на основе списков разрешенных и запрещенных категорий (например, категория "Общение в сети").

- **Контроль приложений.** Приложение определяет категорию приложения для ограничения запуска приложения, которые не удовлетворяют требованиям корпоративной безопасности, на основе списков разрешенных и запрещенных категорий (например, категория "Игры").

  Информация о типах данных, передаваемых в "Лабораторию Касперского" при использовании KSN во время работы компонентов Защита от вредоносного ПО и Контроль приложений, приведена в Лицензионном соглашении. Принимая условия Лицензионного соглашения, вы соглашаетесь передавать следующую информацию.

  Информация о типах данных, передаваемых в "Лаборатории Касперского" при использовании KSN во время работы Веб-Фильтра, доступна в Положении об обработке данных для использования Веб-Фильтра. Принимая условия этого Положения, вы соглашаетесь передавать перечисленную ниже информацию.

  В целях выявления новых и сложных для обнаружения угроз информационной безопасности и их источников, угроз вторжения, а также повышения уровня защиты информации, хранимой и обрабатываемой на устройстве, вы можете расширить участие в Kaspersky Security Network.

  Для обмена данными с KSN в целях повышения качества работы приложения должны быть выполнены следующие условия:

- Вам или пользователю устройства необходимо прочитать и принять условия Положения о Kaspersky Security Network. Если выбран вариант, при котором Положение принимается пользователями, на главном экране приложения отобразится уведомление с предложением принять условия Положения. Пользователи также могут принять Положение в разделе **О приложении** в настройках Kaspersky Endpoint Security для Android.

  Если выбран вариант, при котором Положения принимаются глобально, версии Положений, принимаемые в Kaspersky Security Center, должны совпадать с версиями, уже принятыми пользователями. В противном случае пользователи будут проинформированы об этой проблеме, и им будет предложено принять ту версию Положения, которая соответствует версии, принятой администратором глобально. Статус устройства в плагине Kaspersky Security for Mobile (Devices) изменится на *Предупреждение*.

- Необходимо разрешить передачу статистики в KSN в параметрах групповой политики.

  Вы можете в любой момент отказаться от отправки статистических данных в KSN. Информация о типах статистических данных, передаваемых в "Лабораторию Касперского" при использовании KSN во время работы мобильного приложения

Kaspersky Endpoint Security для Android, приведена в Положении о Kaspersky Security Network.

Подробная информация о предоставлении данных в KSN приведена в разделе Предоставление данных.

Предоставление данных в KSN является добровольным. При желании можно отключить обмен данными с KSN.

Включение и выключение использования Kaspersky Security Network

Для работы компонентов приложения Kaspersky Endpoint Security для Android, использующих Kaspersky Security Network, выполняется отправка запросов в облачные службы. Запросы содержат данные, описанные в разделе Предоставление данных.

Если использование Kaspersky Security Network на устройстве выключено, компоненты Облачная защита, Веб-Фильтр и Контроль приложений автоматически выключаются.

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

1. Откройте окно параметров политики управления мобильными устройствами, на которых установлено приложение Kaspersky Endpoint Security для Android.
2. В политике, в окне **Свойства** выберите раздел **Дополнительно**.
3. В блоке **Параметры Kaspersky Security Network (KSN)** настройте параметры использования Kaspersky Security Network:

- Установите флажок **Использовать Kaspersky Security Network** для работы следующих компонентов: Защита от вредоносного ПО (Облачная защита), Веб-Фильтр, Контроль приложения (категории приложений).
- Установите флажок **Разрешить передачу статистических данных в KSN** для передачи данных в "Лабораторию Касперского". Данные позволят увеличить скорость реакции приложения Kaspersky Endpoint Security для Android на угрозы, улучшить производительность компонентов защиты, снизить вероятность ложных срабатываний.

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

Параметры на мобильном устройстве будут изменены после очередной синхронизации устройства с Kaspersky Security Center. После применения

политики компоненты, использующие Kaspersky Security Network, будут выключены и настройка компонентов будет недоступна.

Использование Kaspersky Private Security Network

Kaspersky Private Security Network (далее также *KPSN*) – это решение, предоставляющее доступ к репутационным базам Kaspersky Security Network (KSN) без отправки данных с устройств пользователей в Kaspersky Security Network.

База данных репутации объектов (файлов или веб-адресов) хранится на сервере Kaspersky Private Security Network, а не на серверах Kaspersky Security Network. Репутационные базы данных KPSN хранятся в корпоративной сети и управляются администратором компании.

При включенном KPSN Kaspersky Endpoint Security не отправляет статистические данные с устройств пользователей в KSN.

Чтобы включить использование KPSN в Kaspersky Security Center, выполните следующие действия:

1. В главном окне Kaspersky Security Center Web Console или Cloud Console нажмите на кнопку **Настройка** ( ).

   Откроется окно свойств Сервера администрирования.
2. На закладке **Общие** перейдите в раздел **Параметры прокси-сервера KSN**.
3. Установите переключатель в положение **Использование Kaspersky Private Security Network включено**.
4. Нажмите на кнопку **Выбрать файл с параметрами прокси-сервера KSN**, а затем выберите файл конфигурации с расширением pkcs7 или pem (предоставляется "Лабораторией Касперского").
5. Нажмите кнопку **Открыть**.
6. Если в свойствах Сервера администрирования настроены параметры прокси-сервера, но для архитектуры сети требуется использовать KPSN напрямую, включите параметр **Игнорировать параметры прокси-сервера при подключении к Локальному KSN**. В противном случае запросы от управляемых программ не попадут в KPSN.
7. Нажмите на кнопку **Сохранить**.

   После загрузки параметров в интерфейсе отобразится имя и контакты поставщика услуг, а также дата создания файла с параметрами KPSN. Параметры KPSN применятся к мобильным устройствам.

При переходе на KPSN компонент Контроль приложений не будет поддерживать категории приложений, доступные при использовании KSN. Категоризация приложений станет доступна при возврате к KSN.

Предоставление данных сторонним сервисам

Kaspersky Endpoint Security для Android использует сервисы Google: Firebase Cloud Messaging, Google Analytics для Firebase, Firebase Performance Monitoring и Crashlytics. Kaspersky Endpoint Security для Android использует сервис Firebase Cloud Messaging (FCM) для своевременной доставки команд на мобильные устройства и принудительной синхронизации при изменении параметров политики. Kaspersky Endpoint Security для Android использует сервисы Google Analytics для Firebase, Firebase Performance Monitoring и Crashlytics для повышения качества работы приложения и формирования "Лабораторией Касперского" эффективных маркетинговых материалов.

В этом разделе

Обмен информацией с Google Analytics для Firebase, Firebase Performance Monitoring и Crashlytics

Обмен информацией с Google Analytics для Firebase, Firebase Performance Monitoring и Crashlytics

Если при использовании плагина управления более ранней версии вы включили обмен данными с сервисом Google Analytics, Kaspersky Endpoint Security для Android Service Pack 4 Maintenance Release 3 будет выполнять обмен данными с сервисом Google Analytics для Firebase. Поддержка Google Analytics прекращена.

Kaspersky Endpoint Security для Android осуществляет обмен данными с сервисами Google Analytics для Firebase, Firebase Performance Monitoring и Crashlytics по следующим причинам:

- В целях повышения качества работы приложения.

Для обмена данными с сервисами Google Analytics для Firebase, Firebase Performance Monitoring и Crashlytics в целях повышения качества работы приложения должны быть выполнены следующие условия:

- Администратор или пользователь устройства должен прочитать и принять условия Положения о Kaspersky Security Network. Если выбран вариант, при котором Положение принимается пользователями, на главном экране приложения

отобразится уведомление с предложением принять условия Положения. Пользователи также могут принять Положение в разделе **О приложении** в настройках Kaspersky Endpoint Security для Android.

- Администратор должен разрешить передачу статистических данных в KSN в настройках групповой политики (см. ниже).

- В целях эффективного формирования "Лабораторией Касперского" маркетинговых материалов.

  Для обмена данными с сервисами Google Analytics для Firebase, Firebase Performance Monitoring и Crashlytics в целях формирования "Лабораторией Касперского" эффективных маркетинговых материалов должны быть выполнены следующие условия:

- Администратор или пользователь устройства должен прочитать и принять условия Положения об обработке данных для маркетинговых целей. Если выбран вариант, при котором Положение принимается пользователями, они могут принять условия Положения при установке приложения или в разделе **О приложении** в настройках Kaspersky Endpoint Security для Android.

- Администратор должен разрешить передачу данных в Google Analytics для Firebase, Firebase Performance Monitoring и Crashlytics в настройках групповой политики (см. ниже).

  Предоставление данных в Google Analytics для Firebase, Firebase Performance Monitoring и Crashlytics в рамках Положения об обработке данных для маркетинговых целей

  Правообладатель использует для обработки данных информационные системы третьих лиц. Обработка данных в информационных системах третьих лиц регулируется соответствующими политиками конфиденциальности таких систем. Правообладатель использует следующие сервисы для обработки перечисленных данных:

  Google Analytics для Firebase

  При использовании ПО следующие данные будут автоматически отправляться на регулярной основе в сервис Google Analytics для Firebase для их обработки для заявленных целей:

- информация о приложении: версия, идентификатор, название и идентификатор приложения в сервисе Firebase, уникальный идентификатор установки в сервисе Firebase, название магазина, из которого ПО было получено, время первого запуска ПО на устройстве;

- идентификатор установки приложения на устройство и способ установки на устройство;

- информация о регионе и языковой локализации;

- разрешение экрана устройства;
- информация о получении root -прав пользователем;
- признак установки Kaspersky Endpoint Security для Android в качестве службы Специальных возможностей;
- информация о переходах между окнами приложения, продолжительности сессии, начале и окончании сессии работы с экраном, названии экрана;
- информация о протоколе отправки данных в сервис Firebase, его версии и идентификаторе используемого метода отправки данных;
- информация о типе и параметрах события, в отношении которого происходит отправка данных;
- информация о лицензии на приложение, ее наличии, количестве устройств;
- интервалы обновления баз вредоносного ПО и синхронизации с Сервером администрирования;
- информация о консоли администрирования (Kaspersky Security Center или сторонние EMM-системы);
- идентификатор Android ID;
- идентификатор Advertising ID;
- информация о пользователе: возрастная категория и половая принадлежность пользователя, идентификатор страны проживания, список интересов пользователя;
- информация о компьютере, на котором установлено ПО: название производителя компьютера, тип компьютера, модель устройства, версия и информация о языковой локализации ОС, информация о первом запущенном приложении за последнюю неделю и ранее.

Передача данных в сервис Google Analytics для Firebase осуществляется по защищенному каналу. Информация об условиях обработки данных в сервисе Google Analytics для Firebase доступна по адресу https://firebase.google.com/support/privacy.

Firebase Performance Monitoring

При использовании ПО следующие данные будут автоматически отправляться на регулярной основе в сервис Firebase Performance Monitoring для их обработки для заявленных целей:

- уникальный идентификатор установки;

- название пакета приложения;
- версия установленного ПО;
- уровень и статус заряда батареи;
- оператор связи;
- признак работы ПО в фоновом режиме;
- регион;
- IP-адрес;
- код языка устройства;
- информация о радио- и интернет-соединении;
- идентификатор-псевдоним экземпляра ПО;
- ОЗУ и размер диска;
- признак того, что на устройстве выполнена процедура рутинга или джейлбрейка;
- уровень сигнала;
- продолжительность автоматической трассировки;
- информация о сети и сопутствующая информация ответа: код ответа, размер полезной нагрузки в байтах, время отклика;
- описание устройства.

Передача данных в сервис Firebase Performance Monitoring осуществляется по защищенному каналу. Информация об условиях обработки данных в сервисе Firebase Performance Monitoring доступна по адресу https://firebase.google.com/support/privacy.

Crashlytics

При использовании ПО следующие данные будут автоматически отправляться на регулярной основе в сервис Crashlytics для их обработки для заявленных целей:

- идентификатор ПО;
- версия установленного ПО;
- признак работы ПО в фоновом режиме;

- архитектура ЦП;
- уникальный идентификатор события;
- дата и время события;
- модель устройства;
- объем полного и используемого дискового пространства;
- название и версия ОС;
- объем полной и используемой оперативной памяти;
- признак того, что на устройстве выполнена процедура рутинга;
- ориентация экрана в момент события;
- производитель продукта / устройства;
- уникальный идентификатор установки;
- версия отправляемой статистики;
- тип исключения ПО;
- текст сообщения об ошибке;
- признак того, что исключение ПО вызвано исключением на вложенном уровне;
- идентификатор потока;
- признак того, что фрейм стал причиной ошибки ПО;
- признак того, что выполнение потока привело к неожиданному завершению работы ПО;
- данные о сигнале, который привел к неожиданному завершению работы ПО: название сигнала, код сигнала, адрес сигнала;
- для каждого фрейма, ассоциированного с потоком, исключением или ошибкой: имя файла фрейма, номер строки файла фрейма, отладочные символы, адрес и смещение в бинарном образе, отображаемое имя библиотеки, содержащей фрейм, тип фрейма, признак того, что фрейм стал причиной ошибки;
- идентификатор ОС;
- идентификатор проблемы, связанной с событием;

- информация о событиях, предшествующих неожиданному завершению работы ПО: идентификатор события, дата и время события, тип события и значение;
- значения регистра ЦП;
- тип события и значение.

Передача данных в сервис Crashlytics осуществляется по защищенному каналу. Информация об условиях обработки данных в сервисе Crashlytics доступна по адресу https://firebase.google.com/terms/crashlytics-app-distribution-data-processing-terms.

Предоставление вышеуказанной информации для обработки в маркетинговых целях является добровольным.

Чтобы запретить обмен данными с сервисами Google Analytics для Firebase, Firebase Performance Monitoring и Crashlytics, выполните следующие действия:

1. Откройте окно настройки параметров политики управления мобильными устройствами, на которых установлено приложение Kaspersky Endpoint Security для Android.
2. В политике, в окне **Свойства** выберите раздел **Дополнительно**.
3. В разделе **Передача данных** снимите флажок **Разрешить передачу данных, чтобы помочь улучшить качество работы, интерфейс и производительность приложения**.
4. Нажмите на кнопку **Применить**, чтобы сохранить внесенные изменения.

   Параметры на мобильном устройстве будут изменены после очередной синхронизации устройства с Kaspersky Security Center.

Настройка KNOX-контейнеров

Этот раздел содержит информацию о работе с KNOX-контейнерами на Samsung-устройствах под управлением операционной системы Android.

Использование KNOX-контейнеров доступно только на Samsung-устройствах под управлением операционной системы Android версии 6 или выше.

В этом разделе

О KNOX-контейнере

KNOX-контейнер – безопасная среда на устройстве пользователя с отдельным рабочим столом, панелью запуска, приложениями, виджетами. KNOX-контейнер позволяет изолировать корпоративные приложения и данные от персональных. KNOX-контейнер является компонентом мобильного решения Samsung KNOX.

Samsung KNOX – мобильное решение для настройки и защиты мобильных устройств Samsung под управлением операционной системы Android. Подробная информация о Samsung KNOX приведена на *сайте Службы технической поддержки Samsung*.

KNOX-контейнеры позволяют разделить персональные и корпоративные данные на мобильном устройстве. Например, невозможно отправить файл, расположенный в KNOX-контейнере, с помощью личного почтового ящика. Рекомендуется разворачивать KNOX-контейнер, если для работы с корпоративными данными используются личные мобильные устройства сотрудников.

Для использования KNOX-контейнеров требуется активировать Samsung KNOX. После синхронизации устройства с Kaspersky Security Center пользователю мобильного устройства будет предложено установить KNOX-контейнер. Перед установкой KNOX-контейнера пользователь должен принять условия Лицензионного соглашения от компании Samsung.

После установки KNOX-контейнера на рабочий стол мобильного устройства будет добавлен значок KNOX  . Или рабочая область будет добавлена в список приложений на мобильном устройстве. Для работы с корпоративными данными пользователю нужно запустить приложение из KNOX-контейнера.

Kaspersky Endpoint Security для Android не устанавливается в KNOX-контейнер и не защищает корпоративные данные. Kaspersky Endpoint Security для Android не обнаруживает загрузку вредоносных файлов и не блокирует вредоносные сайты в KNOX-контейнере. В KNOX-контейнере невозможно контролировать загрузку приложений и запретить использование камеры. Kaspersky Endpoint Security для Android защищает только личные данные. Корпоративные данные можно

защитить с помощью инструментов Samsung KNOX. Подробная информация о Samsung KNOX приведена на *сайте Службы технической поддержки Samsung*.

Активация Samsung KNOX

Чтобы использовать KNOX-контейнер на мобильном устройстве пользователя, требуется активировать Samsung KNOX. Процедура активации Samsung KNOX зависит от версии Kaspersky Endpoint Security для Android, установленной на устройствах пользователей:

- Если на устройствах установлена текущая версия Kaspersky Endpoint Security для Android, для активации Samsung KNOX ключи не требуются.
- Если на устройствах установлена устаревшая версия Kaspersky Endpoint Security для Android (10.8.3.174 или ниже), необходимо получить ключ KNOX License Manager (KLM-ключ) от Samsung. *Ключ KNOX License Manager* – уникальный код, который используется системой лицензирования Samsung KNOX. Более подробная информация о KLM-ключе приведена на сайте технической поддержки Samsung KNOX.

Использование KNOX-контейнеров возможно только на Samsung-устройствах.

Чтобы активировать Samsung KNOX, выполните следующие действия:

1. В дереве консоли в папке **Управляемые устройства** выберите группу администрирования, в которую входят Android-устройства.
2. В рабочей области группы выберите закладку **Политики**.
3. Откройте окно свойств политики двойным щелчком мыши по любому столбцу.

В течение 15 минут выполните следующие действия. По истечении этого времени при сохранении изменений политики может возникнуть ошибка.

4. В политике, в окне **Свойства** выберите раздел **Управление Samsung KNOX → KNOX-контейнеры**.
5. В поле **Ключ KNOX License Manager** укажите следующие данные:

- Если на устройствах установлена текущая версия Kaspersky Endpoint Security для Android, введите любой символ.

- Если на устройствах установлена устаревшая версия Kaspersky Endpoint Security для Android (10.8.3.174 или ниже), введите KLM-ключ, полученный от Samsung.

6. Установите атрибут "замок" в закрытое положение  .

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

   Samsung KNOX будет активирован после очередной синхронизации устройства с Kaspersky Security Center. Пользователю будет предложено принять условия Лицензионного соглашения от компании Samsung и установить KNOX-контейнер.

Чтобы деактивировать Samsung KNOX, выполните следующие действия:

1. В дереве консоли в папке **Управляемые устройства** выберите группу администрирования, в которую входят Android-устройства.

2. В рабочей области группы выберите закладку **Политики**.

3. Откройте окно свойств политики двойным щелчком мыши по любому столбцу.

   В течение 15 минут выполните следующие действия. По истечении этого времени при сохранении изменений политики может возникнуть ошибка.

4. В политике, в окне **Свойства** выберите раздел **Управление Samsung KNOX → KNOX-контейнеры**.

5. Удалите значение, указанное в поле **Ключ KNOX License Manager**.

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

   Samsung KNOX будет деактивирован после очередной синхронизации устройства с Kaspersky Security Center. Доступ в KNOX-контейнер будет заблокирован.

Ограничения Samsung KNOX

- Использование KNOX-контейнеров возможно только на Samsung-устройствах.

- На Samsung-устройствах с поддержкой KNOX 2.6, 2.7 и 2.7.1 в KNOX-контейнере не работает Веб-Фильтр и Контроль приложений. Проблема связана с отсутствием необходимых прав в KNOX-контейнере (служба Специальных возможностей). На устройствах с поддержкой KNOX 2.8 и выше все компоненты приложения работают без ограничений.

- Kaspersky Endpoint Security для Android версии ниже, чем Service Pack 4 Maintenance Release 3 Update 2 может работать нестабильно на устройствах Samsung с операционной системой Android 10 из-за обновлений Samsung KNOX. Рекомендуется обновить Kaspersky Endpoint Security для Android до версии Service Pack 4 Maintenance Release 3 Update 2.

Настройка Сетевого экрана в KNOX

Для контроля сетевых соединений в KNOX-контейнере следует настроить параметры Сетевого экрана.

Чтобы настроить Сетевой экран в KNOX-контейнере, выполните следующие действия:

1. В дереве консоли в папке **Управляемые устройства** выберите группу администрирования, в которую входят Android-устройства.

2. В рабочей области группы выберите закладку **Политики**.

3. Откройте окно свойств политики двойным щелчком мыши по любому столбцу.

> В течение 15 минут выполните следующие действия. По истечении этого времени при сохранении изменений политики может возникнуть ошибка.

4. В политике, в окне **Свойства** выберите раздел **Управление Samsung KNOX → KNOX-контейнеры**.

5. В блоке **Сетевой экран** нажмите на кнопку **Настроить**.

   Откроется окно **Сетевой экран**.

6. Выберите режим работы Сетевого экрана:

- Чтобы разрешить все входящие и исходящие соединения, переместите ползунок в положение **Разрешать все**.

- Чтобы блокировать любую сетевую активность, кроме приложений из списка исключений, переместите ползунок в положение **Блокировать все, кроме исключений**.

7. Если вы выбрали режим работы Сетевого экрана **Блокировать все, кроме исключений**, сформируйте список исключений:

α. Нажмите на кнопку **Добавить**.

   Откроется окно **Исключение для Сетевого экрана**.

β. В поле **Название приложения** введите название мобильного приложения.

χ. В поле **Имя пакета** введите системное имя пакета мобильного приложения (например, `com.mobileapp.example`).

δ. Нажмите кнопку **ОК**.

Нажмите на кнопку **Применить**, чтобы сохранить внесенные изменения.

Параметры на мобильном устройстве будут изменены после очередной синхронизации устройства с Kaspersky Security Center.

В начало

Настройка почтового ящика Exchange в KNOX

Для работы с корпоративной почтой, контактами и календарем в KNOX-контейнере следует настроить параметры почтового ящика Exchange (доступно только в Android 9 и ниже).

Чтобы настроить почтовый ящик Exchange в KNOX-контейнере, выполните следующие действия:

1. В дереве консоли в папке **Управляемые устройства** выберите группу администрирования, в которую входят Android-устройства.
2. В рабочей области группы выберите закладку **Политики**.
3. Откройте окно свойств политики двойным щелчком мыши по любому столбцу.

В течение 15 минут выполните следующие действия. По истечении этого времени при сохранении изменений политики может возникнуть ошибка.

4. В политике, в окне **Свойства** выберите раздел **Управление Samsung KNOX → KNOX-контейнеры**.
5. В блоке **Exchange ActiveSync** нажмите на кнопку **Настроить**.

Откроется окно **Параметры почтового сервера Exchange**.

6. В поле **Адрес сервера** введите IP-адрес или DNS-имя сервера, на котором размещен почтовый сервер.
7. В поле **Домен** введите имя домена пользователя мобильного устройства в корпоративной сети.

8. В раскрывающемся списке **Периодичность синхронизации** выберите желаемый период синхронизации мобильного устройства с сервером Microsoft Exchange.

9. Чтобы использовать транспортный протокол передачи данных SSL, установите флажок **Использовать SSL-соединение**.

10. Чтобы использовать цифровые сертификаты для защиты передачи данных между мобильным устройством и сервером Microsoft Exchange, установите флажок **Проверять сертификат сервера**.

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

    Параметры на мобильном устройстве будут изменены после очередной синхронизации устройства с Kaspersky Security Center.

Использование приложения Kaspersky Endpoint Security для Android

В этом разделе справки описаны функции и действия, доступные пользователям приложения Kaspersky Endpoint Security для Android.

Статьи в этом разделе содержат описание всех параметров, доступных и видимых на мобильных устройствах. Фактический внешний вид и работа приложения зависит от используемой системы удаленного администрирования и от того, как администратор настроил устройство в соответствии с требованиями корпоративной безопасности. Некоторые функции и параметры приложения, описанные в этом разделе, могут не соответствовать тем, что вы увидите при работе приложением. При возникновении вопросов о работе приложения на вашем конкретном устройстве, обратитесь к администратору.

В этом разделе

Возможности приложения

Kaspersky Endpoint Security обладает следующими основными возможностями.

Защита от вирусов и других вредоносных приложений

Для защиты от вирусов и других вредоносных приложений используется компонент Защита от вредоносного ПО.

Защита от вредоносного ПО выполняет следующие функции:

- проверяет на наличие угроз все устройство, установленные приложения или выбранные папки;
- защищает устройство в режиме реального времени;
- проверяет новые установленные приложения до их первого запуска;
- обновляет базы вредоносного ПО.

Если на мобильном устройстве установлено приложение, выполняющее сбор и отправку информации на обработку, Kaspersky Endpoint Security для Android может классифицировать такое приложение как вредоносное.

Защита данных при потере или краже устройств

Для защиты информации от попадания в чужие руки, а также для поиска устройства при его потере или краже используется компонент Анти-Вор.

Анти-Вор позволяет дистанционно выполнить следующие действия:

- Заблокировать устройство.

> Чтобы злоумышленник не имел возможности разблокировать устройство, на мобильных устройствах под управлением операционной системы Android версии 7.0 и выше Kaspersky Endpoint Security должен быть включен в качестве службы Специальных возможностей.

- Включить на устройстве громкую сирену, даже если на устройстве выключен звук.
- Получить координаты местоположения устройства.
- Удалить данные, хранящиеся на устройстве.
- Сбросить настройки до заводских.
- Незаметно сделать фотографии человека, который использует ваше устройство.

> Для работы Анти-Вора Kaspersky Endpoint Security должен быть включен в качестве администратора устройства. Если вы не предоставили права администратора устройства во время первоначальной настройки приложений, предоставьте Kaspersky Endpoint Security права администратора с помощью соответствующего уведомления или в настройках устройства (**Настройки Android → Безопасность → Администраторы устройства**).

Защита от интернет-угроз

Для защиты от интернет-угроз используется компонент Веб-Фильтр.

Веб-Фильтр блокирует вредоносные веб-сайты, цель которых – распространить вредоносный код, а также фишинговые веб-сайты, цель которых – украсть ваши конфиденциальные данные и получить доступ к вашим финансовым счетам. Веб-Фильтр проверяет веб-сайты перед открытием, используя облачную службу Kaspersky Security Network.

Контроль приложений

В соответствии с требованиями корпоративной безопасности *администратор системы удаленного администрирования* (далее также "администратор") формирует списки рекомендованных, запрещенных и обязательных приложений. Для установки рекомендованных и обязательных приложений, их обновления, а также для удаления запрещенных приложений используется компонент Контроль приложений.

Контроль приложений позволяет вам устанавливать на ваше устройство рекомендованные и обязательные приложения с помощью прямой ссылки на дистрибутив или ссылки на Google Play. С помощью Контроля приложений вы можете удалять запрещенные приложения, которые не удовлетворяют требованиям корпоративной безопасности.

Для работы Контроля приложений Kaspersky Endpoint Security должен быть установлен в качестве службы Специальных возможностей. Если вы не включили службу во время работы Мастера первоначальной настройки приложения, включите Kaspersky Endpoint Security в качестве службы Специальных возможностей с помощью соответствующего уведомления или в настройках устройства (**Настройки Android** → **Специальные возможности** → **Службы**).

Контроль соответствия

Компонент Контроль соответствия автоматически проверяет соответствие устройства требованиям корпоративной безопасности. Если ваше устройство не соответствует требованиям корпоративной безопасности, приложение показывает уведомление со следующей информацией:

- причина несоответствия (например, на устройстве были обнаружены запрещенные приложения или базы вредоносного ПО устарели);
- время, за которое вы должны устранить несоответствие (например, 24 часа);
- действие, которое будет выполнено с устройством, если вы не устраните несоответствие в течение указанного времени (например, блокировка устройства);
- вариант действия для устранения несоответствия устройства требованиям корпоративной безопасности.

Обзор главного окна

Вид главного окна для разных разрешений экрана незначительно отличается.

В главном окне отображается общий статус защиты вашего устройства. Этот статус определяет цвет окна:

- Зеленый цвет указывает на оптимальный уровень защиты устройства.
- Красный цвет указывает на критические проблемы с безопасностью устройства.

  В главном окне приложения вы также можете:

- Просматривать уведомления, нажав на кнопку в правом верхнем углу. Они информируют вас о проблемах безопасности, проблемах в работе приложения, соответствии требованиям корпоративной безопасности и статусе вашей лицензии.
- Переходить между главным окном и настройками приложения с помощью кнопок внизу.

Значок в строке состояния

После завершения мастера первого запуска приложения значок Kaspersky Endpoint Security появляется в строке состояния.

Значок служит индикатором работы приложения и обеспечивает доступ к главному окну Kaspersky Endpoint Security.

Значок служит индикатором работы Kaspersky Endpoint Security и отражает состояние защиты вашего устройства:

 – Устройство защищено.

 – Есть проблемы с защитой (например, базы вредоносного ПО устарели или установлено новое непроверенное приложение).

Проверка устройства

Защита от вредоносного ПО имеет ряд ограничений:

- При работе Защиты от вредоносного ПО в рабочем профиле (Приложения с "портфелем", Настройка рабочего профиля Android) невозможно автоматически устранить угрозу, обнаруженную во внешней памяти устройства (например, на SD-карте). У Kaspersky Endpoint Security для Android в рабочем профиле нет доступа к внешней памяти. Информация об обнаруженных объектах отображается в уведомлениях приложения. Для устранения обнаруженных во внешней памяти объектов необходимо удалить файл вручную и запустить проверку устройства повторно.

- Из-за технических ограничений Kaspersky Endpoint Security для Android не может проверять файлы размером 2 ГБ и более. Во время проверки приложение пропускает такие файлы и не уведомляет вас, если такие файлы были пропущены.

- На устройствах с операционной системой Android 11 или выше приложение Kaspersky Endpoint Security для Android не может сканировать папки Android/data и Android/obb и обнаруживать в них вредоносные программы из-за технических ограничений.

Чтобы запустить проверку устройства, выполните следующие действия:

1. В главном окне Kaspersky Endpoint Security нажмите **Настройки** → **Настройки приложения** → **Защита от вредоносного ПО** → **Запустить проверку**.

2. Выберите область проверки устройства:

- **Проверить все устройство**. Приложение проверит всю файловую систему устройства.

- **Проверить установленные приложения**. Приложение проверит только установленные приложения.

- **Выборочная проверка**. Приложение проверит выбранную папку или отдельный файл. Вы можете выбрать отдельный объект (папку или файл) или один из следующих разделов памяти устройства:

- **Память устройства**. Память всего устройства, доступная для чтения. В эту область также входит системный раздел памяти, на котором хранятся файлы операционной системы.

- **Внутренняя память**. Раздел памяти устройства, предназначенный для установки приложений, хранения медиаконтента, документов и других файлов.

- **Внешняя память**. Память внешней SD-карты. Если внешняя SD-карта не установлена, вариант скрыт.

Доступ к настройкам поиска вредоносного ПО может быть ограничен вашим администратором.

Чтобы настроить поиск вредоносного ПО, выполните следующие действия:

1. В главном окне Kaspersky Endpoint Security нажмите **Настройки** → **Настройки приложения** → **Защита от вредоносного ПО** → **Настройки проверки**.

2. Если вы хотите, чтобы во время проверки приложение обнаруживало рекламные приложения и приложения, которые могут быть использованы злоумышленниками

для нанесения вреда устройству или вашим данным, включите переключатель **Реклама, автодозвон и другое**.

3. Нажмите **Действие при обнаружении угрозы** и выберите действие, выполняемое приложением по умолчанию:

- **Карантин**

  Карантин хранит файлы в упакованном виде, в котором они не могут нанести вред устройству. Карантин предоставляет возможность удалить или восстановить файлы, помещенные в изолированное хранилище.

- **Запросить действие**

  Приложение предложит вам выбрать действие для каждого обнаруженного объекта: пропустить, поместить на карантин или удалить. При обнаружении нескольких объектов вы можете применить выбранное действие ко всем объектам.

- **Удалить**

  Обнаруженные объекты будут удалены автоматически. Никаких дополнительных действий не требуется. Перед удалением Kaspersky Endpoint Security отобразит временное уведомление об обнаружении объекта.

- **Пропустить**

  Если обнаруженные объекты были пропущены, Kaspersky Endpoint Security предупреждает вас о проблемах в защите устройства. Для каждой пропущенной угрозы приведены действия, которые вы можете выполнить для ее устранения. Список пропущенных объектов может измениться, например, если вредоносный файл был удален или перемещен. Чтобы получить актуальный список угроз, запустите полную проверку устройства. Для надежной защиты ваших данных устраните все обнаруженные объекты.

  > Информация об обнаруженных угрозах и выполненных над ними действиях записывается в отчеты приложения (**Настройки** → **Отчеты**). Вы можете выбрать отображение отчетов по работе Защиты от вредоносного ПО.

Проверка устройства по расписанию

Защита от вредоносного ПО имеет ряд ограничений:

- При работе Защиты от вредоносного ПО в рабочем профиле (Приложения с "портфелем", Настройка рабочего профиля Android) невозможно автоматически устранить угрозу, обнаруженную во внешней памяти устройства (например, на SD-карте). У Kaspersky Endpoint Security для Android в рабочем профиле нет доступа к внешней памяти. Информация об обнаруженных объектах отображается в уведомлениях приложения. Для устранения обнаруженных во внешней памяти

объектов необходимо удалить файл вручную и запустить проверку устройства повторно.

- Из-за технических ограничений Kaspersky Endpoint Security для Android не может проверять файлы размером 2 ГБ и более. Во время проверки приложение пропускает такие файлы и не уведомляет вас, если такие файлы были пропущены.

- На устройствах с операционной системой Android 11 или выше приложение Kaspersky Endpoint Security для Android не может сканировать папки Android/data и Android/obb и обнаруживать в них вредоносные программы из-за технических ограничений.

Чтобы настроить расписание полной проверки устройства, выполните следующие действия:

1. В главном окне Kaspersky Endpoint Security нажмите **Настройки** → **Настройки приложения** → **Защита от вредоносного ПО** → **Настройки проверки**.

2. Нажмите **Расписание** и выберите периодичность запуска полной проверки:

- **Раз в неделю**

- **Раз в день**

- **Выключено**

- **После обновления баз**

3. Нажмите **День запуска** и выберите день недели, в который требуется запускать полную проверку.

4. Нажмите **Время запуска** и укажите время запуска полной проверки.

Полная проверка устройства будет запускаться согласно расписанию.

Если устройство находится в режиме экономии заряда батареи, приложение может выполнить эту задачу позже, чем указано. Чтобы обеспечить своевременную реакцию устройств KES на Android на команды администратора, включите использование Google Firebase Cloud Messaging.

Изменение режима защиты

Постоянная защита позволяет обнаруживать угрозы в открытых файлах, а также проверять приложения во время их установки на устройство в режиме реального времени. Для обеспечения защиты в автоматическом режиме используются базы вредоносного ПО и облачная служба Kaspersky Security Network (Облачная защита).

Чтобы изменить режим защиты устройства, выполните следующие действия:

1. В главном окне Kaspersky Endpoint Security нажмите **Настройки → Настройки приложения → Защита от вредоносного ПО → Режим постоянной защиты**.

2. Выберите режим защиты устройства:

- **Выключена**. Защита выключена.

- **Рекомендуемый**. В процессе поиска вредоносного ПО проверяются только установленные приложения и файлы из папки "Загрузки". Защита от вредоносного ПО проверяет новые приложения один раз, сразу после их установки.

- **Расширенный**. Защита от вредоносного ПО проверяет на наличие вредоносных объектов все файлы на устройстве при любом действии с ними (например, сохранении, перемещении или изменении). Также Защита от вредоносного ПО проверяет новые приложения сразу после их установки.

  Информация о действующем режиме защиты отображается под описанием компонента.

Доступ к настройкам постоянной защиты может быть ограничен вашим администратором.

Чтобы включить Облачную защиту (KSN), выполните следующие действия:

1. Нажмите **Настройки → Настройки приложения → Защита от вредоносного ПО** в главном окне Kaspersky Endpoint Security.

2. Включите переключатель **Облачная защита (KSN)**.

Переключатель **Облачная защита (KSN)** управляет использованием Kaspersky Security Network только для постоянной защиты устройства. Если флажок выключен, Kaspersky Endpoint Security продолжает использовать KSN для работы других компонентов приложения.

В результате приложение получает доступ к оперативной базе знаний "Лаборатории Касперского" о репутации файлов и приложений. Проверка производится на угрозы, информация о которых еще не вошла в базы вредоносного ПО, но уже содержится в KSN. Облачная служба Kaspersky Security Network обеспечивает полноценную работу Защиты от вредоносного

ПО и снижает вероятность ложных срабатываний. Полностью выключить использование Kaspersky Security Network может только ваш администратор.

Чтобы настроить постоянную защиту, выполните следующие действия:

1. В главном окне Kaspersky Endpoint Security нажмите **Настройки** → **Настройки приложения** → **Защита от вредоносного ПО** → **Настройки проверки**.

2. Если вы хотите, чтобы во время проверки приложение обнаруживало рекламные приложения и приложения, которые могут быть использованы злоумышленниками для нанесения вреда устройству или вашим данным, включите переключатель **Реклама, автодозвон и другое**.

3. Нажмите **Действие при обнаружении угрозы** и выберите действие, выполняемое приложением по умолчанию:

- **Карантин**

  Карантин хранит файлы в упакованном виде, в котором они не могут нанести вред устройству. Карантин предоставляет возможность удалить или восстановить файлы, помещенные в изолированное хранилище.
- **Удалить**

  Обнаруженные объекты будут удалены автоматически. Никаких дополнительных действий не требуется. Перед удалением Kaspersky Endpoint Security отобразит временное уведомление об обнаружении объекта.
- **Пропустить**

  Если обнаруженные объекты были пропущены, Kaspersky Endpoint Security предупреждает вас о проблемах в защите устройства. Для каждой пропущенной угрозы приведены действия, которые вы можете выполнить для ее устранения. Список пропущенных объектов может измениться, например, если вредоносный файл был удален или перемещен. Чтобы получить актуальный список угроз, запустите полную проверку устройства. Для надежной защиты ваших данных устраните все обнаруженные объекты.

  Информация об обнаруженных угрозах и выполненных над ними действиях записывается в отчеты приложения (**Настройки** → **Отчеты**). Вы можете выбрать отображение отчетов по работе Защиты от вредоносного ПО.

Обновление баз вредоносного ПО

Чтобы обновить базы вредоносного ПО:

В главном окне Kaspersky Endpoint Security нажмите **Настройки** → **Настройки приложения** → **Защита от вредоносного ПО** → **Запустить обновление баз**.

Обновление баз по расписанию

Приложение может автоматически обновлять базы вредоносного ПО по заданному расписанию.

Чтобы настроить расписание обновления, выполните следующие действия:

1. В главном окне Kaspersky Endpoint Security нажмите **Настройки** → **Настройки приложения** → **Защита от вредоносного ПО** → **Настройки обновления баз**.
2. Нажмите **Расписание** и выберите периодичность запуска обновления:

- **Раз в неделю**
- **Раз в день**
- **Выключено**

3. Нажмите **День запуска** и выберите день недели, в который нужно запускать обновление.
4. Нажмите **Время запуска** и укажите время запуска обновления.

   Обновление баз вредоносного ПО будет запускаться согласно расписанию.

Если устройство находится в режиме экономии заряда батареи, приложение может выполнить эту задачу позже, чем указано. Чтобы обеспечить своевременную реакцию устройств KES на Android на команды администратора, включите использование Google Firebase Cloud Messaging.

Действия в случае кражи или потери устройства

В случае кражи или потери устройства обратитесь к системному администратору. Администратор дистанционно запустит на устройстве функции Анти-Вора в соответствии с требованиями корпоративной безопасности.

Если на устройство отправлена команда сброса настроек до заводских, контроль над устройством будет потерян, и остальные команды Анти-Вора выполняться не будут.

Веб-Фильтр

Для включения Веб-Фильтра должны быть выполнены следующие условия:

- Положение об обработке данных в целях использования Веб-Фильтра (Положение о Веб-Фильтре) должно быть принято. Kaspersky Endpoint Security использует Kaspersky Security Network (KSN) для проверки веб-сайтов. Положение о Веб-Фильтре содержит условия обмена данными с KSN.

  Администратор вашей сети может принять Положение о Веб-Фильтре в Kaspersky Security Center. В этом случае вам не потребуется выполнять никаких действий.

  Если администратор вашей сети не принял Положение о Веб-Фильтре и направил вам запрос на принятие Положения, прочитайте и примите Положение о Веб-Фильтре в настройках приложения.

  Если администратор вашей сети не принял Положение о Веб-Фильтре, Веб-Фильтр будет недоступен.

  Веб-Фильтр на Android-устройствах поддерживается только браузерами Google Chrome, HUAWEI Browser, Samsung Internet Browser и Яндекс Браузер.

  Если приложение Kaspersky Endpoint Security для Android в режиме device owner не установлено в качестве службы Специальных возможностей, Веб-Фильтр поддерживается только браузером Google Chrome и проверяет только домен сайта. Чтобы Веб-Фильтр поддерживался другими браузерами (Samsung Internet Browser, Яндекс Браузер и HUAWEI Browser), приложение Kaspersky Endpoint Security должно быть включено в качестве службы Специальных возможностей. Это также позволит использовать функцию Custom Tabs.

  Функция Custom Tabs поддерживается браузерами Google Chrome, HUAWEI Browser и Samsung Internet Browser.

  В браузерах HUAWEI Browser, Samsung Internet Browser и Яндекс Браузер Веб-Фильтр не блокирует сайты на мобильном устройстве, если используется рабочий профиль и установлен флажок Включить Веб-Фильтр только в рабочем профиле.

  Для постоянного использования Веб-Фильтра для проверки сайтов во время работы в интернете, назначьте Google Chrome, HUAWEI Browser, Samsung Internet Browser или Яндекс Браузер браузером по умолчанию.

  Чтобы назначить поддерживаемый браузер браузером по умолчанию и использовать Веб-Фильтр для постоянной проверки веб-сайтов, выполните следующие действия:

1. В главном окне Kaspersky Endpoint Security нажмите **Настройки** → **Настройки приложения** → **Веб-Фильтр**.

2. Включите переключатель **Веб-Фильтр**.

3. Нажмите **Установить браузер по умолчанию**.

   Эта кнопка отображается, если Веб-Фильтр включен, но поддерживаемый браузер не установлен в качестве браузера по умолчанию.

   Запустится мастер выбора браузера по умолчанию.

4. Следуйте указаниям мастера.

   В результате работы мастера Google Chrome, HUAWEI Browser или Samsung Internet Browser будет назначен браузером по умолчанию. Веб-Фильтр будет постоянно проверять веб-сайты во время работы в интернете.

Получение сертификата

Чтобы получить сертификат для доступа к ресурсам сети организации, выполните следующие действия:

1. В главном окне Kaspersky Endpoint Security нажмите **Настройки** → **Настройки приложения** → **Дополнительно** → **Получение сертификата**.

2. Укажите ваши учетные данные в сети организации. Логин должен иметь один из следующих форматов:

- `userPrincipalName@DNSDomainName`
- `sAMAccountName`
- `sAMADomain\sAMAccountName`

   Для получения дополнительных сведений об этих атрибутах перейдите на веб-сайт Microsoft в раздел Техническая документация. Обратитесь к вашему администратору для получения подробной информации.

3. Если вы получили от администратора одноразовый пароль, установите флажок **Одноразовый пароль** и введите полученный пароль.

   Запустится мастер установки сертификата.

4. Следуйте указаниям мастера.

Синхронизация с Kaspersky Security Center

Синхронизация мобильного устройства с системой удаленного администрирования Kaspersky Security Center необходима для защиты и

настройки вашего устройства в соответствии с требованиями корпоративной безопасности. Синхронизация устройства с Kaspersky Security Center выполняется автоматически. Можно также запускать синхронизацию вручную. После первой синхронизации ваше устройство добавляется в список мобильных устройств, управляемых через Kaspersky Security Center. После этого администратор может настраивать ваше устройство в соответствии с требованиями корпоративной безопасности.

Вы можете задать значения параметров синхронизации во время работы мастера первоначальной настройки или в настройках Kaspersky Endpoint Security. Параметры синхронизации требуется настраивать, если вы установили Kaspersky Endpoint Security с помощью Google Play. Для получения значений параметров синхронизации обратитесь к администратору.

Изменяйте параметры синхронизации устройства с системой удаленного администрирования Kaspersky Security Center только по указанию администратора.

Чтобы синхронизировать устройство с Kaspersky Security Center, выполните следующие действия:

1. В главном окне Kaspersky Endpoint Security нажмите **Настройки** → **Настройки приложения** → **Синхронизация**.

2. В разделе **Параметры синхронизации** укажите значения следующих параметров:

- **Сервер**
- **Порт**
- **Группа**
- **Адрес корпоративной электронной почты**

Параметры синхронизации могут быть скрыты администратором.

3. Нажмите **Синхронизировать**.

Активация Kaspersky Endpoint Security для Android без использования Kaspersky Security Center

В большинстве случаев установленное на устройстве приложение Kaspersky Endpoint Security для Android активируется администратором централизованно с помощью системы удаленного администрирования Kaspersky Security Center. Если ваше устройство не подключено к Kaspersky Security Center, вы можете ввести код активации вручную. Для получения кода активации обратитесь к администратору.

Активируйте приложение вручную только по указанию администратора.

Чтобы ввести код активации, выполните следующие действия:

1. В сообщении об ошибке, в котором говорится, что срок действия вашей лицензии скоро истечет или уже истек, и что ваше устройство не подключено к Серверу администрирования, нажмите **Активировать**.

2. В окне активации введите код активации, предоставленный администратором, и нажмите **Активировать**.

3. Если код активации правильный, отображается уведомление об активации приложения, а также дата истечения срока действия лицензии.

   Приложение Kaspersky Endpoint Security для Android на вашем устройстве будет активировано.

Установка приложения в режиме device owner

Режим device owner – это режим работы корпоративных Android-устройств. Этот режим позволяет администратору осуществлять полный контроль над устройством и настраивать множество функций.

Приложение Kaspersky Endpoint Security для Android можно установить одним из следующих способов.

- С помощью QR-кода, сгенерированного в Kaspersky Security Center, для установки приложения на устройства под управлением Android версии 7 и выше.

- С помощью пакета установки, загруженного из Kaspersky Security Center, и выполнения команды в ADB. Этот способ подходит для установки приложения на устройства под управлением Android версий 5–6 и на устройства под управлением более поздних версий Android, на которых не установлен сканер QR-кода.

В этом разделе

Настройка приложения в режиме device owner на устройствах с Android версий 5–6

Настройка приложения в режиме device owner на устройствах с Android версии 7 и выше

Для развертывания приложения в режиме device owner необходимо сбросить настройки устройства до заводских и установить приложение, используя QR-код, сгенерированный в Kaspersky Security Center. QR-код содержит все необходимые данные для настройки приложения.

Чтобы установить Kaspersky Endpoint Security для Android на устройство в режиме device owner:

1. Сбросьте настройки устройства до заводских.

   Устройство перезагрузится, откроется экран приветствия.
2. Шесть раз нажмите на пустое пространство на экране приветствия.

   Откроется утилита для считывания QR-кодов.
3. Отсканируйте QR-код, сгенерированный в Kaspersky Security Center, для установки приложения.
4. Выполните первоначальную настройку устройства. Операционная система установит приложение Kaspersky Endpoint Security для Android в фоновом режиме.

   После завершения настройки устройства на нем запустится Kaspersky Endpoint Security для Android.

   На устройствах Xiaomi под управлением Android 12 автоматический запуск Kaspersky Endpoint Security для Android не предусмотрен. Запустите приложение вручную.
5. Активируйте приложение, следуя указаниям мастера первоначальной настройки.

Если для развертывания приложения используется пакет установки, загруженный из Kaspersky Security Center, после сброса настроек устройства до заводских и сканирования QR-кода на экране устройства может появиться сообщение **Заблокировано Play Защитой**. Это связано с тем, что сертификат подписи пакета установки отличается от указанного в Google Play. Для продолжения установки необходимо нажать кнопку **Все равно установить**. При нажатии кнопки **OK** процесс установки будет прерван, а настройки устройства будут сброшены до заводских.

Приложение Kaspersky Endpoint Security для Android будет установлено и активировано на устройстве в режиме device owner.

Настройка приложения в режиме device owner на устройствах с Android версий 5–6

На устройствах с Android версий 5–6 процедура настройки режима device owner отличается от стандартной. Необходимо предварительно настроить устройство, установить приложение и настроить дополнительные параметры с помощью Android Debug Bridge (ADB).

Этот способ подходит для установки приложения на устройства под управлением других версий Android, а также на устройства без сканера QR-кода.

Предварительная настройка

Для создания пакета установки в Консоли администрирования в разделе **Тип устройства** выберите **Персональное устройство**, а на странице **Способ установки Kaspersky Endpoint Security для Android** выберите **Загрузить пакет установки из Kaspersky Security Center**. Подробнее см. в разделе Установка Kaspersky Endpoint Security для Android на персональные устройства.

Развертывание

Чтобы развернуть Kaspersky Endpoint Security для Android на устройстве с Android версий 5–6 в режиме device owner, выполните следующие действия:

1. Сбросьте настройки устройства до заводских. Если устройство ранее не использовалось, пропустите этот шаг и перейдите к шагу 3.

2. Перейдите в раздел **Параметры** → **Учетные записи** и удалите с устройства все учетные записи.

3. Отключите блокировку экрана.

4. Включите режим разработчика. Для этого:

a. Перейдите в раздел **Параметры** → **Сведения о телефоне**.

b. Нажмите на параметр **Номер сборки** семь раз. Появится сообщение "**Вы стали разработчиком!**"

> На некоторых устройствах эти разделы могут находиться в другом расположении или иметь другие названия. Подробнее смотрите в документации к Android.

5. Перейдите в раздел **Параметры** → **Параметры разработчика** и включите параметр **Отладка по USB**.

6. Разрешите установку приложений, полученных не из Google Play. Для этого:

a. Перейдите в раздел **Параметры** → **Безопасность**.

b. Включите параметр **Неизвестные источники**.

7. Для установки Kaspersky Endpoint Security для Android на устройство используйте пакет установки, загруженный из Kaspersky Security Center, или другой подходящий способ (например, файл .apk).

8. После установки приложения в открывшемся окне нажмите **Готово**, чтобы завершить работу мастера установки.

Для успешной реализации этого сценария приложение следует запускать только после выполнения команды ADB (см. шаг 11).

9. Установите ADB на компьютер.

10. Подключите устройство к компьютеру с помощью USB-кабеля.

    Появится диалоговое окно с запросом на разрешение отладки устройства на компьютере. Нажмите на кнопку **OK**.

11. Запустите ADB и выполните следующую команду:

```
adb shell dpm set-device-owner com.kaspersky.kes/com.kms.selfprotection.DeviceAdmin.
```

12. Запустите приложение Kaspersky Endpoint Security для Android и активируйте его, следуя инструкциям мастера первоначальной настройки.

На некоторых устройствах Xiaomi невозможно развернуть приложение в этом режиме через ADB, если включена оптимизация MIUI. Для развертывания приложения в этом режиме необходимо отключить оптимизацию MIUI. Для этого перейдите в раздел **Параметры** → **Номер сборки**. Нажмите на номер сборки 6–8 раз, чтобы перейти в **Параметры разработчика** для отключения оптимизации MIUI. Повторите перечисленные шаги для развертывания приложения на этих устройствах.

Установка корневых сертификатов на устройстве

Корневой сертификат – это сертификат открытого ключа, выпущенный доверенным центром сертификации (CA). Корневые сертификаты используются, чтобы проверять пользовательские сертификаты и гарантировать их подлинность.

Ваш администратор может указать корневые сертификаты, которые необходимо установить на устройство. На устройства, работающие в режиме device owner и использующие рабочий профиль, эти сертификаты устанавливаются автоматически. Если вы используете личный профиль, то будете получать уведомления, при этом вам нужно будет вручную устанавливать каждый сертификат, следуя приведенным ниже инструкциям.

Чтобы вручную установить корневой сертификат на устройстве:

1. Откройте **Параметры** устройства.
2. Перейдите в параметры безопасности. Путь зависит от модели устройства и версии операционной системы. Например, вам может понадобиться перейти в **Расширенные настройки** → **Безопасность** или **Безопасность и экран блокировки** → **Хранилище учетных данных**.
3. Выберите **Установить из встроенной памяти** / **Установить с SD-карты** или аналогичную опцию.
4. Нажмите **Сертификат ЦС**.
5. В окне подтверждения нажмите **Все равно установить**.
6. В открывшемся файловом менеджере выберите необходимый корневой сертификат.

На некоторых устройствах загруженные сертификаты могут не отображаться в списке **Последние файлы**. Подождите 3–5 минут и снова откройте файловый менеджер. Время ожидания зависит от модели устройства. Если через 3–5 минут файлы не появились, перейдите в папку **Внутреннее хранилище\Загрузки\kesm_certs** или **Карта памяти\Загрузки\kesm_certs** и выберите требуемый корневой сертификат.

Корневой сертификат будет установлен на устройство.

Включение специальных возможностей на Android 13

На Android 13 специальные возможности ограничены для приложений, загруженных не из Google Play и не из HUAWEI AppGallery. Если вы загрузили Kaspersky Endpoint Security для Android с сервера Kaspersky Security Center или с

сайта "Лаборатории Касперского", вам необходимо вручную разрешить доступ к специальным возможностям.

Специальные возможности используются для следующих целей:

- проверки веб-сайтов и приложений в Kaspersky Security Network;
- блокировки устройства в случае кражи;
- отображения уведомлений;
- блокировки камеры, если это запрещено администратором.

Чтобы включить специальные возможности для Kaspersky Endpoint Security, выполните следующие действия:

1. Откройте страницу **Специальные возможности** в настройках устройства и найдите Kaspersky Endpoint Security.
2. Включите переключатель Kaspersky Endpoint Security. В окне, в котором говорится, что доступ к специальным возможностям ограничен, нажмите **ОК**.

   Теперь вы можете предоставить Kaspersky Endpoint Security доступ к ограниченным настройкам.
3. Откройте страницу с информацией о Kaspersky Endpoint Security в настройках устройства. Например, перейдите в **Настройки** > **Приложения**, а затем найдите приложение в списке.
4. На странице с информацией о Kaspersky Endpoint Security нажмите ⋮ в правом верхнем углу и выберите пункт меню **Разрешить ограниченные настройки**.

   Теперь Kaspersky Endpoint Security имеет доступ к ограниченным настройкам.
5. Вернитесь на страницу **Специальные возможности** в настройках устройства и найдите Kaspersky Endpoint Security.
6. Включите переключатель **Kaspersky Endpoint Security**. В открывшемся окне предоставьте приложению полный контроль над вашим устройством.

   Службы специальных возможностей теперь включены для Kaspersky Endpoint Security.

Включение специальных возможностей для приложения на Android 13

Чтобы включить специальные возможности для Kaspersky Endpoint Security, выполните следующие действия:

1. В окне включения служб специальных возможностей нажмите **Включить**.

   Откроется страница **Специальные возможности** в настройках устройства.
2. Включите переключатель Kaspersky Endpoint Security. В окне, в котором говорится, что доступ к специальным возможностям ограничен, нажмите **ОК**.

   Теперь вы можете предоставить Kaspersky Endpoint Security доступ к ограниченным настройкам.
3. Откройте страницу с информацией о Kaspersky Endpoint Security в настройках устройства. Например, перейдите в **Настройки** > **Приложения**, а затем найдите приложение в списке.
4. На странице с информацией о Kaspersky Endpoint Security нажмите ⋮ в правом верхнем углу и выберите пункт меню **Разрешить ограниченные настройки**.

   Теперь Kaspersky Endpoint Security имеет доступ к ограниченным настройкам.
5. Вернитесь в приложение и в окне включения специальных возможностей нажмите **Включить**.

   Откроется страница **Специальные возможности** в настройках устройства.
6. Включите переключатель **Kaspersky Endpoint Security**. В открывшемся окне предоставьте приложению полный контроль над вашим устройством.

   Службы специальных возможностей теперь включены для Kaspersky Endpoint Security.

Обновление приложения

Kaspersky Endpoint Security можно обновить следующими способами:

- Самостоятельно с помощью Google Play. Вы загружаете с Google Play новую версию приложения и устанавливаете приложение на ваше устройство.
- С помощью администратора. Администратор дистанционно обновляет версию приложения на вашем устройстве с помощью системы удаленного администрирования Kaspersky Security Center.

Обновление с помощью Google Play

Администратор может запретить вам обновлять приложение с помощью Google Play.

Обновление с помощью Google Play выполняется обычным способом, принятым для платформы Android. Для обновления приложения должны быть выполнены следующие условия:

- у вас должна быть учетная запись Google;
- устройство должно быть привязано к учетной записи Google;
- на устройстве должно быть установлено соединение с интернетом.

Подробная информация о создании учетной записи Google, привязке устройства к учетной записи и работе с приложением Google Play Маркет приведена на сайте технической поддержки Google.

Обновление с помощью Kaspersky Security Center

Обновление приложения с помощью Kaspersky Security Center состоит из следующих этапов:

1. Администратор отправляет на ваше мобильное устройство дистрибутив приложения, версия которого удовлетворяет требованиям корпоративной безопасности.

   Отобразится запрос на установку Kaspersky Endpoint Security на ваше устройство.
2. Примите условия обновления.

   Новая версия приложения будет установлена на ваше устройство. Дополнительная настройка приложения после обновления не требуется.

Удаление приложения

Kaspersky Endpoint Security можно удалить следующими способами:

- Самостоятельно в настройках устройства.
- С помощью администратора. Администратор может дистанционно удалить приложение с вашего устройства с помощью системы удаленного администрирования Kaspersky Security Center.

На устройствах, работающих в режиме device owner, приложение Kaspersky Endpoint Security для Android может быть удалено только администратором с помощью сброса устройства до заводских настроек.

Удаление в настройках устройства

Удаление приложения выполняется обычным способом, принятым для платформы Android. Для удаления приложения требуется выключить права администратора для Kaspersky Endpoint Security в настройках безопасности устройства.

На устройствах под управлением операционной системы Android версии 7.0 и выше, если администратор запретил удаление, при попытке удалить приложение в настройках Android устройство будет заблокировано. Для разблокирования устройства обратитесь к вашему администратору.

Удаление с помощью Kaspersky Security Center

Удаление приложения с помощью Kaspersky Security Center состоит из следующих этапов:

1. Администратор отправляет на ваше мобильное устройство команду удаления приложения.

   На мобильном устройстве отобразится предложение подтвердить удаление Kaspersky Endpoint Security.
2. Подтвердите удаление приложения.

   Приложение будет удалено с вашего устройства.

Приложения с "портфелем"

Значок приложения в рабочем профиле Android

Приложения, отмеченные значком портфеля (корпоративные приложения), находятся на вашем устройстве в рабочем профиле Android (далее также "Рабочий профиль"). *Рабочий профиль Android* – это безопасная среда на вашем

устройстве, в которой администратор может управлять приложениями и учетными записями, не ограничивая ваши возможности работы с персональными данными.

Рабочий профиль позволяет хранить корпоративные данные отдельно от персональных данных. Это обеспечивает конфиденциальность корпоративных данных и их защиту от вредоносных приложений. При создании рабочего профиля на вашем устройстве в рабочий профиль автоматически устанавливаются следующие корпоративные приложения: Google Play Маркет, Google Chrome, Загрузки, Kaspersky Endpoint Security для Android и другие.

Приложение KNOX

Значок KNOX

Приложение KNOX открывает KNOX-контейнер на вашем устройстве. *KNOX-контейнер* – безопасная среда на вашем устройстве с отдельным рабочим столом, панелью запуска, приложениями, виджетами. Администратор может управлять приложениями и учетными записями в KNOX-контейнере, не ограничивая ваши возможности работы с персональными данными.

KNOX-контейнер позволяет хранить корпоративные данные отдельно от персональных данных. Это обеспечивает конфиденциальность корпоративных данных и их защиту от вредоносных приложений.

В KNOX-контейнере вам доступны корпоративный почтовый ящик, контактные данные сотрудников организации, хранилище файлов и другие приложения.

Подробная информация о работе с KNOX приведена на *сайте Службы технической поддержки Samsung*.

Защита Kaspersky Endpoint Security для Android от удаления

Для защиты мобильного устройства и выполнения требований корпоративной безопасности вы можете включить защиту Kaspersky Endpoint Security для Android от удаления. В этом случае пользователю недоступно удаление приложения с помощью интерфейса Kaspersky Endpoint Security для Android. При удалении приложения с помощью инструментов операционной системы Android пользователю отобразится запрос на выключение прав администратора для Kaspersky Endpoint Security для Android. После выключения прав мобильное устройство будет заблокировано.

Чтобы включить защиту Kaspersky Endpoint Security для Android от удаления, выполните следующие действия:

1. Откройте окно свойств политики:

- В главном окне Kaspersky Security Center Web Console или Cloud Console выберите **Устройства** > **Политики и профили**. В открывшемся списке групповых политик выберите политику, которую вы хотите настроить.

- В главном окне Kaspersky Security Center Web Console или Cloud Console выберите **Устройства** > **Мобильные** > **Устройства**. Выберите мобильное устройство, подпадающее под действие политики, которую вы хотите настроить, а затем выберите политику на закладке **Активные политики и профили политик**.

2. На странице свойств политики выберите **Параметры приложений** > **Контроль безопасности**.

3. В разделе **Управление приложениями на мобильном устройстве** снимите флажок **Разрешить удаление приложения Kaspersky Endpoint Security для Android на устройстве**.

> На устройствах под управлением операционной системы Android 7.0 или выше для защиты приложения от удаления Kaspersky Endpoint Security для Android должен быть установлен в качестве службы Специальных возможностей. Во время работы мастера первоначальной настройки Kaspersky Endpoint Security для Android предлагает пользователю предоставить приложению необходимые права. Пользователь может пропустить эти шаги или выключить права в параметрах устройства позднее. В этом случае защита приложения от удаления не работает.

4. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения, внесенные в политику, и закрыть окно свойств политики.

   Параметры на мобильном устройстве будут настроены после очередной синхронизации устройства с Kaspersky Security Center.

   При попытке удаления приложения мобильное устройство будет заблокировано.

Настройка синхронизации мобильных устройств с Kaspersky Security Center

Для управления мобильными устройствами и получения отчетов и статистики от мобильных устройств настройте параметры синхронизации. Синхронизация мобильных устройств с Kaspersky Security Center может быть выполнена следующими способами:

- **По расписанию**. Синхронизация по расписанию выполняется с помощью протокола HTTP. Вы можете настроить расписание синхронизации в свойствах политики. Изменение параметров политик, команд и задач выполняется при синхронизации мобильных устройств с Kaspersky Security Center по расписанию, то есть с задержкой. По умолчанию мобильные устройства автоматически синхронизируются с Kaspersky Security Center каждые шесть часов.

- **Принудительно** (для Android-устройств). Принудительная синхронизация выполняется с помощью push-уведомлений сервиса FCM (Firebase Cloud Messaging). Принудительная синхронизация, в первую очередь, предназначена для своевременной доставки команд на мобильное устройство. Это может быть полезно, если устройство находится в режиме экономии заряда батареи, поскольку в этом случае приложение может выполнять задачи позже, чем указано. Если вы хотите использовать принудительную синхронизацию, убедитесь что параметры FSM в Kaspersky Security Center настроены.

  Чтобы настроить синхронизацию мобильного устройства с Kaspersky Security Center, выполните следующие действия:

1. Откройте окно свойств политики:

- В главном окне Kaspersky Security Center Web Console или Cloud Console выберите **Устройства** > **Политики и профили**. В открывшемся списке групповых политик выберите политику, которую вы хотите настроить.

- В главном окне Kaspersky Security Center Web Console или Cloud Console выберите **Устройства** > **Мобильные** > **Устройства**. Выберите мобильное устройство, подпадающее под действие политики, которую вы хотите настроить, а затем выберите политику на закладке **Активные политики и профили политик**.

2. На странице свойств политики выберите **Параметры приложений** > **Синхронизация**.

3. В разделе **Синхронизация с Сервером администрирования** в раскрывающемся списке **Период синхронизации** выберите период синхронизации.

   По умолчанию синхронизация выполняется каждые шесть часов.

   При выставлении малых периодов синхронизации фактический период синхронизации может быть немного больше из-за технических ограничений. Это особенно актуально для устройств в режиме экономии заряда батареи. Частые синхронизации приводят к повышенному расходу заряда аккумулятора устройства.
4. Вы можете отключить синхронизацию для устройств Android, когда устройство находится в роуминге. Для этого установите флажок **Выключить синхронизацию в роуминге**.

   По умолчанию синхронизация в роуминге включена.
5. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения, внесенные в политику, и закрыть окно свойств политики.

Параметры на мобильном устройстве будут настроены после очередной синхронизации устройства с Kaspersky Security Center.

Обмен информацией с Google Analytics для Firebase, Firebase Performance Monitoring и Crashlytics

Вы можете определить эти параметры политики только для устройств Android.

Kaspersky Endpoint Security для Android обменивается данными с сервисами Google Analytics для Firebase, Firebase Performance Monitoring и Crashlytics для улучшения качества, внешнего вида и производительности программного обеспечения, продуктов, сервисов и инфраструктуры "Лаборатории Касперского" по результатам анализа работы пользователей, функций, статуса и используемых настроек устройств.

Обмен информацией с сервисами Google Analytics для Firebase, Firebase Performance Monitoring и Crashlytics по умолчанию отключен.

Чтобы включить обмен данными, выполните следующие действия:

1. Откройте окно свойств политики:

- В главном окне Kaspersky Security Center Web Console или Cloud Console выберите **Устройства** > **Политики и профили**. В открывшемся списке групповых политик выберите политику, которую вы хотите настроить.

- В главном окне Kaspersky Security Center Web Console или Cloud Console выберите **Устройства** > **Мобильные** > **Устройства**. Выберите мобильное устройство, подпадающее под действие политики, которую вы хотите настроить, а затем выберите политику на закладке **Активные политики и профили политик**.

2. На странице свойств политики выберите **Параметры приложений** > **KSN и статистика**.

3. В разделе **Отправка статистики в сторонние сервисы** установите флажок **Разрешить передачу данных, чтобы помочь улучшить качество работы, интерфейс и производительность приложения**.

4. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения, внесенные в политику, и закрыть окно свойств политики.

Параметры на мобильном устройстве будут настроены после очередной синхронизации устройства с Kaspersky Security Center.

Настройка уведомлений на мобильных устройствах

Вы можете определить эти параметры политики только для устройств Android.

Если вы хотите, чтобы пользователь мобильного устройства не отвлекался на уведомления Kaspersky Endpoint Security для Android, вы можете выключить некоторые уведомления.

В Kaspersky Endpoint Security используются следующие средства для отображения статуса защиты устройства:

- **Уведомление о состоянии защиты**. Уведомление закреплено в панели уведомлений. Уведомление о состоянии защиты нельзя удалить. В уведомлении отображается статус защиты устройства (например, ) и количество проблем, если они имеются. Пользователь устройства может нажать на статус защиты устройства и посмотреть список проблем в приложении.
- **Уведомления приложения**. Уведомления информируют пользователя устройства о приложении (например, об обнаружении угрозы).
- **Всплывающие сообщения**. Всплывающие сообщения требуют внимания со стороны пользователя устройства (например, предпринять действия при обнаружении угрозы).

По умолчанию все уведомления Kaspersky Endpoint Security для Android включены.

На Android 13 пользователь устройства должен предоставить разрешение на отправку уведомлений во время работы Мастера начальной настройки или позже.

Пользователь Android-устройства может выключить все уведомления от Kaspersky Endpoint Security для Android в настройках панели уведомлений. Если уведомления выключены, пользователь не контролирует работу приложения и может пропустить важную информацию (например, о сбоях при синхронизации устройства с Kaspersky Security Center). Чтобы пользователь узнал статус работы приложения, ему необходимо открыть Kaspersky Endpoint Security для Android.

Чтобы настроить отображение уведомлений о работе Kaspersky Endpoint Security для Android на мобильном устройстве, выполните следующие действия:

1. Откройте окно свойств политики:

- В главном окне Kaspersky Security Center Web Console или Cloud Console выберите **Устройства** > **Политики и профили**. В открывшемся списке групповых политик выберите политику, которую вы хотите настроить.

- В главном окне Kaspersky Security Center Web Console или Cloud Console выберите **Устройства** > **Мобильные** > **Устройства**. Выберите мобильное устройство, подпадающее под действие политики, которую вы хотите настроить, а затем выберите политику на закладке **Активные политики и профили политик**.

2. На странице свойств политики выберите **Параметры приложений** > **Уведомления и отчеты**.

3. В разделе **Уведомления** настройте отображение уведомлений:

- Чтобы скрыть все уведомления и всплывающие сообщения, отключите переключатель **Отображать уведомления, если Kaspersky Endpoint Security работает в фоновом режиме**.

  Kaspersky Endpoint Security для Android будет показывать только уведомления о состоянии защиты. В уведомлении отображается статус защиты устройства (например, ) и количество проблем. Приложение также отображает уведомления, когда пользователь работает с приложением (например, обновляет базы вредоносного ПО вручную).

  Специалисты "Лаборатории Касперского" рекомендуют включить уведомления и всплывающие сообщения. Если уведомления и всплывающие сообщения отключены, когда приложение работает в фоновом режиме, приложение не уведомляет пользователей об угрозах в реальном времени. Пользователи мобильных устройств узнают о состоянии защиты устройства, только когда откроют приложение.

- В разделе **Список проблем безопасности, отображаемый на устройствах пользователей** выберите проблемы Kaspersky Endpoint Security для Android, которые должны отображаться на мобильных устройствах пользователей.

4. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения, внесенные в политику, и закрыть окно свойств политики.

   Параметры на мобильном устройстве будут настроены после очередной синхронизации устройства с Kaspersky Security Center.

Обнаружение взлома устройства

Kaspersky Security Center Web Console позволяет обнаруживать взлом устройства (получение root-прав) на устройствах Android. На взломанном устройстве системные файлы не защищены и доступны для изменения. Также на взломанном устройстве доступна установка сторонних приложений из неизвестных источников. После обнаружения взлома рекомендуется восстановить нормальную работу устройства.

Kaspersky Endpoint Security для Android использует следующие службы для обнаружения получения пользователем root-прав:

- *Встроенная служба Kaspersky Endpoint Security для Android*. Служба "Лаборатории Касперского", которая проверяет получение root-прав пользователем мобильного устройства (Kaspersky Mobile Security SDK).

При взломе устройства вы получите уведомление. Вы можете просмотреть уведомления о взломах в Kaspersky Security Center Web Console на закладке **Мониторинг и отчетность** > **Панель мониторинга**. Вы также можете выключить уведомление о взломе в параметрах уведомлений о событиях.

На Android-устройствах можно установить ограничения на действия пользователя в случае взлома устройства (например, заблокировать устройство). Вы можете установить ограничения с помощью компонента Контроль соответствия. Для этого создайте правило соответствия с критерием **На устройстве получены root-права**.

Задание параметров лицензирования

Вы можете настроить эти параметры политики для устройств Android.

Для управления мобильными устройствами в Kaspersky Security Center Web Console или Cloud Console необходимо активировать мобильное приложение на мобильных устройствах. Активация приложения Kaspersky Endpoint Security для Android на мобильном устройстве осуществляется путем предоставления приложению информации о действующей лицензии. Информация о лицензии передается на мобильное устройство вместе с политикой при синхронизации устройства с Kaspersky Security Center.

Если мобильное приложение не было активировано в течение 30 дней с момента установки на мобильное устройство, оно автоматически переключается в режим работы с ограниченной функциональностью. В этом режиме работы большинство компонентов приложения не работает. При переходе в режим работы с ограниченной функциональностью приложение прекращает выполнять автоматическую синхронизацию с Kaspersky Security Center. Поэтому, если приложение не было активировано в течение 30 дней с момента установки,

пользователю необходимо вручную выполнить синхронизацию устройства с Kaspersky Security Center.

Чтобы задать параметры лицензирования для групповой политики, выполните следующие действия:

1. Откройте окно свойств политики:

- В главном окне Kaspersky Security Center Web Console или Cloud Console выберите **Устройства** > **Политики и профили**. В открывшемся списке групповых политик выберите политику, которую вы хотите настроить.

- В главном окне Kaspersky Security Center Web Console или Cloud Console выберите **Устройства** > **Мобильные** > **Устройства**. Выберите мобильное устройство, подпадающее под действие политики, которую вы хотите настроить, а затем выберите политику на закладке **Активные политики и профили политик**.

2. На странице свойств политики выберите **Параметры приложений** > **Лицензии**.

3. С помощью раскрывающегося списка выберите требуемый лицензионный ключ в хранилище ключей Сервера администрирования.

   Подробная информация о лицензионном ключе отображается в полях ниже.

> Вы можете заменить существующий ключ активации на мобильном устройстве, если он отличается от ключа, выбранного в раскрывающемся списке. Для этого установите флажок **Если на устройстве используется другой ключ, замените его этим ключом**.

4. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения, внесенные в политику, и закрыть окно свойств политики.

   Параметры на мобильном устройстве будут настроены после очередной синхронизации устройства с Kaspersky Security Center.

Лицензирование программы

Этот раздел содержит информацию об основных понятиях, связанных с лицензированием Kaspersky Endpoint Security для Android.

В этом разделе

О Лицензионном соглашении

Лицензионное соглашение – это юридически обязывающее соглашение между вами и АО "Лаборатория Касперского", в котором определены условия использования Kaspersky Endpoint Security для Android.

Рекомендуется внимательно ознакомиться с условиями Лицензионного соглашения перед началом работы с Kaspersky Endpoint Security для Android.

Условия и положения Лицензионного соглашения можно посмотреть следующими способами:

- Во время установки Kaspersky Endpoint Security для Android.
- В разделе **О приложении** в Kaspersky Endpoint Security для Android.

Вы принимаете условия Лицензионного соглашения, подтверждая свое согласие с текстом Лицензионного соглашения во время установки компонентов Kaspersky Endpoint Security для Android. Если вы не согласны с условиями Лицензионного соглашения, следует прервать установку компонентов Kaspersky Secure Mobility Management и отказаться от их использования.

О лицензии

Лицензия - это ограниченное по времени право на использование Kaspersky Endpoint Security для Android, предоставляемое в соответствии с условиями подписанного Лицензионного соглашения с конечным пользователем.

Объем предоставляемых услуг и срок использования программы зависят от лицензии, по которой используется программа.

Предусмотрены следующие типы лицензий:

- *Пробная.*

Бесплатная лицензия, предназначенная для ознакомления с Kaspersky Endpoint Security для Android.

Пробная лицензия имеет срок 30 дней. По истечении срока действия пробной лицензии мобильное приложение Kaspersky Endpoint Security для Android

прекращает выполнять большинство функций, кроме синхронизации с Сервером администрирования. Чтобы продолжить использование приложения, вам нужно приобрести коммерческую лицензию.

- *Коммерческая.*

  Платная лицензия.

  По истечении срока действия коммерческой лицензии мобильные приложения продолжают работу, но с ограниченной функциональностью.

  В режиме ограниченной функциональности в зависимости от приложения доступны следующие компоненты:

- Приложение Kaspersky Endpoint Security для Android:

- Защита от вредоносного ПО. Доступна постоянная защита и поиск вредоносного ПО на устройстве, но не доступно обновление баз вредоносного ПО.

- Анти-Вор. Доступна только отправка команд на мобильные устройства.

- Синхронизация с Сервером администрирования.

> Приложение Kaspersky Endpoint Security для Android прекращает обмен информацией с Kaspersky Security Network, Google Analytics для Firebase, Firebase Performance Monitoring и Crashlytics в случае блокировки ключа, выданного "Лабораторией Касперского", по истечении срока действия пробной лицензии и при отсутствии лицензии (код активации удален из групповой политики).

- Синхронизация с Сервером администрирования.

  Остальные компоненты мобильных приложений недоступны пользователю устройства. Вы можете использовать групповые политики для управления этими компонентами в режиме ограниченной функциональности, но настроить другие компоненты приложений с помощью групповых политик невозможно.

  Чтобы продолжить использование приложения в режиме полной функциональности, вам нужно продлить срок действия коммерческой лицензии. Рекомендуется продлевать срок действия лицензии или приобретать новую лицензию не позднее даты окончания ее срока действия, чтобы обеспечить максимальную защиту компьютера от всех угроз безопасности.

О лицензионном ключе

Лицензионный ключ – последовательность битов, с помощью которой вы можете активировать и затем использовать комплексное решение Kaspersky Endpoint Security для Android в соответствии с условиями Лицензионного соглашения. Лицензионные ключи создаются специалистами "Лаборатории Касперского".

Вы можете добавить лицензионный ключ в мобильное приложение с помощью файла ключа или кода активации:

- Если в вашей организации развернут программный комплекс Kaspersky Security Center, требуется применить файл ключа и распространить его на мобильные приложения для Android. Лицензионный ключ отображается в интерфейсе Kaspersky Security Center и интерфейсе мобильного приложения для Android в виде уникальной буквенно-цифровой последовательности.

  После добавления лицензионных ключей вы можете заменять их другими.
- Если ваша организация не использует Kaspersky Security Center, вам необходимо предоставить пользователю код активации. Пользователь вводит этот код активации в мобильном приложении для Android. Лицензионный ключ отображается в интерфейсе мобильного приложения в виде уникальной буквенно-цифровой последовательности.

  Лицензионный ключ может быть заблокирован "Лабораторией Касперского", если, например, условия Лицензионного соглашения нарушены. Если лицензионный ключ заблокирован, мобильное приложение прекращает выполнять все свои функции, кроме синхронизации с Сервером администрирования. Чтобы продолжить использование приложения, вам нужно добавить другой лицензионный ключ.

О коде активации

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

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

Если код активации был потерян после активации мобильного приложения, вы можете восстановить код активации. Вам может потребоваться код активации, например, для регистрации в Kaspersky CompanyAccount. Для восстановления кода активации требуется обратиться в Службу технической поддержки "Лаборатории Касперского".

О файле ключа

Файл ключа – это файл с расширением key, который вам предоставляет "Лаборатория Касперского". Файл ключа предназначен для добавления ключа, активирующего приложение Kaspersky Endpoint Security для Android.

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

Чтобы активировать приложения с помощью файла ключа, не требуется подключение к серверам активации "Лаборатории Касперского".

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

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

- Обратиться к продавцу лицензии;
- Получить файл ключа на веб-сайте "Лаборатории Касперского" с помощью имеющегося кода активации.

Предоставление данных в Kaspersky Security для Android

Kaspersky Endpoint Security для Android соответствует требованиям Общего регламента по защите данных (GDPR).

Чтобы установить приложение, администратору или пользователю устройства необходимо прочитать и принять условия Лицензионного соглашения. Можно также настроить политику для принятия перечисленных ниже Положений глобально для всех пользователей. В противном случае у пользователей на главном экране приложения будет отображаться уведомление с предложением принять следующие Положения об обработке персональных данных:

- Положение о Kaspersky Security Network;
- Положение об обработке данных для использования Веб-Фильтра;
- Положение об обработке данных в маркетинговых целях.

Если выбран вариант, при котором Положения принимаются глобально, версии Положений, принимаемые в Kaspersky Security Center, должны совпадать с версиями, уже принятыми пользователями. В противном случае пользователи будут проинформированы об этой проблеме, и им будет предложено принять ту версию Положения, которая соответствует версии, принятой администратором глобально. Статус устройства в плагине Kaspersky Security for Mobile (Devices) изменится на *Предупреждение*.

Пользователь может в любой момент принять условия Положения или отказаться от них в разделе **О приложении** в настройках Kaspersky Endpoint Security для Android.

Обмен информацией с Kaspersky Security Network

Для повышения уровня постоянной защиты Kaspersky Endpoint Security для Android использует облачную службу Kaspersky Security Network в работе следующих компонентов:

- **Защита от вредоносного ПО.** Приложение получает доступ к оперативной базе знаний "Лаборатории Касперского" о репутации файлов и приложений. Проверка производится на угрозы, информация о которых еще не вошла в базы вредоносного ПО, но уже содержится в KSN. Облачная служба Kaspersky Security Network обеспечивает полноценную работу Защиты от вредоносного ПО и снижает вероятность ложных срабатываний.

- **Веб-Фильтр.** Приложение выполняет проверку веб-сайтов перед открытием с учетом данных, полученных от KSN. Также приложение определяет категорию веб-сайта для контроля доступа пользователей в интернет на основе списков разрешенных и запрещенных категорий (например, категория "Общение в сети").

- **Контроль приложений.** Приложение определяет категории для ограничения запуска приложений, которые не удовлетворяют требованиям корпоративной безопасности, на основе списков разрешенных и запрещенных категорий (например, категория "Игры").

  Информация о типах данных, передаваемых в "Лабораторию Касперского" при использовании KSN во время работы компонентов Защита от вредоносного ПО и Контроль приложений, приведена в Лицензионном соглашении. Принимая условия Лицензионного соглашения, вы соглашаетесь передавать следующую информацию.

  Информация о типах данных, передаваемых в "Лаборатории Касперского" при использовании KSN во время работы Веб-Фильтра, доступна в Положении об обработке данных для использования Веб-Фильтра. Принимая условия этого Положения, вы соглашаетесь передавать перечисленную ниже информацию.

  Информация о типах статистических данных, передаваемых в "Лабораторию Касперского" при использовании KSN во время работы мобильного приложения Kaspersky Endpoint Security для Android, приведена в Положении о Kaspersky Security Network. Принимая условия этого Положения, вы соглашаетесь передавать перечисленную ниже информацию.

Предоставление данных в рамках Лицензионного соглашения

Если для активации ПО применяется Код активации, с целью проверки правомерности использования ПО Пользователь соглашается периодически предоставлять Правообладателю следующую информацию:

- формат данных в запросе к инфраструктуре Правообладателя; IP-адрес (IPv4) веб-службы, на который осуществлялось обращение; размер содержимого запроса к инфраструктуре Правообладателя; идентификатор протокола; код активации ПО; тип сжатия данных; идентификатор ПО; набор идентификаторов ПО, которое может быть активировано на устройстве пользователя; локализация ПО; полная версия ПО; уникальный идентификатор устройства; дата и время на устройстве пользователя; идентификатор установки ПО (PCID); версия ОС, номер сборки ОС, номер обновления ОС, редакция ОС, расширенная информация о редакции ОС; модель устройства; семейство операционной системы; формат данных в запросе к инфраструктуре Правообладателя; тип контрольной суммы обрабатываемого объекта; заголовок лицензии на использование ПО; идентификатор регионального центра активации; дата и время создания лицензионного ключа ПО; идентификатор лицензии ПО; идентификатор информационной модели, примененной при предоставлении лицензии на использование ПО; дата и время истечения срока действия лицензии на использование ПО; текущий статус лицензионного ключа ПО; тип используемой лицензии ПО; тип лицензии, с помощью которой активировано ПО; идентификатор ПО, полученный из лицензии.

Для защиты Компьютера от угроз информационной безопасности Пользователь соглашается периодически предоставлять Правообладателю следующую информацию:

- тип контрольной суммы обрабатываемого объекта; контрольная сумма обрабатываемого объекта; идентификатор компонента ПО;

- идентификатор сработавшей записи в базах вредоносного ПО; временная метка сработавшей записи в базах вредоносного ПО; тип сработавшей записи в базах вредоносного ПО; название обнаруженной вредоносной программы или легальной программы, которая может быть использована для нанесения вреда устройству или данным пользователя;

- название магазина, из которого приложение было установлено; название пакета приложения; публичный ключ, которым подписан APK-файл; контрольная сумма сертификата, которым подписан APK-файл; временная метка цифрового сертификата;

- полная версия ПО; идентификатор обновления ПО; тип установленного ПО; идентификатор конфигурации; результат действий, выполненных ПО; код ошибки;

- числовые значения, полученные из APK-файла приложения Android в соответствии с определенными математическими правилами и не позволяющие восстановить исходное содержимое файла; эти данные не содержат имен файлов, путей к файлам, адресов, номеров телефонов и другой личной информации пользователей.

Если получение Обновлений выполняется с серверов обновления Правообладателя, то в целях улучшения качества работы механизма обновления Пользователь соглашается периодически предоставлять Правообладателю следующую информацию:

- идентификатор ПО, полученный из лицензии; полная версия ПО; идентификатор лицензии ПО; тип используемой лицензии ПО; идентификатор установки ПО (PCID); идентификатор запуска обновления ПО; обрабатываемый веб-адрес.

  Правообладатель может также использовать такую информацию для получения статистической информации о распространении и использовании ПО.

  Полученная информация защищается "Лабораторией Касперского" в соответствии с установленными законом требованиями. Исходная полученная информация хранится в зашифрованном виде и уничтожается по мере накопления (два раза в год) или по запросу Пользователя. Данные общей статистики хранятся бессрочно.

Предоставление данных в рамках Положения о Kaspersky Security Network

Использование KSN может повысить эффективность защиты, предоставляемой ПО, от угроз информационной и сетевой безопасности.

Если вы используете лицензию для 5 и более узлов, то при использовании KSN Правообладатель будет получать и обрабатывать следующие данные в автоматическом режиме:

- идентификатор сработавшей записи в базах вредоносного ПО; временная метка сработавшей записи в базах вредоносного ПО; тип сработавшей записи в базах вредоносного ПО; дата и время выпуска баз ПО; версия ОС, номер сборки ОС, номер обновления ОС, редакция ОС, расширенная информация о редакции ОС; версия пакета обновления ОС; характеристики обнаружения; контрольная сумма (MD5) обрабатываемого объекта; имя обрабатываемого объекта; признак того, что обрабатываемый объект является PE-файлом; контрольная сумма (MD5) маски, по которой была заблокирована веб-служба; контрольная сумма (SHA256) обрабатываемого объекта; размер обрабатываемого объекта; код типа объекта; заключение ПО по обрабатываемому объекту; путь к обрабатываемому объекту; код каталога файлов; версия компонента ПО; версия отправляемой статистики; адрес веб-службы, на который осуществлялось обрабатываемое обращение (веб-адрес, IP); тип клиента, используемого для обращения к веб-службе; IP-адрес (IPv4) веб-службы, на который осуществлялось обращение; IP-адрес (IPv6) веб-службы, на который осуществлялось обращение; веб-адрес источника запроса к веб-службе (referer); обрабатываемый веб-адрес;

- информация о проверяемых объектах (версия приложения, извлеченная из AndroidManifest.xml; решение ПО по приложению; метод, использованный для получения решения ПО по приложению; название пакета установщика магазина; название пакета (package/bundle) из androidmanifest.xml; категория Google SafetyNet; признак того, что SafetyNet включен на устройстве; значение SHA256 в ответе от Google SafetyNet; APK Signature Scheme для APK-сертификата; код

версии установленного ПО; серийный номер сертификата, которым подписан APK; название устанавливаемого APK-файла; путь до устанавливаемого APK-файла; компания, выпустившая сертификат, которым подписан APK-файл; публичный ключ, которым подписан APK-файл; контрольная сумма сертификата, которым подписан APK-файл; дата и время истечения сертификата; дата и время выдачи сертификата; версия отправляемой статистики; алгоритм расчета отпечатка цифрового сертификата; хеш MD5 от установленного APK-файла; Хеш MD5 от DEX-файла, расположенного внутри установленного APK-файла; динамические разрешения, которые есть у приложения; версия стороннего ПО; информация о том, является ли приложение SMS-менеджером по умолчанию; информация о том, есть ли у приложения права администратора устройства; признак того, что приложение находится в системном каталоге; информация о том, использует ли приложение специальные возможности (accessibility));

- информация обо всех потенциально вредоносных объектах и действиях (содержимое фрагмента в обрабатываемом объекте; дата и время истечения сертификата; дата и время выдачи сертификата; идентификатор ключа из хранилища ключей, используемого для шифрования; протокол, используемый для передачи данных в KSN; порядковый номер фрагмента в обрабатываемом объекте; данные внутреннего журнала, сформированного компонентом Защиты от вредоносного ПО для обрабатываемого объекта; наименование эмитента сертификата; публичный ключ сертификата; алгоритм вычисления публичного ключа сертификата; серийный номер сертификата; дата и время подписи объекта; имя и параметры владельца сертификата; отпечаток цифрового сертификата проверяемого объекта и алгоритм хеширования; дата и время последней модификации обрабатываемого объекта; дата и время создания обрабатываемого объекта; обрабатываемые объекты или их части; описание обрабатываемого объекта, указанное в его свойствах; формат обрабатываемого объекта; тип контрольной суммы обрабатываемого объекта; контрольная сумма (MD5) обрабатываемого объекта; имя обрабатываемого объекта; контрольная сумма (SHA256) обрабатываемого объекта; размер обрабатываемого объекта; название продавца ПО; заключение ПО по обрабатываемому объекту; версия обрабатываемого объекта; источник заключения по обрабатываемому объекту; контрольная сумма обрабатываемого объекта; имя приложения, частью которого является обрабатываемый объект; путь к обрабатываемому объекту; информация о результатах проверки подписи файла; ключ сеанса входа; алгоритм шифрования ключа сеанса входа; время хранения обрабатываемого объекта; алгоритм расчета отпечатка цифрового сертификата);

- тип сборки, например, "user" или "eng"; полное имя продукта; производитель продукта / устройства; разрешена ли установка приложений не из Google Play; статус облачной службы по проверке приложений от Google; статус облачной службы по проверке приложений от Google, устанавливаемых через ADB; текущее название или строка "REL" для публичных сборок; инкрементальный номер сборки; строка версии, отображающаяся у пользователя; название устройства пользователя; идентификатор сборки ПО, отображающийся у пользователя; отпечаток прошивки; идентификатор прошивки; признак рутованности устройства; операционная система; название ПО; тип используемой лицензии ПО;

- информация о качестве работы служб KSN (протокол, используемый для передачи данных в KSN; идентификатор службы KSN, к которой обращается ПО; дата и время окончания получения статистик; количество подключений к KSN,

взятых из кеша; количество запросов, для которых был найден ответ в локальной базе запросов; количество неуспешных подключений к KSN; количество неуспешных KSN-транзакций; распределение по времени выполнения отмененных запросов к KSN; распределение по времени выполнения неуспешных подключений к KSN; распределение по времени выполнения неуспешных KSN-транзакций; распределение по времени выполнения успешных подключений к KSN; распределение по времени выполнения успешных KSN-транзакций; распределение по времени выполнения успешных запросов к KSN; распределение по времени выполнения запросов к KSN, превысивших ограничение на время ожидания; количество новых подключений к KSN; количество неуспешных запросов к KSN из-за ошибок маршрутизации; количество неуспешных запросов из-за выключенного KSN в параметрах ПО; количество неуспешных запросов к KSN из-за сетевых проблем; количество успешных подключений к KSN; количество успешных KSN-транзакций; количество выполненных запросов к KSN; дата и время начала получения статистики);

- идентификатор устройства; полная версия ПО; идентификатор обновления ПО; идентификатор установки ПО (PCID); тип установленного ПО;

- высота экрана устройства; ширина экрана устройства; информация о перекрывающем приложении: хеш MD5 APK-файла; информация о перекрывающем приложении: хеш MD5 файла classes.dex; информация о перекрывающем приложении: имя APK-файла; информация о перекрывающем приложении: путь к APK-файлу без имени файла; высота перекрытия; информация о перекрытом ПО: хеш MD5 APK-файла; информация о перекрытом приложении: хеш MD5 файла classes.dex; информация о перекрытом приложении: имя файла APK; информация о перекрытом приложении: путь к файлу APK без имени файла; информация о перекрытом приложении: название пакета приложения (для перекрытого приложения: если реклама отображается на пустом экране, должно быть значение "launcher"); дата и время перекрытия; информация о перекрывающем приложении: название пакета приложения; ширина перекрытия;

- параметры используемой точки доступа Wi-Fi (тип обнаруженного устройства; настройки протокола DHCP (контрольные суммы локального IPv6-адреса шлюза, DHCP IPv6, DNS1 IPv6, DNS2 IPv6, контрольная сумма длины префикса сети; контрольная сумма локального адреса IPv6); настройки DHCP (контрольные суммы: локального IP-адреса шлюза, DHCP IP, DNS1 IP, DNS2 IP, маски подсети); признак наличия домена DNS; контрольная сумма выданного локального IP-адреса (IPv6); контрольная сумма выданного локального IP-адреса (IPv4); признак работы устройства от электрической сети; тип аутентификации Wi-Fi сети; список доступных Wi-Fi сетей и их параметры; контрольная сумма (MD5 с модификатором) MAC-адреса точки доступа; контрольная сумма (SHA256 с модификатором) MAC-адреса точки доступа; типы соединений, поддерживаемые точкой доступа Wi-Fi; тип шифрования сети Wi-Fi; локальное время начала и конца подключения к сети Wi-Fi; идентификатор сети Wi-Fi, посчитанный по MAC-адресу точки доступа; идентификатор сети Wi-Fi, посчитанный по её названию; идентификатор сети Wi-Fi, посчитанный по её названию и MAC-адресу точки доступа; уровень сигнала сети Wi-Fi; название Wi-Fi сети; набор протоколов аутентификации, поддерживаемых этой конфигурацией; используемый протокол аутентификации при подключении вида WPA-EAP; используемый протокол внутренней аутентификации; набор групповых шифров, поддерживаемых этой

конфигурацией; набор протоколов управления ключами, поддерживаемых этой конфигурацией; итоговая категория публичности сети в ПО; итоговая категория безопасности сети в ПО; набор парных шифров для WPA, поддерживаемых этой конфигурацией; набор протоколов безопасности, поддерживаемых этой конфигурацией);

- дата и время установки ПО; дата активации ПО; идентификатор компании партнера, у которого был размещен заказ на покупку лицензии на использование ПО; идентификатор ПО, полученный из лицензии; серийный номер лицензионного ключа ПО; локализация ПО; признак участия в KSN; идентификатор ПО, для которого предназначена лицензия; идентификатор лицензии ПО; идентификатор ОС; разрядность операционной системы.

  Также для достижения заявленной цели повышения эффективности защиты, предоставляемой ПО, Правообладатель может получать объекты (файл или его часть, служебная информация), в отношении которых существует риск их использования злоумышленниками для нанесения вреда устройству и создания угроз информационной безопасности.

Участие в Kaspersky Security Network для обработки статистических данных является добровольным. Вы можете в любой момент отказаться от участия в Kaspersky Security Network.

Предоставление данных в рамках Положения об обработке данных для использования Веб-Фильтра

В соответствии с Положением о Веб-Фильтре, Правообладатель обрабатывает данные в целях обеспечения работы Веб-Фильтра. Заявленная цель включает обнаружение веб-угроз и определение категорий посещаемых веб-сайтов с помощью облачной службы Kaspersky Security Network (KSN).

С вашего согласия, следующие данные будут автоматически регулярно отправляться Правообладателю в соответствии с Положением о Веб-Фильтре:

- версия продукта, уникальный идентификатор устройства, идентификатор установки, тип продукта;

- адрес веб-сайта, посещаемого в текущий момент пользователем, номер порта, протокол передачи данных, адрес веб-сайта, с которого был осуществлен переход.

Предоставление данных в рамках Положения об обработке данных для маркетинговых целей

Правообладатель использует для обработки данных информационные системы третьих лиц. Обработка данных в информационных системах третьих лиц

регулируется соответствующими политиками конфиденциальности таких систем. Правообладатель использует следующие сервисы для обработки перечисленных данных:

Google Analytics для Firebase

При использовании ПО следующие данные будут автоматически отправляться на регулярной основе в сервис Google Analytics для Firebase для их обработки для заявленных целей:

- информация о приложении: версия, идентификатор, название и идентификатор приложения в сервисе Firebase, уникальный идентификатор установки в сервисе Firebase, название магазина, из которого ПО было получено, время первого запуска ПО на устройстве;
- идентификатор установки приложения на устройство и способ установки на устройство;
- информация о регионе и языковой локализации;
- разрешение экрана устройства;
- информация о получении root -прав пользователем;
- признак установки Kaspersky Endpoint Security для Android в качестве службы Специальных возможностей;
- информация о переходах между окнами приложения, продолжительности сессии, начале и окончании сессии работы с экраном, названии экрана;
- информация о протоколе отправки данных в сервис Firebase, его версии и идентификаторе используемого метода отправки данных;
- информация о типе и параметрах события, в отношении которого происходит отправка данных;
- информация о лицензии на приложение, ее наличии, количестве устройств;
- интервалы обновления баз вредоносного ПО и синхронизации с Сервером администрирования;
- идентификатор Android ID;
- идентификатор Advertising ID;
- информация о пользователе: возрастная категория и половая принадлежность пользователя, идентификатор страны проживания, список интересов пользователя;

- информация о компьютере, на котором установлено ПО: название производителя компьютера, тип компьютера, модель устройства, версия и информация о языковой локализации ОС, информация о первом запущенном приложении за последнюю неделю и ранее.

  Передача данных в сервис Google Analytics для Firebase осуществляется по защищенному каналу. Информация об условиях обработки данных в сервисе Google Analytics для Firebase доступна по адресу https://firebase.google.com/support/privacy.

  Firebase Performance Monitoring

  При использовании ПО следующие данные будут автоматически отправляться на регулярной основе в сервис Firebase Performance Monitoring для их обработки для заявленных целей:

- уникальный идентификатор установки;
- название пакета приложения;
- версия установленного ПО;
- уровень и статус заряда батареи;
- оператор связи;
- признак работы ПО в фоновом режиме;
- регион;
- IP-адрес;
- код языка устройства;
- информация о радио- и интернет-соединении;
- идентификатор-псевдоним экземпляра ПО;
- ОЗУ и размер диска;
- признак того, что на устройстве выполнена процедура рутинга или джейлбрейка;
- уровень сигнала;
- продолжительность автоматической трассировки;
- информация о сети и сопутствующая информация ответа: код ответа, размер полезной нагрузки в байтах, время отклика;
- описание устройства.

Передача данных в сервис Firebase Performance Monitoring осуществляется по защищенному каналу. Информация об условиях обработки данных в сервисе Firebase Performance Monitoring доступна по адресу https://firebase.google.com/support/privacy.

Crashlytics

При использовании ПО следующие данные будут автоматически отправляться на регулярной основе в сервис Crashlytics для их обработки для заявленных целей:

- идентификатор ПО;
- версия установленного ПО;
- признак работы ПО в фоновом режиме;
- архитектура ЦП;
- уникальный идентификатор события;
- дата и время события;
- модель устройства;
- объем полного и используемого дискового пространства;
- название и версия ОС;
- объем полной и используемой оперативной памяти;
- признак того, что на устройстве выполнена процедура рутинга;
- ориентация экрана в момент события;
- производитель продукта / устройства;
- уникальный идентификатор установки;
- версия отправляемой статистики;
- тип исключения ПО;
- текст сообщения об ошибке;
- признак того, что исключение ПО вызвано исключением на вложенном уровне;
- идентификатор потока;
- признак того, что фрейм стал причиной ошибки ПО;

- признак того, что выполнение потока привело к неожиданному завершению работы ПО;
- данные о сигнале, который привел к неожиданному завершению работы ПО: название сигнала, код сигнала, адрес сигнала;
- для каждого фрейма, ассоциированного с потоком, исключением или ошибкой: имя файла фрейма, номер строки файла фрейма, отладочные символы, адрес и смещение в бинарном образе, отображаемое имя библиотеки, содержащей фрейм, тип фрейма, признак того, что фрейм стал причиной ошибки;
- идентификатор ОС;
- идентификатор проблемы, связанной с событием;
- информация о событиях, предшествующих неожиданному завершению работы ПО: идентификатор события, дата и время события, тип события и значение;
- значения регистра ЦП;
- тип события и значение.

Передача данных в сервис Crashlytics осуществляется по защищенному каналу. Информация об условиях обработки данных в сервисе Crashlytics доступна по адресу https://firebase.google.com/terms/crashlytics-app-distribution-data-processing-terms.

Предоставление вышеуказанной информации для обработки в маркетинговых целях является добровольным.

Обращение в Службу технической поддержки

Этот раздел содержит информацию о способах и условиях получения технической поддержки.

В этом разделе

Способы получения технической поддержки

Если вы не нашли решения вашей проблемы в документации или других источниках информации о Kaspersky Endpoint Security для Android, обратитесь в Службу технической поддержки. Сотрудники Службы технической поддержки ответят на ваши вопросы об установке и использовании Kaspersky Endpoint Security для Android.

"Лаборатория Касперского" обеспечивает поддержку Kaspersky Endpoint Security для Android в течение его жизненного цикла (см. таблицу поддерживаемых продуктов). Перед обращением в Службу технической поддержки ознакомьтесь с правилами предоставления технической поддержки.

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

- Посетить веб-сайт Службы технической поддержки
- Отправить запрос в Службу технической поддержки с портала Kaspersky CompanyAccount

Техническая поддержка через Kaspersky CompanyAccount

Kaspersky CompanyAccount – это портал для организаций, использующих программы "Лаборатории Касперского". Портал Kaspersky CompanyAccount предназначен для взаимодействия пользователей со специалистами "Лаборатории Касперского" с помощью электронных запросов. Kaspersky CompanyAccount можно также использовать для отслеживания статуса и хранения истории ваших онлайн-обращений.

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.

Более подробная информация о Kaspersky CompanyAccount приведена на веб-сайте Службы технической поддержки.

Источники информации о программе

В полной справке для приложений Kaspersky Endpoint Security для Android вы можете найти информацию о настройке и использовании мобильных приложений.

Обсуждение программ "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.

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

Глоссарий

IMAP

Протокол для доступа к электронной почте. В отличие от протокола POP3, IMAP предоставляет расширенные возможности работы с почтовыми ящиками, такие как управление папками, манипуляция сообщениями без копирования их содержимого с почтового сервера. Протокол IMAP использует порт 134.

Kaspersky Private Security Network (KPSN)

Kaspersky Private Security Network – это решение, предоставляющее пользователям устройств с установленными программами "Лаборатории Касперского" доступ к репутационным базам данных Kaspersky Security Network и

другим статистическим данным без отправки данных с устройств в Kaspersky Security Network. Kaspersky Private Security Network разработан для корпоративных клиентов, которые не могут участвовать в Kaspersky Security Network по следующим причинам:

- Устройства не подключены к интернету.
- Передача любых данных за пределы страны или корпоративной локальной сети запрещена законом или корпоративными политиками безопасности.

Kaspersky Security Network (KSN)

Инфраструктура облачных служб, предоставляющая доступ к базе данных "Лаборатории Касперского" с постоянно обновляемой информацией о репутации файлов, веб-ресурсов и программного обеспечения. Kaspersky Security Network обеспечивает более высокую скорость реакции программ "Лаборатории Касперского" на угрозы, повышает эффективность работы некоторых компонентов защиты, а также снижает вероятность ложных срабатываний.

KES-устройство

Мобильное устройство, подключенное к Серверу администрирования Kaspersky Security Center и управляемое через приложение Kaspersky Endpoint Security для Android.

POP3

Сетевой протокол получения сообщений почтовым клиентом с почтового сервера.

SSL

Протокол шифрования данных в локальных сетях и в интернете. Протокол SSL (Secure Sockets Layer) используется в веб-приложениях для создания защищенных соединений между клиентом и сервером.

Автономный пакет установки

Установочный файл программы Kaspersky Endpoint Security для операционной системы Android, содержащий параметры подключения программы к Серверу администрирования. Создается на основе инсталляционного пакета для этой программы и является частным случаем пакета мобильных приложений.

Агент администрирования

Компонент программы Kaspersky Security Center, осуществляющий взаимодействие между Сервером администрирования и приложениями "Лаборатории Касперского", установленными на конкретном сетевом узле (рабочей станции или сервере).

Администратор Kaspersky Security Center

Лицо, управляющее работой программы через систему удаленного централизованного администрирования Kaspersky Security Center.

Администратор устройства

Набор прав приложения на Android-устройстве, позволяющий приложению использовать политики управления устройством. Необходим для реализации полной функциональности Kaspersky Endpoint Security на Android-устройстве.

Активация программы

Перевод программы в полнофункциональный режим. Активация выполняется пользователем во время или после установки программы. Для активации программы необходим код активации или файл ключа.

Базы вредоносного ПО

Базы данных, которые содержат информацию об угрозах компьютерной безопасности, известных "Лаборатории Касперского" на момент выпуска баз вредоносного ПО. Записи в базах вредоносного ПО позволяют обнаруживать вредоносный код в проверяемых объектах. Базы вредоносного ПО формируются специалистами "Лаборатории Касперского" и обновляются каждый час.

Веб-сервер Kaspersky Security Center

Компонент Kaspersky Security Center, который устанавливается совместно с Сервером администрирования. Веб-сервер предназначен для передачи по сети автономных пакетов установки, а также файлов из папки общего доступа.

Виртуальный Сервер администрирования

Компонент программы Kaspersky Security Center, предназначенный для управления системой защиты сети организации-клиента.

Виртуальный Сервер администрирования является частным случаем подчиненного Сервера администрирования и, по сравнению с физическим Сервером администрирования, имеет следующие основные ограничения:

- Виртуальный Сервер администрирования может функционировать только в составе главного Сервера администрирования.
- Виртуальный Сервер администрирования при работе использует основную базу данных главного Сервера администрирования. Задачи резервного копирования и восстановления данных, а также задачи проверки и загрузки обновлений, не поддерживаются на виртуальном Сервере администрирования.
- Для виртуального Сервера не поддерживается создание подчиненных Серверов администрирования (в том числе и виртуальных).

Вредоносное ПО

Программа, которая заражает другие программы – добавляет в них свой код, чтобы получить управление при запуске зараженных файлов. Это простое определение дает возможность выявить основное действие, выполняемое вредоносным программным обеспечением – заражение.

Группа администрирования

Набор управляемых устройств, например, мобильных устройств, объединенных в соответствии с их функциями и установленным на них набором программ. Управляемые устройства группируются с целью управления ими как единым целым. Например, в группу администрирования могут быть объединены мобильные устройства под управлением одной операционной системы. В состав группы могут входить другие группы администрирования. Для устройств в группах могут быть созданы групповые политики и сформированы групповые задачи.

Групповая задача

Задача, назначенная для группы администрирования и выполняемая на всех управляемых устройствах, входящих в состав группы.

Инсталляционный пакет

Набор файлов, формируемый для удаленной установки программы "Лаборатории Касперского" с помощью системы удаленного администрирования. Инсталляционный пакет создается на основании специальных файлов, входящих в состав дистрибутива программы. Инсталляционный пакет содержит набор параметров, необходимых для установки программы и обеспечения ее работоспособности сразу после установки. Значения параметров в инсталляционном пакете соответствуют значениям параметров приложения по умолчанию.

Карантин

Папка, в которую программа "Лаборатории Касперского" перемещает обнаруженные возможно зараженные объекты. Объекты на карантине хранятся в зашифрованном виде во избежание их воздействия на компьютер.

Категории "Лаборатории Касперского"

Готовые категории данных, разработанные сотрудниками "Лаборатории Касперского". Категории могут обновляться при обновлении баз программы. Специалист по информационной безопасности не может изменять или удалять готовые категории.

Код активации

Код, который вы получаете, приобретая лицензию на Kaspersky Endpoint Security. Этот код необходим для активации программы.

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

Код разблокировки

Код, который можно получить в Kaspersky Security Center. Он нужен, чтобы разблокировать устройство после выполнения команд **Блокирование и Поиск**, **Сирена** или **Тайное фото**, а также при срабатывании самозащиты.

Контроль соответствия

Проверка соответствия параметров мобильного устройства и Kaspersky Endpoint Security для Android требованиям корпоративной безопасности. Требования корпоративной безопасности регламентируют использование устройства. Например, на устройстве должна быть включена постоянная защита, базы вредоносного ПО должны быть актуальны, пароль устройства должен быть достаточно сложным. Контроль соответствия работает на основе списка правил. Правило соответствия состоит из следующих компонентов:

- критерий проверки устройства (например, отсутствие на устройстве запрещенных приложений);
- время, выделенное пользователю устройства для устранения несоответствия (например, 24 часа);
- действие, которое будет выполнено с устройством, если пользователь не устранит несоответствие в течение указанного времени (например, блокировка устройства).

Лицензионное соглашение

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

Лицензия

Ограниченное по времени право на использование приложения, предоставляемое на основании Лицензионного соглашения.

Плагин управления программой

Специализированный компонент, предоставляющий интерфейс для управления работой программы "Лаборатории Касперского" через Консоль администрирования. Для каждой программы существует свой плагин управления. Плагин управления входит в состав всех программ "Лаборатории Касперского", управление которыми можно осуществлять через Kaspersky Security Center.

Подписка

Позволяет использовать программу с выбранными параметрами (дата окончания, количество устройств). Можно приостанавливать и возобновлять подписку, продлевать ее в автоматическом режиме, а также отменить ее.

Политика

Набор параметров программы и мобильных приложений Kaspersky Endpoint Security, применяемый к устройствам в группах администрирования или к отдельным устройствам. К разным группам администрирования могут применяться разные политики. Политика включает в себя настроенные параметры всех функций мобильных приложений Kaspersky Endpoint Security.

Прокси-сервер

Служба в компьютерных сетях, позволяющая пользователям выполнять косвенные запросы к другим сетевым службам. Сначала пользователь подключается к прокси-серверу и запрашивает ресурс (например, файл), расположенный на другом сервере. Затем прокси-сервер либо подключается к указанному серверу и получает ресурс у него, либо возвращает ресурс из собственного кеша (в случаях, если прокси имеет свой кеш). В некоторых случаях запрос клиента или ответ сервера может быть изменен прокси-сервером в определенных целях.

Рабочее место администратора

Компьютер, на котором развернута Консоль администрирования Kaspersky Security Center. Если на рабочем месте администратора установлен плагин управления программой, то администратор может управлять мобильными приложениями Kaspersky Endpoint Security, развернутыми на устройствах пользователей.

Рабочий профиль Android

Безопасная среда на устройстве пользователя, в которой администратор может управлять приложениями и учетными записями пользователя, не ограничивая его возможности при работе с персональными данными. При создании рабочего профиля на мобильном устройстве пользователя в рабочий профиль автоматически устанавливаются следующие корпоративные приложения: Google Play Маркет, Google Chrome, Загрузки, Kaspersky Endpoint Security для Android и другие. Корпоративные приложения, размещенные в рабочем профиле, а также уведомления этих приложений, отмечены красным значком портфеля. Для приложения Google Play Маркет требуется создать отдельную корпоративную учетную запись Google. Приложения, размещенные в рабочем профиле, отображаются в общем списке приложений.

Сервер администрирования

Компонент программы Kaspersky Security Center, осуществляющий функции централизованного хранения информации об установленных в сети организации программах "Лаборатории Касперского" и управления ими.

Серверы обновлений "Лаборатории Касперского"

HTTP(S)-серверы "Лаборатории Касперского", с которых программы "Лаборатории Касперского" получают обновления баз и модулей программы.

Срок действия лицензии

Период времени, в течение которого вы можете пользоваться функциями программы и дополнительными услугами. Дополнительные услуги зависят от типа лицензии.

Файл ключа

Файл вида xxxxxxxx.key, который позволяет использовать программу "Лаборатории Касперского" по пробной или коммерческой лицензии. Программа формирует файл ключа на основе кода активации. Программу можно использовать только при наличии файла ключа.

Фишинг

Вид интернет-мошенничества, целью которого является получение несанкционированного доступа к конфиденциальным данным пользователей.

Информация о стороннем коде

Информацию о стороннем коде можно загрузить и ознакомиться с ней в следующих файлах:

- legal_notices_Android.txt (для приложения Kaspersky Endpoint Security для Android)

На мобильных устройствах информация о стороннем коде доступна в разделе **О приложении** мобильных приложений.

Уведомления о товарных знаках

Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.

Adobe, Flash и PostScript являются либо зарегистрированными товарными знаками, либо товарными знаками компании Adobe в США и/или других странах.

AMD64 является товарным знаком или зарегистрированным товарным знаком Advanced Micro Devices, Inc.

Amazon, Amazon EC2, Amazon Web Services, AWS и AWS Marketplace являются товарными знаками Amazon.com, Inc. или ее дочерних компаний.

Apache и Apache feather logo – товарные знаки Apache Software Foundation.

Apple, Apple Configurator, AirDrop, AirPlay, AirPort, AirPort Express, AirPrint, Aperture, App Store, Apple Music, Apple TV, Apple Watch, AppleScript, Bonjour, Face ID,

FaceTime, FileVault, Find My, Find My Friends, Handoff, iBeacon, iBooks, iBooks Store, iCal, iCloud, iCloud Keychain, iMessage, iPad, iPadOS, iPhone, iPhoto, iTunes, iTunes Store, iTunes U, Keychain, macOS OS X, Safari, Siri, Spotlight и Touch ID – товарные знаки Apple Inc.

Aruba Networks – товарный знак Aruba Networks, Inc. в США и некоторых других странах.

Словесный товарный знак Bluetooth и лого принадлежат Bluetooth SIG, Inc.

Aironet, Cisco, Cisco AnyConnect являются зарегистрированными товарными знаками или товарными знаками Cisco Systems, Inc. и/или ее аффилированных компаний в США и в определенных других странах.

Dell Technologies, Dell, SecurID и другие товарные знаки являются товарными знаками компании Dell Inc или её дочерних компаний.

F5 – товарный знак F5 Networks, Inc. в США и в некоторых других странах.

Google, Android, Chrome, Chromebook, Chromium, Crashlytics, Firebase, Gmail, Google Analytics, Google Assistant, Google Chrome, Google Mail, Google Maps, Google Mobile, Google Play, Google Safe Browsing, Google SafeSearch, Google Translate, Nexus, SPDY и YouTube – товарные знаки Google LLC.

HTC – товарный знак HTC Corporation.

HUAWEI и EMUI являются товарными знаками HUAWEI Technologies Co., Ltd.

IBM и Maas360 – товарные знаки International Business Machines Corporation, зарегистрированные во многих юрисдикциях по всему миру.

Juniper Networks, Juniper и JUNOS – товарные знаки или зарегистрированные в США и других странах товарные знаки Juniper Networks, Inc.

Microsoft, Active Directory, ActiveSync, Forefront, Microsoft Intune, Microsoft Outlook, Tahoma, Windows, Windows Mobile, Windows Phone и Window Server являются товарными знаками группы компаний Microsoft.

MOTOROLA и стилизованный логотип M являются зарегистрированными товарными знаками Motorola Trademark Holdings, LLC.

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

OPPO является товарным знаком или зарегистрированным товарным знаком компании Guangdong OPPO Mobile Telecommunications Co., Ltd.

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

Товарный знак BlackBerry принадлежит Research In Motion Limited, зарегистрирован в США и может быть подан на регистрацию или зарегистрирован в других странах.

Samsung – товарный знак компании SAMSUNG в США или других странах.

SonicWALL, Aventail, SonicWALL Mobile Connect – товарные знаки SonicWall, Inc.

SOTI и MobiControl – зарегистрированные в США и в других юрисдикциях товарные знаки SOTI Inc.

Symantec – товарный знак или зарегистрированный в США и других странах товарный знак Symantec Corporation или аффилированных компаний.

Владельцем товарного знака Symbian является Symbian Foundation Ltd.

AirWatch, VMware и VMware Workspace ONE – товарные знаки VMware, Inc. или зарегистрированные в США и/или других юрисдикциях товарные знаки VMware, Inc.