ESET Endpoint Security for Android

Руководство пользователя

Щелкните здесь чтобы отобразить этого документа (онлайн-справка)

Digital Security
Progress. Protected.

Авторское право ©2023 ESET, spol. s r.o.

ESET Endpoint Security for Android разработано компанией ESET, spol. s r.o.

Дополнительные сведения можно получить на сайте https://www.eset.com.

Все права защищены. Ни одна часть этой документации не может воспроизводиться, храниться в системе получения и передаваться в любой форме или любыми средствами, в том числе электронными и механическими способами, с помощью фотокопирования, записи, сканирования, а также любыми другими способами без письменного разрешения автора.

ESET, spol. s r.o. оставляет за собой право изменять любое описанное прикладное программное обеспечение без предварительного уведомления.

Служба технической поддержки: https://support.eset.com

ПРОВ. 04.12.2023

1 Введение ... 1
1.1 Новые возможности версии 3 ... 1
1.2 Минимальные требования к системе ... 1
1.3 Журнал изменений ... 2
2 Пользователи, подключенные к ESET PROTECT и ESET PROTECT Cloud ... 2
3 Удаленная установка ... 3
4 Локальная установка на устройство ... 4
4.1 Загрузка с веб-сайта ESET ... 4
4.2 Мастер начальной настройки ... 5
5 Удаление ... 7
6 Активация программы ... 7
7 Документация по конечным точкам под удаленным управлением ... 8
7.1 Введение в ESET PROTECT ... 9
7.2 Введение в ESET PROTECT Cloud ... 11
7.3 Политики ... 11
7.3 Применение политик ... 12
7.3 Пометки ... 12
7.3 Использование режима переопределения ... 14
8 Защита от вирусов ... 16
8.1 Автоматическое сканирование ... 18
8.2 Журналы сканирования ... 19
8.3 Правила игнорирования ... 20
8.4 Дополнительные параметры ... 20
9 Антивор ... 22
9.1 Контакты администратора ... 22
9.1 Добавление контактов администратора ... 22
9.2 Информация на заблокированном экране ... 23
9.3 Доверенные SIM-карты ... 23
9.4 Удаленные команды ... 23
10 Контроль приложений ... 24
10.1 Правила блокировки ... 24
10.1 Блокировка по имени приложения ... 25
10.1 Блокировка приложений по имени ... 26
10.1 Блокировка по категории приложений ... 26
10.1 Блокировка приложений по категориям ... 26
10.1 Блокировка приложений по типу разрешений ... 27
10.1 Блокировка приложений по типу разрешений ... 27
10.1 Блокировка неизвестных источников ... 27
10.2 Исключения ... 27
10.2 Добавление исключений ... 28
10.3 Обязательные приложения ... 29
10.3 Разрешенные приложения ... 29
10.3 Разрешения ... 30
10.3 Использование ... 31
11 Безопасность устройства ... 32
11.1 Политика блокирования экрана ... 32
11.2 Политика настроек устройства ... 34
12 Защита от фишинга ... 35
13 Контроль доступа в Интернет ... 37

14 Фильтрация вызовов 39
14.1 Правила 40
14.1 Добавление нового правила 41
14.2 Журнал 41
15 Параметры 41
15.1 Импорт и экспорт параметров 42
15.1 Экспорт параметров 43
15.1 Импорт параметров 44
15.1 Журнал 44
15.2 Пароль администратора 44
15.3 Удаленное управление 45
15.4 ИД устройства 46
15.5 Управление разрешениями 46
16 Служба технической поддержки клиентов 47
17 Программа улучшения пользовательского опыта 48
18 Лицензионное соглашение с конечным пользователем 49
19 Политика конфиденциальности 59

Введение

Новое поколение программы ESET Endpoint Security for Android для (EESA) предназначено для работы с ESET PROTECT и ESET PROTECT Cloud — новой консолью управления, с помощью которой можно удаленно управлять всеми решениями для обеспечения безопасности ESET.

Программа ESET Endpoint Security for Android версии 3 совместима со следующими решениями:

- ESET Security Management Center 7,
- ESET PROTECT и ESET PROTECT Cloud.

Приложение ESET Endpoint Security for Android предназначено для защиты корпоративных мобильных устройств от новейших угроз, а также для защиты данных даже в случае потери или кражи устройства. Также оно помогает системным администраторам обеспечивать соответствие устройств корпоративным политикам безопасности.

Приложение ESET Endpoint Security for Android может также применяться компаниями малого и среднего размера без необходимости в удаленном управлении с помощью ESET PROTECT. ИТ-специалист, системный администратор или сам пользователь может просто поделиться своей конфигурацией ESET Endpoint Security for Android с коллегами. Этот процесс полностью устраняет необходимость в активации программы и ручной настройке каждого модуля продукта, которые в ином случае следует выполнять сразу же после установки ESET Endpoint Security for Android.

Новые возможности версии 3

Добавлено:

- Поддержка развертывания MS Intune.
- Поддержка автоматической миграции из локальной среды в облако.

Удалена:

- Функции, связанные с управлением избыточными устройствами, при регистрации через MS Intune.
- Удалена: удаление функций защиты от фишинга и веб-контроля при установке в рабочем профиле.

Минимальные требования к системе

Чтобы установить ESET Endpoint Security for Android на устройство под управлением Android, оно должно соответствовать следующим минимальным требованиям к системе.

- Операционная система: Android 5 (Lollipop) и более поздние версии.
- Разрешение сенсорного экрана: 480 x 800 пкс.

- Процессор: ARM с набором инструкций ARMv7 или x86 Intel Atom
- Свободное место для хранения данных: 20 МБ.
- Подключение к Интернету.

Android Go не поддерживается

Устройства с двумя SIM-картами и устройства, на которых получены права суперпользователя root, не поддерживаются. Некоторые возможности (например, модуль Антивор и Фильтрация вызовов) недоступны на планшетах, которые не поддерживают телефонные звонки и обмен сообщениями.

Журнал изменений

Пользователи, подключенные к ESET PROTECT и ESET PROTECT Cloud

ESET PROTECT и ESET PROTECT Cloud — это приложения, позволяющие осуществлять централизованное управление установленными в сетевой среде продуктами ESET. Системы управления задачами ESET PROTECT и ESET PROTECT Cloud позволяют установить программы безопасности ESET на удаленные компьютеры и быстро реагировать на новые проблемы и угрозы. Сама программа ESET PROTECT не защищает от вредоносного кода. На каждом клиенте должно быть установлено решение ESET для обеспечения безопасности.

Решения по обеспечению безопасности ESET поддерживают сети с различными типами платформ. В сети могут сосуществовать операционные системы Microsoft, Linux и macOS, а также системы, работающие на мобильных устройствах (мобильных телефонах и планшетах).

ESET PROTECT и ESET PROTECT Cloud представляют собой новое поколение удаленной системы управления, значительно отличающееся от предыдущих версий ESET Remote Administrator. Проверить совместимость с предыдущими версиями продуктов безопасности ESET можно здесь:

- Поддерживаемые продукты ESET PROTECT
- Поддерживаемые продукты ESET PROTECT Cloud

Различия между ESET PROTECT и ESET PROTECT Cloud можно найти в нашей документации.

Дополнительные сведения см. в следующей документации:
- Электронная документация по ESET PROTECT
- Электронная документация по ESET PROTECT Cloud

Удаленная установка

Чтобы установить программу ESET Endpoint Security for Android с сервера ESET PROTECT удаленно, требуется выполнить следующие действия:

- установить Mobile Device Connector;
- Зарегистрировать мобильное устройство.

Сценарии установки ESET Endpoint Security for Android

• Администратор отправляет конечным пользователям по электронной почте ссылку для регистрации, установочный APK-файл и описание процесса установки. Пользователь переходит по ссылке для регистрации, которая открывается в интернет-браузере, используемом в системе Android по умолчанию. Установленное на устройстве приложение ESET Endpoint Security for Android регистрируется и подключается к ESET PROTECT. Если приложение ESET Endpoint Security for Android не установлено на устройстве, пользователь перенаправляется в магазин Google Play для его загрузки. После загрузки приложения происходит стандартная установка.

• Администратор отправляет конечным пользователям по электронной почте файл настроек приложения, установочный APK-файл и описание процесса установки. После установки пользователь должен открыть файл настроек приложения. Все настройки импортируются, и приложение активируется (при условии, что была добавлена информация о лицензии).

Регистрация устройств с ограниченными возможностями ввода

ESET Endpoint Security for Android позволяет регистрировать в ESET PROTECT Cloud устройства без камеры, браузера или электронной почты (например, телевизоры, «умные» дисплеи, рекламные дисплеи и т. д.). Чтобы зарегистрировать такие устройства, установите ESET Endpoint Security for Android на устройстве с помощью магазина Google Play или APK-файла. В мастере начальной настройки на этапе **Удаленное управление** выберите **Да, управлять удаленно** и нажмите **Устройство с ограниченным вводом**.

В разделе ESET PROTECT Cloud (Основные настройки):

1.Щелкните **Компьютеры** > **Добавить устройство** > **Android или iOS/iPadOS** > **Настроить регистрацию**.

2.Щелкните **Устройства Android с ограниченными опциями ввода** и выберите предпочтительный способ распространения. Дополнительные сведения о способах распространения можно найти в консоли ESET PROTECT Cloud.

3.Я принимаю лицензионное соглашение с конечным пользователем и соглашаюсь с политикой конфиденциальности.

4.Если это новое устройство, щелкните **Добавить**. Введите все необходимые сведения и щелкните **Сохранить**. Если добавляется существующее устройство, выберите нужное устройство.

5.Вы получите ссылку для регистрации устройства. Щелкните ссылку и введите шестизначный код безопасности, который отображается в разделе **Удаленное управление** мастера начальной настройки.

6.Щелкните **Принять**.

Теперь устройство зарегистрировано в ESET PROTECT Cloud.

Локальная установка на устройство

ESET Endpoint Security for Android дает администратору возможность настраивать Endpoint приложение и управлять им локально, если не используется ESET PROTECT. Все параметры приложения защищены администраторским паролем, поэтому администратор всегда и всецело контролирует приложение.

Если администратор небольшой компании не использует ESET PROTECT и при этом ему необходимо обеспечивать защиту корпоративных устройств и применять базовые политики безопасности, ему будут доступны два варианта локального управления устройствами.

1.Получить к каждому устройству компании физический доступ и настроить параметры вручную.

2.Администратор может подготовить необходимую конфигурацию на своем устройстве Android (на котором установлена программа ESET Endpoint Security for Android) и экспортировать эти настройки в файл. Дополнительные сведения см. в разделе Импорт и экспорт параметров данного руководства.). Администратор может передать экспортированный файл конечным пользователям (например, по электронной почте), чтобы они могли импортировать его на любое устройство, на котором установлена программа ESET Endpoint Security for Android. Когда пользователь открывает и принимает файл параметров, все параметры импортируются автоматически и приложение активируется (если в файл были включены сведения о лицензии). Все параметры будут защищены паролем администратора.

Загрузка с веб-сайта ESET

Скачайте ESET Endpoint Security for Android, просканировав QR-код ниже с помощью приложения для сканирования QR-кодов на вашем мобильном устройстве.

Кроме того, APK-файл для установки ESET Endpoint Security for Android можно загрузить с веб-сайта ESET:

1.Загрузите установочный файл с веб-сайта ESET.

2.Откройте этот файл из области уведомлений Android или найдите его с помощью приложения для работы с файлами. Обычно файл сохраняется в папку загрузок.

3.Убедитесь, что приложения, полученные из неизвестных источников разрешены на вашем устройстве. Для этого коснитесь значка запуска на главном экране Android или последовательно выберите **Главный экран** > **Меню**. Нажмите **Настройки** > **Безопасность**. Необходимо разрешить использование **неизвестных источников**.

4.Открыв файл, нажмите **Установить**.

приложение ESET Endpoint Security for Android, загруженное с сайта ESET, можно обновить только с помощью файла, загруженного с сайта ESET, или внутри приложения. Выполнить обновление с помощью магазина Google Play нельзя.

Мастер начальной настройки

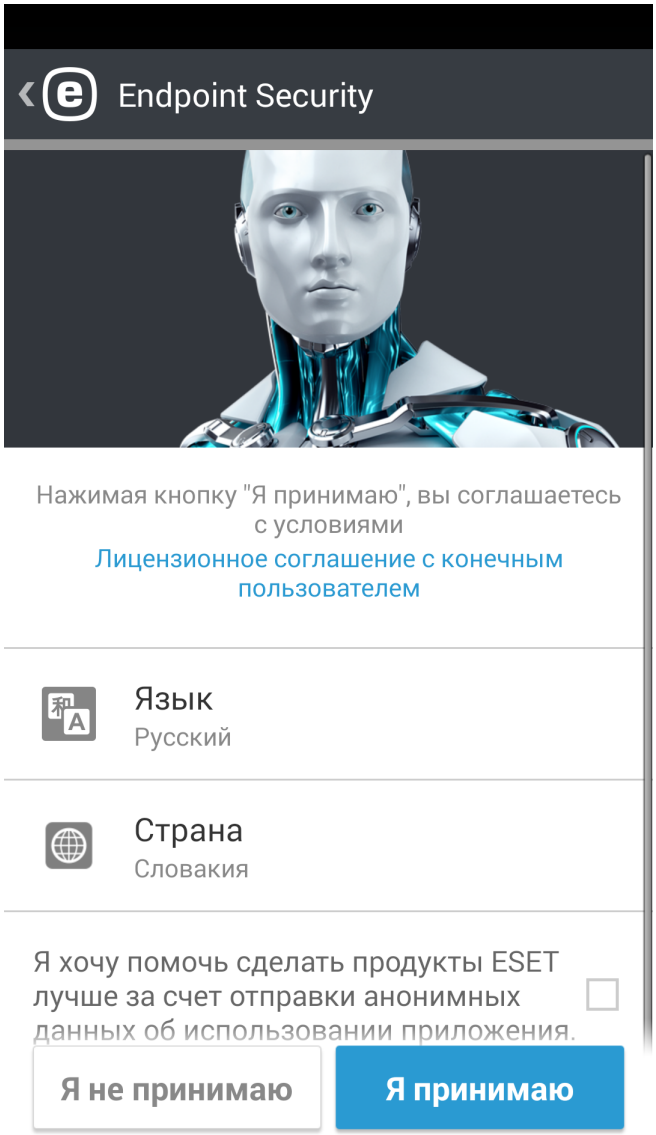
После установки приложения нажмите **Настройки администратора** и следуйте подсказкам мастера начальной настройки. Эта процедура предназначена только для администраторов:

1.Выберите **язык**, который необходимо использовать в ESET Endpoint Security for Android.

2.Выберите **страну,** в которой вы работаете или находитесь в настоящее время.

3.Если вы хотите помочь улучшить продукты ESET путем отправки анонимных данных об использовании приложения, установите соответствующий флажок.

4.Нажмите **Я принимаю**. Нажатие **Я принимаю** означает, что вы соглашаетесь с условиями лицензионного соглашения.



5.Чтобы подтвердить согласие пользователя, коснитесь элемента **Принять**.

6.Выберите **Да, управлять удаленно**, чтобы подключить ESET Endpoint Security for Android к ESET PROTECT или выполнить настройку вручную, нажимав **Нет, просто защищать**.

7.Для ручной настройки требуются разрешения телефона и хранилища. Нажмите **Продолжить**, а затем нажмите **Разрешить**, чтобы предоставить все разрешения.

8.Нажмите **Продолжить**, чтобы разрешить отображение поверх других приложений.

9.Для ручной настройки требуется выполнить активацию продукта. Вы можете активировать ESET Endpoint Security for Android с помощью лицензионного ключа или через ESET Business Account (EBA).

10.Создайте пароль администратора.

11.**Защита от удаления программы** не дает пользователям, которые не имеют соответствующего разрешения, удалить ESET Endpoint Security for Android. Нажмите **Включить**, а затем выберите **Активировать** в запросе **Активировать приложение администратора устройства**.

12.Разрешите доступ к статистике использования, чтобы обеспечить надлежащую работу приложения. Нажмите **Продолжить** и выберите **ESET Endpoint Security for Android**, чтобы разрешить **доступ к данным об использовании**. Дважды нажмите стрелку назад, чтобы вернуться к мастеру начальной настройки.

13.Выберите **Принять** или **Отклонить** для участия в системе обратной связи ESET LiveGrid®. Чтобы узнать больше об ESET LiveGrid®, ознакомьтесь с этим разделом.

14.Выберите для ESET Endpoint Security for Android **Включить обнаружение** или **Не включать обнаружение** потенциально нежелательных приложений. Дополнительные сведения о таких приложениях приведены в этом разделе. Нажмите **Далее**.

15.Нажмите **Готово**, чтобы закрыть мастер начальной настройки и запустить первое сканирование устройства.

Удаление

Программу ESET Endpoint Security for Android можно удалить вручную, выполнив следующие действия.

> **Важно**
> В данном руководстве описаны настройки стоковой версии Android. Процесс удаления может отличаться в зависимости от производителя устройства.

1.На устройстве Android откройте раздел **Настройки** > **Биометрия и безопасность** > **Другие настройки безопасности** > **Приложения администратора устройства**. Снимите флажок рядом с программой **ESET Endpoint Security for Android** и коснитесь элемента **Отключить**. Коснитесь элемента **Разблокировать** и введите пароль администратора. Если программа ESET Endpoint Security for Android не указана в качестве администратора устройства, пропустите этот этап.

2.Вернитесь в раздел **Настройки** и нажмите **Приложения** > **ESET Endpoint Security for Android** > **Удалить** > **OK**.

Активация программы

Активировать ESET Endpoint Security for Android можно несколькими способами. Доступность того или иного способа зависит от страны и того, как продукт был получен (с веб-страницы ESET и т. д.).

Чтобы активировать ESET Endpoint Security for Android непосредственно на устройстве Android, нажмите значок **Меню** на главном экране программы ESET Endpoint Security for Android и выберите элемент **Лицензия**.

Можно воспользоваться любым из перечисленных ниже способов для активации ESET Endpoint Security for Android:

- **Лицензионный ключ**-уникальная строка в формате XXXX-XXXX-XXXX-XXXX-XXXX которая

используется для идентификации владельца лицензии и активации лицензии.

• **ESET Business Account** — учетная запись, созданная на портале ESET Business Account с использованием учетных данных (адрес электронной почты и пароль). Этот метод позволяет централизовано управлять несколькими лицензиями.

ESET PROTECT может активировать клиентские устройства в автоматическом режиме, используя предоставленные администратором лицензии.

Документация по конечным точкам под удаленным управлением

Продуктами ESET для бизнеса и решением ESET Endpoint Security for Android на клиентских рабочих станциях, серверах и мобильных устройствах в сетевой среде можно управлять удаленно из одного центрального расположения. Системным администраторам, управляющим более чем 10 клиентскими рабочими станциями, рекомендуется использовать средство удаленного управления ESET. С его помощью можно централизованно развертывать решения ESET, управлять задачами, применять политики безопасности, отслеживать состояние системы и оперативно реагировать на проблемы и угрозы, возникающие на удаленных компьютерах.

Средства удаленного управления ESET

ESET Endpoint Security for AndroidРешением можно управлять удаленно с помощью ESET PROTECT или ESET PROTECT Cloud.

• Введение в ESET PROTECT

• Введение в ESET PROTECT Cloud

Средство переноса

ESET Endpoint Security for Android 3.5 и более поздних версий поддерживает средство переноса, используемое для перехода от ESET PROTECT к ESET PROTECT Cloud.

Рекомендации

• Регистрация устройства с помощью ESET PROTECT

• Настройка пароля администратора на подключенных клиентских компьютерах для предотвращения несанкционированных изменений

• Примените рекомендуемую политику, чтобы активировать доступные функции безопасности.

Практические руководства

• Использование режима переопределения

Устройство Android, зарегистрированное с помощью Microsoft Intune

Если устройство с ОС Android 9 и более поздних версий зарегистрировано с помощью Microsoft Intune, приложение ESET Endpoint Security for Android 3.5 и более поздних версий игнорирует следующие настройки при применении соответствующей политики:

- Безопасность устройства
- Контроль приложений
- Антивор

Введение в ESET PROTECT

ESET PROTECT дает возможность управлять продуктами ESET на рабочих станциях, серверах и мобильных устройствах в сетевой среде из одного центрального расположения.

С помощью веб-консоли ESET PROTECT можно развертывать решения ESET, управлять задачами, применять политики безопасности, отслеживать состояние системы и оперативно реагировать на проблемы и обнаружения, возникающие на удаленных компьютерах. Ознакомьтесь также с разделами Обзор архитектуры и элементов инфраструктуры ESET PROTECT, Начало работы с веб-консолью ESET PROTECT и Поддерживаемые среды подготовки рабочих столов.

ESET PROTECT состоит из следующих компонентов.

- Сервер ESET PROTECT. Сервер ESET PROTECT устанавливается на сервера под управлением Windows или Linux, а также в качестве виртуального устройства. Он управляет связью с агентами, собирает и сохраняет данные приложений в базе данных.

- Веб-консоль ESET PROTECT. Веб-консоль ESET PROTECT является основным интерфейсом, который позволяет управлять клиентскими компьютерами в вашей среде. В ней отображаются общие сведения о состоянии клиентов в сети, и ее можно использовать для удаленного развертывания решений ESET на неуправляемых компьютерах. После установки сервера ESET PROTECT вы можете получить доступ к веб-консоли с помощью браузера. Если разрешить доступ к веб-серверу из Интернета, можно будет использовать ESET PROTECT практически в любом месте и на любом устройстве с подключением к Интернету.

- ESET Management Агент. Агент ESET Management облегчает обмен данными между сервером ESET PROTECT и клиентскими компьютерами. Агент должен быть установлен на клиентском компьютере, чтобы установить связь между этим компьютером и сервером ESET PROTECT. Поскольку он находится на клиентском компьютере и может хранить несколько сценариев безопасности, использование ESET Management значительно сокращает время реагирования на новые обнаружения. С помощью веб-консоли ESET PROTECT можно развернуть агент ESET Management на неуправляемых компьютерах, распознанных с помощью Active Directory или ESET RD Sensor. Можно также вручную установить агент ESET Management на клиентских компьютерах, если это необходимо.

- Rogue Detection Sensor. ESET PROTECT Rogue Detection (RD) Sensor обнаруживает неуправляемые компьютеры, присутствующие в сети, и отправляет сведения о них на сервер ESET PROTECT. Это позволяет легко добавлять новые клиентские компьютеры в защищенную сеть. Rogue Detection Sensor запоминает компьютеры, которые были обнаружены, и не будет отправлять

одну и ту же информацию дважды.

- Прокси-сервер Apache HTTP. Это служба, которую можно использовать вместе с ESET PROTECT, чтобы:
  - oРассылать обновления на клиентские компьютеры и установочные пакеты — агенту ESET Management.
  - oПересылать данные с агентов ESET Management на сервер ESET PROTECT.
- Mobile Device Connector — это компонент, позволяющий использовать средства управления мобильными устройствами в ESET PROTECT для управления мобильными устройствами (Android и iOS) и администрирования ESET Endpoint Security для Android.
- Виртуальное устройство ESET PROTECT — виртуальное устройство ESET PROTECT доступно для пользователей, которым требуется запустить ESET PROTECT в виртуализированной среде.
- ESET PROTECT Virtual Agent Host — компонент ESET PROTECT, который виртуализирует сущности агентов, позволяя управлять безагентными виртуальными машинами. Это решение обеспечивает автоматизацию, использование динамических групп и тот же уровень управления задачами, что и агент ESET Management на физических компьютерах. Виртуальный агент собирает информацию с виртуальных машин и передает ее на сервер ESET PROTECT.
- Средство «Зеркало». Это средство необходимо для автономного обновления модулей. Если у клиентских компьютеров нет подключения к Интернету и при этом им нужны обновления модулей, с помощью средства «Зеркало» можно загрузить файлы обновления с серверов обновления ESET и хранить эти файлы локально.
- ESET Remote Deployment Tool. Этот инструмент предназначен для развертывания комплексных пакетов, созданных в веб-консоли <%PRODUCT%>. Это удобный способ распространения агентов ESET Management с продуктом ESET на компьютерах по сети.
- ESET Business Account. Новый портал лицензирования для бизнес-продуктов ESET позволяет управлять своими лицензиями. См. раздел <%EBA%> этого документа, чтобы узнать больше об активации своего продукта, или см. <%EBA%> руководство пользователя, чтобы получить дополнительные сведения об использовании <%EBA%>.
- ESET Enterprise Inspector (EEI) — это комплексная система обнаружения и реагирования конечных точек, которая включает в себя такие функции, как обнаружение инцидентов, управление инцидентами и реагированием, сбор данных, индикаторы обнаружения компромиссов, обнаружение аномалий, обнаружение поведения, нарушения политики.

С помощью веб-консоли ESET PROTECT можно развертывать решения ESET, управлять задачами, применять политики безопасности, отслеживать состояние системы и оперативно реагировать на проблемы и угрозы, возникающие на удаленных компьютерах.

> Более подробная информация приведена в онлайн-руководстве пользователя ESET PROTECT.

Введение в ESET PROTECT Cloud

ESET PROTECT Cloud дает возможность управлять продуктами ESET на рабочих станциях и серверах в сетевой среде из одного центрального местоположения без необходимости использовать физический или виртуальный сервер, как в случае с ESET PROTECT или ESET Security Management Center. С помощью веб-консоли ESET PROTECT Cloud можно развертывать решения ESET, управлять задачами, применять политики безопасности, отслеживать состояние системы и оперативно реагировать на проблемы и угрозы, возникающие на удаленных компьютерах.

- Дополнительные сведения см. в интерактивном руководстве пользователя ESET PROTECT Cloud

Политики

Администратор может применять определенные конфигурации к продуктам ESET, работающим на клиентских устройствах, с помощью политик из веб-консоли ESET PROTECT или веб-консоли ESET Security Management Center. Политика может применяться непосредственно к отдельным устройствам или к их группам. Кроме того, для устройства или группы можно назначить несколько политик.

Пользователь должен иметь следующие разрешения для создания новой политики: **Чтение** — для чтения списка политик, **Использование** — для назначения политик целевым компьютерам и **Запись** — для создания, изменения или редактирования политик.

Политики применяются в том порядке, в котором расположены статические группы. Это не относится к динамическим группам, где политики сначала применяются к дочерним динамическим группам. Это позволяет применять политики с большим влиянием на верхние группы в иерархии и применять более конкретные политики для подгрупп. Используя флажки, ESET Endpoint Security for Android пользователь, имеющий доступ к группам, расположенным выше в иерархии, может переопределить политики нижних групп. Алгоритм описан в Онлайн-справке ESET PROTECT.

Установка политик на устройстве отключает возможность локального изменения настроек, управляемых политикой. Эти настройки заблокированы от изменений даже в режиме администратора. Можно разрешить временные изменения, создав политику режима переопределения.

Для установки определенных политик может потребоваться локальное предоставление дополнительного разрешения для ESET Endpoint Security for Android на затронутом устройстве.

Рекомендуется назначать дополнительные общие политики (например, для сервера обновлений) группам, расположенным на вершине иерархии. Специализированные политики (касающиеся, например, контроля устройств) следует располагать ниже в иерархии групп. Это необходимо потому, что при объединении расположенная ниже политика обычно заменяет параметры расположенной выше политики (если иное не задано флажками политики).

Используемые по умолчанию политики для ESET Endpoint Security for Android

Имя политики	Описание политики
Общее — максимальная защита	В ESET Endpoint Security for Android используются все возможности для обеспечения максимальной защиты устройства.
Общее — сбалансированная настройка	В ESET Endpoint Security for Android используется конфигурация, рекомендуемая для большинства систем.
Общее — максимальная производительность	В ESET Endpoint Security for Android сочетается защита от угроз и минимальное влияние на ежедневные задачи и производительность устройства.

Применение политик

После подключения ESET Endpoint Security for Android к консоли управления ESET лучший вариант — это применить рекомендуемую или пользовательскую политику.

Для ESET Endpoint Security for Android есть несколько встроенных политик:

Имя политики	Описание политики
Общее — максимальная защита	В ESET Endpoint Security for Android используются все возможности для обеспечения максимальной защиты устройства.
Общее — сбалансированная настройка	В ESET Endpoint Security for Android используется конфигурация, рекомендуемая для большинства систем.
Общее — максимальная производительность	В ESET Endpoint Security for Android сочетается защита от угроз и минимальное влияние на ежедневные задачи и производительность устройства.

Дополнительные сведения о политиках можно найти в следующих разделах:

- ESET PROTECT политики
- ESET PROTECT Cloud политики
- Применение рекомендуемой или предварительно заданной политики для ESET Endpoint Security for Android с помощью ESET Security Management Center

Пометки

Политика, применяемая на клиентском компьютере, обычно является результатом объединения нескольких политик в одну окончательную. При объединении политик можно настроить ожидаемое поведение конечной политики с помощью порядка применяемых политик, используя флажки политики. Флажки определяют, как политика будет обрабатывать определенный параметр.

Для каждого параметра можно выбрать один из следующих флажков.

Не применять	Любой параметр с этим флажком политикой игнорируется. Поскольку этот параметр не задан политикой, его можно изменить с помощью других политик, применяемых позже.
Применить	Параметры с флажком «**Применить**» будут применены к клиентскому компьютеру. Однако при слиянии политик он может быть перезаписан другими политиками, применяемыми позже. Когда политика передается на клиентский компьютер, содержащий параметры, отмеченные этим флажком, эти параметры изменят локальную конфигурацию клиентского компьютера. Поскольку для параметра не выбрано принудительное применение, его значение можно будет изменить другими политиками, применяемыми позже.
Принудительно применить	Настройки с флажком **Принудительно применить** имеют высший приоритет и не могут быть перезаписаны какой-либо политикой, примененной позже (даже если у нее также есть флажок **Принудительно применить**). Это гарантирует, что другие политики, примененные позже, не смогут изменить этот параметр при слиянии. Когда политика передается на клиентский компьютер, содержащий параметры, отмеченные этим флажком, эти параметры изменят локальную конфигурацию клиентского компьютера.

Сценарий. Администратору нужно разрешить пользователю *John* создавать или изменять политики в своей домашней группе, а также просматривать все политики, созданные Администратором, включаяПолитики, которые имеют флажки Применить принудительно. Администратор хочет, чтобы *John* мог просматривать все политики, но не редактировать существующие политики, созданные администратором. *John* может создавать или редактировать политики в своей домашней группе San Diego.
РешениеАдминистратор должен сделать следующее.
Создать настраиваемые статические группы и наборы разрешений
1. Создайте новую статическую группу с именем Санкт-Петербург.
2. Создайте новый набор разрешений с именем *Policy — All John* с доступом к статической группе *All* и с разрешением **Чтение** для объекта **Политики**.
3. Создайте новый набор разрешений с именем *Policy John* с доступом к статической группе *San Diego* и с разрешением доступа к функциональности **Запись** для объектов **Группы и компьютеры** и **Политики**. Этот набор разрешений позволяет пользователю *John* создавать или редактировать политики в своей домашней группе *San Diego*.
4. Создайте нового пользователя *John* и в разделе **Наборы разрешений** выберите *Policy — All John* и *Policy John*.
Создание политик
5. Создайте новую политику *All — Enable Firewall*, разверните раздел **Настройка**, выберите **ESET Endpoint для Windows**, выберите **Персональный файервол** > **Основная информация** и примените все настройки флажком **Применить принудительно**. Разверните раздел **Применить** и выберите статическую группу *All*.
6. Создайте новую политику *John Group — Enable Firewall*, разверните раздел **Настройка**, выберите **ESET Endpoint для Windows**, выберите **Персональный файервол** > **Основная информация** и примените все настройки флажком **Применить**. Разверните раздел **Применить** и выберите статическую группу *San Diego*.
Результат
Политики, созданные Администратором, будут применяться сначала, поскольку к параметрам политики были применены флажки **Применить принудительно**. Параметры с установленным этим флажком имеют приоритет и не могут быть перезаписаны другой политикой, применяемой позже. Политики, созданные пользователем *John*, будут применяться после политик, созданных Администратором. Чтобы увидеть окончательный порядок политик, перейдите в раздел **Дополнительно** > **Группы** > **SanDiego**. Щелкните компьютер и выберите **Показать подробности**. В разделе **Конфигурация** нажмите **Действующие политики**.

Использование режима переопределения

Пользователи, на компьютерах которых установлено приложение ESET Endpoint Security for Android (версии 2.1 и более поздних версий), могут использовать функцию переопределения. Режим переопределения позволяет пользователям на уровне клиентского устройства изменять настройки установленного продукта ESET на определенное время, даже если для этих настроек применена политика. По истечении определенного времени настройки, заданные политиками, восстанавливаются.

Согласно настройкам политики по умолчанию приложение ESET Endpoint Security for Android сканирует устройство сразу после завершения сеанса переопределения. Это можно изменить с помощью параметра **Сканировать устройство после сеанса переопределения**.

- Чтобы локально изменить настройки на устройстве в режиме переопределения, необходимо ввести пароль администратора ESET Endpoint Security for Android.
- Если режим переопределения включен, его нельзя отключить с помощью веб-консоли ESET. Он будет отключен автоматически, когда истечет время переопределения.
- У пользователя, использующего режим переопределения, должен быть пароль администратора ESET Endpoint Security for Android. В противном случае пользователь не сможет получить доступ к настройкам ESET Endpoint Security for Android. Для каждой политики можно создать временный пароль переопределения администратора.

Чтобы установить **режим переопределения**, выполните следующие действия.

1. Щелкните **Политики** > **Новая политика**.
2. В разделе **Основная информация** введите **имя** и **описание** для политики.
3. В разделе **Настройки** выберите **ESET Endpoint Security for Android**.
4. В параметрах политики щелкните **Настройки**.
5. Разверните **Настройки режима переопределения** и настройте правила для этого режима.
6. В разделе **Назначение** выберите нужные устройства.
7. Проверьте настройки в разделе **Сводка** и щелкните **Готово**.

Если у Ивана наблюдается проблема с параметрами конечной точки, блокирующими какую-либо важную функцию или доступ к Интернету на его устройстве, администратор может разрешить Ивану переопределить существующую политику конечной точки и вручную настроить параметры на своем устройстве. Впоследствии новые параметры могут быть запрошены системой ESET PROTECT Cloud, чтобы администратор мог создать на их основе новую политику.

Для этого выполните следующие действия:

1.Щелкните **Политики** > **Новая политика**.

2.Заполните поля **Имя** и **Описание**. В разделе **Настройки** выберите **ESET Endpoint Security for Android**.

3.Щелкните **Настройки** в параметрах политики.

4.Разверните настройки **режима переопределения** и включите режим переопределения на один час.

5.Щелкните **Задать** в учетных данных переопределения, чтобы создать временный пароль администратора для Ивана. Дважды введите пароль (например, 12345) и щелкните **OK**.

6.Назначьте политику смартфону Ивана и нажмите кнопку **Готово**, чтобы сохранить политику.

7.Иван должен ввести пароль администратора, чтобы включить **режим переопределения** в своем приложении ESET Endpoint Security for Android и изменить настройки вручную на своем устройстве.

8.В веб-консоли ESET PROTECT Cloud перейдите в раздел **Компьютеры**, выберите Смартфон Ивана и щелкните **Показать подробности**.

9.Чтобы запланировать клиентскую задачу для получения конфигурации от клиента, в разделе **Конфигурация** щелкните **Запросить конфигурацию**.

10.Появится новая конфигурация. Выберите нужный продукт и щелкните **Открыть конфигурацию**.

11.Проверьте настройки и щелкните **Преобразовать в политику**.

12.Заполните поля **Имя** и **Описание**.

13.При необходимости в разделе **Настройки** измените настройки.

14.В разделе **Назначение** назначьте эту политику смартфону Ивана (или другим).

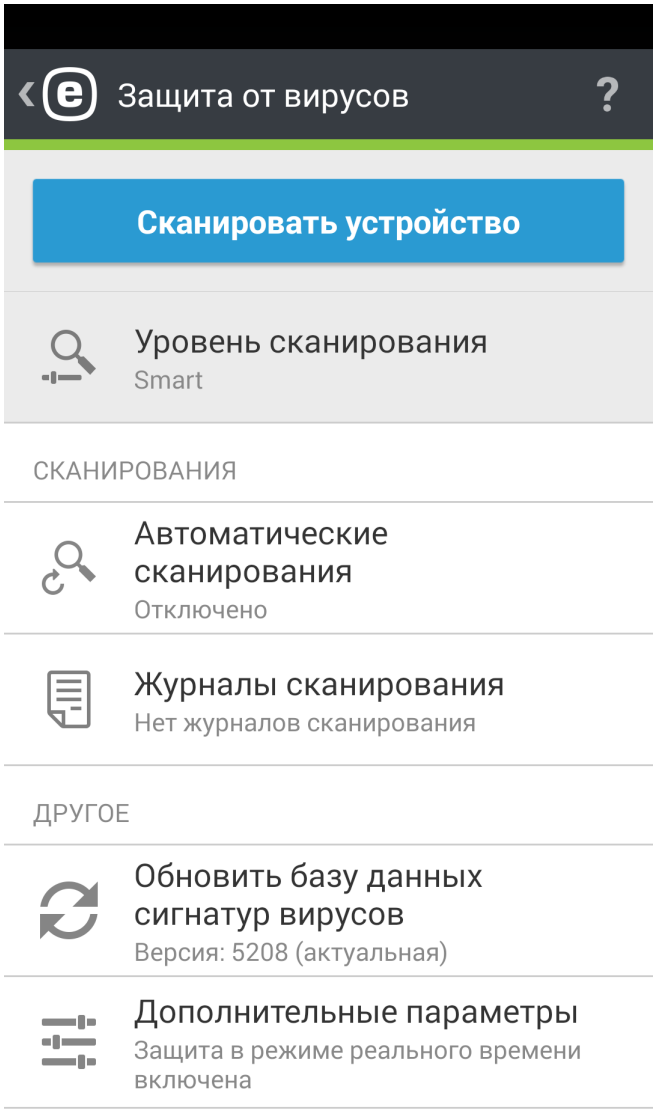
15.Нажмите кнопку **Готово**. Не забудьте удалить политику переопределения после того, как необходимость в ней исчезнет.

Пароль переопределения

С помощью этого параметра можно создать временный пароль администратора, чтобы пользователи могли изменять настройки на клиентском устройстве, не имея доступа к настоящему паролю администратора. Чтобы вставить пароль переопределения, щелкните **Задать** рядом с политикой.

Защита от вирусов

Модуль защиты от вирусов защищает устройство от вредоносного кода, блокируя угрозы и затем удаляя их или перемещая в карантин.



Сканирование устройства

Функцию **«Сканировать устройство»** можно использовать для проверки устройства на наличие заражений.

Файлы некоторых предопределенных типов сканируются по умолчанию. Во время полного сканирования устройства проверяются память, запущенные процессы, зависимые от них динамические библиотеки, а также файлы, находящиеся на съемных носителях и во внутреннем хранилище. Сводные сведения о результатах сканирования сохраняются в файл журнала в разделе «Журналы сканирования».

Чтобы прервать запущенное сканирование, коснитесь значка .

Уровень сканирования

Доступны два уровня сканирования.

- **Сканирование Smart**. Во время сканирования Smart проверяются установленные приложения, DEX-файлы (исполняемые файлы для ОС Android), SO-файлы (библиотеки), ZIP-файлы (максимальная глубина сканирования — три уровня вложения в архиве) и содержимое SD-карт.

• **Тщательное сканирование**. В этом режиме проверяются файлы всех типов с любыми расширениями, находящиеся во внутреннем хранилище и на SD-карте.

Автоматическое сканирование

Кроме сканирования устройства по требованию, приложение ESET Endpoint Security for Android выполняет автоматическое сканирование. Сведения об использовании функций «Сканирование в процессе зарядки» и «Сканирование по расписанию» см. в этом разделе.

Журналы сканирования

В области интерфейса «Журналы сканирования» находятся файлы журналов, содержащие подробные сведения о выполненных сканированиях. Дополнительные сведения см. в разделе этого документа Журналы сканирования средства защиты от вирусов.

Обновить модули обнаружения

По умолчанию программа ESET Endpoint Security for Android регулярно загружает и устанавливает обновления. Это происходит автоматически. Чтобы запустить обновление вручную, нажмите **Обновить модули обнаружения**.

> Чтобы не загружать напрасно полосу пропускания, обновления выпускаются только тогда, когда в базу данных добавляется новая угроза. Обновления для активированного продукта предоставляются бесплатно, но за передачу данных в мобильной сети может взиматься плата.

Подробные сведения о дополнительных параметрах защиты от вирусов можно найти в разделе Дополнительные параметры этого документа.

Автоматическое сканирование

Уровень сканирования

Доступны два уровня сканирования. Этот параметр применяется во время сканирования в процессе зарядки и сканирования по расписанию.

• **Сканирование Smart**. Во время сканирования Smart проверяются установленные приложения, DEX-файлы (исполняемые файлы для ОС Android), SO-файлы (библиотеки), ZIP-файлы (максимальная глубина сканирования — три уровня вложения в архиве) и содержимое SD-карт.

• **Тщательное сканирование**. В этом режиме проверяются файлы всех типов с любыми расширениями, находящиеся во внутреннем хранилище и на SD-карте.

Сканирование в процессе зарядки

Если выбран этот параметр, сканирование начинается автоматически, когда устройство находится в состоянии простоя (полностью заряжено и подключено к зарядному устройству).

Сканирование по расписанию

Этот параметр позволяет указывать время, когда устройство будет сканироваться

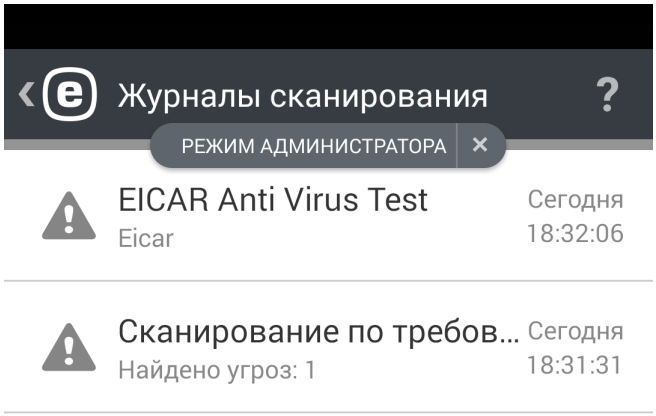
автоматически. Чтобы запланировать сканирование, коснитесь значка  рядом с элементом **Сканирование по расписанию** и укажите дату и время начала сканирования. По умолчанию начало запланировано на понедельник в 4:00.

Журналы сканирования

Журналы сканирования создаются после каждого запланированного или запущенного вручного сканирования устройства.

Каждый журнал содержит такие сведения:

- дата и время события;
- продолжительность сканирования;
- количество просканированных файлов;
- результаты сканирования или ошибки, обнаруженные во время сканирования.



Правила игнорирования

Если управление приложением ESET Endpoint Security for Android осуществляется удаленно с помощью ESET PROTECT, у пользователя есть возможность указать файлы, которые не будут отнесены к разряду вредоносных. Файлы, добавленные в разделе **Правила игнорирования**, при будущих сканированиях будут игнорироваться. Чтобы создать правило, необходимо указать следующее.

- имя файла с правильным расширением apk;
- имя пакета приложения, например uk.co.extorian.EICARAntiVirusTest;
- имя угрозы, определяемое антивирусными программами, например Android/MobileTX.A (это поле является обязательным).

Эта функция недоступна в приложении ESET Endpoint Security for Android.

Дополнительные параметры

Защита в реальном времени

С помощью этой опции можно включить и отключить сканер реального времени. Этот сканер запускается автоматически с системой и сканирует файлы, с которыми работает пользователь. Он автоматически сканирует папки загрузок, установочные APK-файлы и содержимое SD-карты.

Система репутации ESET LiveGrid®

ESET LiveGrid® — это превентивная система, разработанная для обеспечения более высокого уровня безопасности вашего устройства. Оно непрерывно отслеживает запущенные в системе программы и процессы и сравнивает их с новейшими сведениями, полученными от миллионов пользователей ESET по всему миру. Это позволяет обеспечивать более качественную и точную упреждающую защиту, а также более высокие скорости сканирования для всех пользователей ESET. Рекомендуем включить эту функцию. Рекомендуем включить эту функцию.

Система отзывов ESET LiveGrid®

Эта система обратной связи позволяет нам собирать анонимные статистические сведения, отчеты об аварийном завершении и диагностические данные о подозрительных объектах. Мы автоматически обрабатываем собранную информацию и на ее основании создаем механизмы обнаружения в нашей облачной системе.

Обнаруживать потенциально нежелательные приложения

Потенциально нежелательное — это приложение, которое содержит рекламу, устанавливает панели инструментов, отслеживает результаты поиска или выполняет другие неясные функции. В некоторых ситуациях вы можете решить, что преимущества нежелательного приложения перевешивают риски. Поэтому компания ESET относит эти приложения к категории меньшего риска по сравнению с другими вредоносными программами.

Определять потенциально опасные приложения

Существует множество надежных приложений, которые упрощают администрирование подключенных к сети устройств. Однако злоумышленники могут использовать их для причинения вреда. Опция «Определять потенциально опасные приложения» позволяет отслеживать и блокировать эти приложения.Потенциально опасными приложениями считаются нормальные коммерческие программы. В эту категорию входят средства удаленного доступа, приложения для взлома паролей и клавиатурные шпионы.

Блокировать неразрешенные угрозы

С помощью этого параметра определяется действие, которое будет выполняться после того, как сканирование завершено и обнаружены угрозы. Если включить этот параметр, ESET Endpoint Security for Android будет блокировать доступ к файлам, классифицированным как угрозы.

Съемные носители

Вы можете выбрать действие, когда съемные носители подключаются к устройству:

- **Всегда сканировать** — съемные носители всегда будут сканироваться
- **Не сканировать** — съемные носители не будут сканироваться
- **Показать параметры** — параметр сканирования съемных носителей отображается после подключения носителя

Обновление базы данных модулей обнаружения

Этот параметр позволяет задать периодичность автоматической загрузки обновлений для базы данных угроз. Эти обновления выпускаются, когда в базу данных добавляется новая угроза. Рекомендуется оставить значение по умолчанию («Каждый день»).

Пользовательское значение макс. возраста базы данных

С помощью этой настройки задается время между обновлениями базы данных угроз, по истечении которого пользователь получает уведомление о необходимости обновить ESET Endpoint Security for Android.

Сервер обновлений

С помощью этого параметра устройство можно обновлять с **сервера пре-релизов**. Обновления предварительной версии прошли тщательное внутреннее тестирование и вскоре будут доступны широкой публике. Преимущество их использования заключается в том, что у вас появляется доступ к новейшим методам обнаружения и исправлениям. Однако иногда такие обновления могут быть недостаточно стабильны. Список доступных модулей можно просмотреть в области интерфейса **О программе**. Щелкните значок меню  на главном экране ESET Endpoint Security for Android, а затем выберите **О программе** > **ESET Endpoint Security for Android**. Неопытным пользователям рекомендуется для параметра **Сервер релизов** оставить значение по умолчанию.

Программа ESET Endpoint Security for Android дает возможность создавать копии файлов обновления, которые могут использоваться для обновления других устройств в сети. Использование **локального зеркала** (копии файлов обновления в локальной сети) позволяет избежать загрузки одних и тех же файлов обновления с сервера поставщика всеми

мобильными устройствами. Подробная информация о том, как настроить сервер зеркала, используя продукты ESET Endpoint для Windows, приведена в этом документе.

Антивор

Компонент Антивор защищает мобильное устройство от несанкционированного доступа.

Если вы потеряете свое устройство или кто-то украдет его и заменит вашу SIM-карту на новую (недоверенную), устройство будет автоматически заблокировано ESET Endpoint Security for Android, и на указанные вами номера будет отправлено SMS-сообщение. Оно будет включать телефонный номер новой вставленной SIM-карты, номер IMSI и номер IMEI телефона. Неавторизованный пользователь не узнает об отправке сообщения, поскольку оно будет автоматически удалено из диалогов раздела «Сообщения». Кроме того, вы можете запросить GPS-координаты потерянного устройства или удаленно уничтожить все сохраненные на устройстве данные.

Функция доверенных SIM-карт недоступна на устройствах под управлением ОС Android 10 и более поздних версий.

Возможности компонента «Антивор» помогают администраторам защитить и найти пропавшее устройство. Действия могут запускаться из ESET PROTECT.

Выполняя команду на сервере ESET PROTECT, администратор получает подтверждение на сервере ESET PROTECT.

Сведения о расположении, которые получает администратор, выполняя команду **«Найти»** (если при этом используется решение ESET PROTECT), отображаются в виде GPS-координат.

Команды компонента «Антивор» можно выполнять и с сервера ESET PROTECT. Новые функции управления мобильными устройствами позволяют администраторам быстро выполнить любую команду компонента «Антивор». Новый компонент передачи и обработки команд (Mobile Device Connector), ставший частью инфраструктуры ESET PROTECT, позволяет без задержек передавать задачи на выполнение.

Контакты администратора

Речь идет о списке, который включает в себя номера телефонов администратора и который защищен администраторским паролем. Команды компонента «Антивор» можно отправлять только с доверенных номеров. Кроме того, на них приходят уведомления о действиях этого компонента.

Добавление контактов администратора

Имя и номер телефона администратора нужно вводить, когда работает мастер запуска компонента «Антивор». Если контакт содержит более одного номера телефона, то учитываться будут все номера.

Контакты администратора можно добавить или изменить в разделе **Антивор** > **Контакты**

администратора.

Информация на заблокированном экране

Администратор может указать, какая информация может отображаться на экране заблокированного устройства (имя компании, адрес электронной почты, сообщение). При этом можно включить звонок одному из предварительно заданных контактов администратора.

Отображаться может следующая информация:

- имя компании (необязательно);
- Электронная почта (необязательно)
- пользовательское сообщение.

Доверенные SIM-карты

В области интерфейса **Доверенная SIM-карта** отображается список SIM-карт, которые приложение ESET Endpoint Security for Android считает доверенными. Если вставить SIM-карту, которой в списке нет, экран будет заблокирован и администратору будет отправлено SMS-оповещение.

Чтобы добавить новую SIM-карту, коснитесь значка ➕. Введите **имя** SIM-карты (например, «Дом», «Работа») и ее идентификатор IMSI (International Mobile Subscriber Identity — международный идентификатор абонента мобильной связи). Идентификатор IMSI обычно нанесен на SIM-карту и состоит из 15 цифр. Иногда он может быть короче.

Чтобы удалить SIM-карту, коснитесь имени карты и задержите на нем палец, а затем коснитесь значка 🗑.

Функция доверенных SIM-карт недоступна на устройствах под управлением ОС Android 10 и более поздних версий.

Функция «Доверенная SIM-карта» недоступна на устройствах CDMA и WCDMA, а также на устройствах, в которых используется только WiFi.

Удаленные команды

Удаленные команды могут запускаться непосредственно из консоли ESET PROTECT:

Поиск устройства

Вы получите текстовое сообщение, содержащие GPS-координаты целевого устройства и ссылку на его расположение на картах Google. Через 10 минут устройство отправит еще одно сообщение, если появятся более точные координаты местонахождения.

Блокировать устройство

Эта команда заблокирует устройство. Впоследствии вы сможете разблокировать его с помощью пароля администратора или удаленной команды разблокировки.

Разблокировка заблокированного устройства

Устройство будет разблокировано, а используемая в устройстве SIM-карта будет сохранена как доверенная.

Сирена/сигнал режима утери

Устройство будет заблокировано, и в течение пяти минут (или до момента разблокировки) будет воспроизводиться очень громкий звук. Громкий звук сирены будет воспроизводиться, даже если на устройстве отключен звук.

Расширенный сброс до заводских установок

На устройстве будут восстановлены заводские настройки. Все доступные данные будут удалены, а заголовки файлов будут уничтожены. Процесс может занять несколько минут.

Контроль приложений

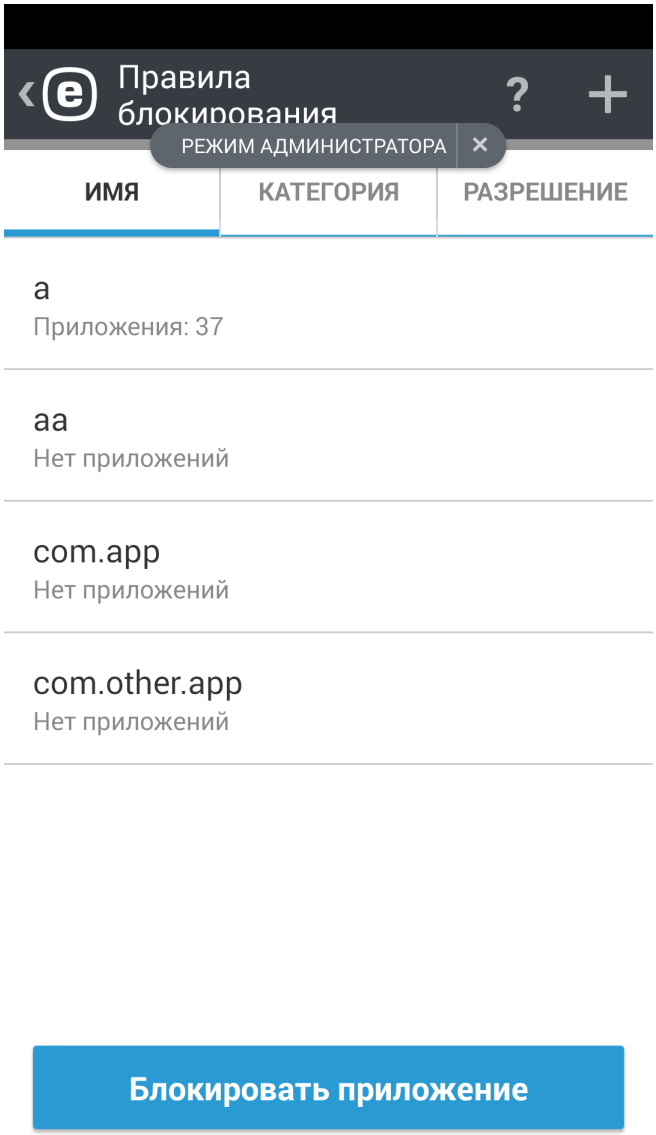
Контроль приложений позволяет администраторам отслеживать установленные приложения, блокировать доступ к определенным приложениям и снижать степень риска, предлагая пользователям удалить некоторые программы. Администратору доступны следующие способы фильтрации приложений:

- блокировка приложений, указанных вручную;
- блокировка приложений по категориям (например, игры или программы для общения);
- блокировка на основе разрешений (например, программы, которые отслеживают расположение пользователя);
- Блокировка по источникам (например, приложений, установленных не из магазина Google Play).

Правила блокировки

В области интерфейса **Контроль приложений** > **Блокирование** > **Правила блокировки** можно создавать правила блокирования приложений на основании следующих критериев:

- имя приложения или пакета;
- категория;
- разрешения



Блокировка по имени приложения

С помощью ESET Endpoint Security for Android администратор может блокировать приложения по их имени или по имени пакета. В разделе **Правила блокировки** представлены общие сведения о созданных правилах и список заблокированных приложений.

Для изменения существующего правила коснитесь и удерживайте его, а затем выберите пункт **Изменить**. Чтобы удалить из списка несколько записей с правилами, коснитесь одного правила и задержите на нем палец, а затем выделите остальные правила, которые нужно удалить, после чего выберите команду **Удалить**. Чтобы удалить все правила в списке, коснитесь элемента **ВЫДЕЛИТЬ ВСЕ** и выберите команду Удалить.

Блокируя приложение по имени, ESET Endpoint Security for Android будет искать точное соответствие с именем запущенного приложения. При изменении языка интерфейса программы ESET Endpoint Security for Android необходимо повторно ввести имя приложения для этого языка, чтобы продолжить его блокировку.

Во избежание возможных проблем, связанных с локализованными именами приложений, рекомендуется блокировать такие приложения по имени пакета — уникальному

идентификатору, который не может быть изменен во время выполнения или повторно использован другим приложением.

При наличии прав локального администратора пользователь может найти имя пакета приложения, выбрав **Контроль приложений** > **Отслеживание** > **Разрешенные приложения**. Если коснуться значка приложения, отобразится экран **Подробности**, содержащий имя пакета приложения. Чтобы заблокировать приложение, выполните следующие действия.

Блокировка приложений по имени

1.Последовательно коснитесь элементов **Контроль приложений** > **Блокирование** > **Блокировать приложение** > **Блокировать по имени**.

2.Укажите, по какому свойству нужно блокировать приложения: по имени приложения или по имени пакета.

3.Введите слова, которые должны присутствовать в имени, чтобы приложение было заблокировано. Для разделения нескольких слов используйте запятую (,).

Например, если в поле **Имя приложения** ввести слово «*poker*», будут заблокированы все приложения, имена которых содержат слово «*poker*». Если в поле **Имя пакета ввести** «*com.poker.game*», программа ESET Endpoint Security for Android заблокирует только одно приложение.

Блокировка по категории приложений

Приложение ESET Endpoint Security for Android позволяет администратору блокировать приложения, относящиеся к тем или иным предварительно заданным категориям. В разделе **Правила блокировки** доступны сводные сведения о созданных правилах и список заблокированных приложений.

Если нужно изменить существующее правило, коснитесь его имени и задержите на нем палец, а затем коснитесь команды **Изменить** .

Чтобы удалить несколько правил из списка, коснитесь одного правила и задержите на нем палец, затем выберите остальные правила, которые нужно удалить, и выберите команду **Удалить** . Чтобы удалить все правила в списке, коснитесь элемента **ВЫДЕЛИТЬ ВСЕ**.

Блокировка приложений по категориям

1.Последовательно коснитесь элементов **Контроль приложений** > **Блокировка** > **Блокировать приложение** > **Блокировать по категории**.

2.Установите флажки напротив предварительно заданных категорий и нажмите кнопку **Блокировать**.

Блокировка приложений по типу разрешений

Программа ESET Endpoint Security for Android позволяет администратору блокировать приложения на основании их разрешений. В разделе **Правила блокировки** доступны сводные сведения о созданных правилах и список заблокированных приложений.

Если нужно изменить существующее правило, коснитесь его имени и задержите на нем палец, а затем коснитесь команды **Изменить** .

Чтобы удалить несколько правил из списка, коснитесь одного правила и задержите на нем палец, затем выберите остальные правила, которые нужно удалить, и выберите команду **Удалить** . Чтобы удалить все правила в списке, коснитесь элемента **ВЫДЕЛИТЬ ВСЕ**.

Блокировка приложений по типу разрешений

1.Последовательно коснитесь элементов **Контроль приложений** > **Блокирование** > **Блокировать приложение** > **Блокировать по типу разрешений**.

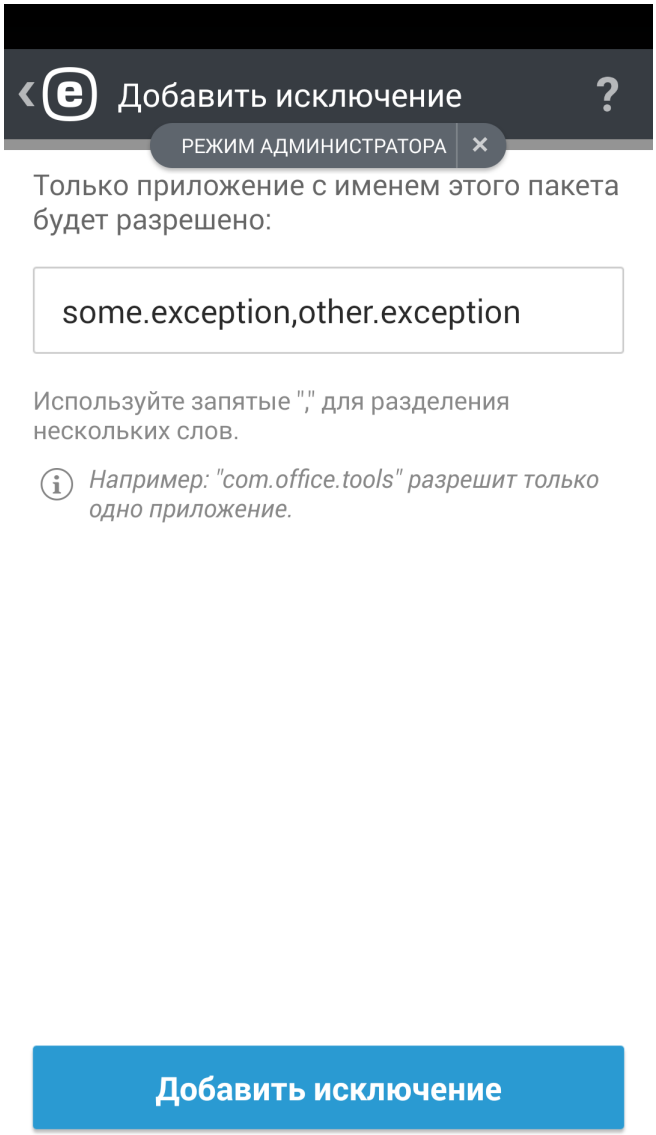
2.Установите флажки напротив разрешений и нажмите кнопку **Блокировать**.

Блокировка неизвестных источников

По умолчанию ESET Endpoint Security for Android не блокирует приложения, полученные из Интернета или любого другого источника, кроме магазина Google Play. В области интерфейса **Заблокированные приложения** доступны сводные сведения о заблокированных программах (имя пакета, применяемое правило), а также возможность удалить приложение или добавить его в «белый» список (находящийся в области интерфейса **Исключения**).

Исключения

Чтобы удалить ту или иную программу из списка заблокированных приложений, можно создать исключения. Для этого нажмите **Контроль приложений** > **Блокирование** > **Исключения** > **Добавить исключение**. Администраторы, управляющие приложением ESET Endpoint Security for Android удаленно, могут с помощью этой новой функции определять, соответствует ли то или иное устройство корпоративной политике относительно установленных приложений.



Добавление исключений

Приложение можно не только исключить (путем ввода имени пакета приложения), но и добавить в «белый» список, удалив его из списка **Заблокированные приложения**:

1. В приложении ESET Endpoint Security for Android нажмите **Контроль приложений**.
2. Нажмите **Блокирование** > **Заблокированные приложения**.
3. Выберите приложение, которое нужно добавить в белый список.
4. Нажмите значок с тремя точками в правом верхнем углу, а затем нажмите **Добавить исключение**.
5. Введите пароль администратора и нажмите **ВВОД**.

Обязательные приложения

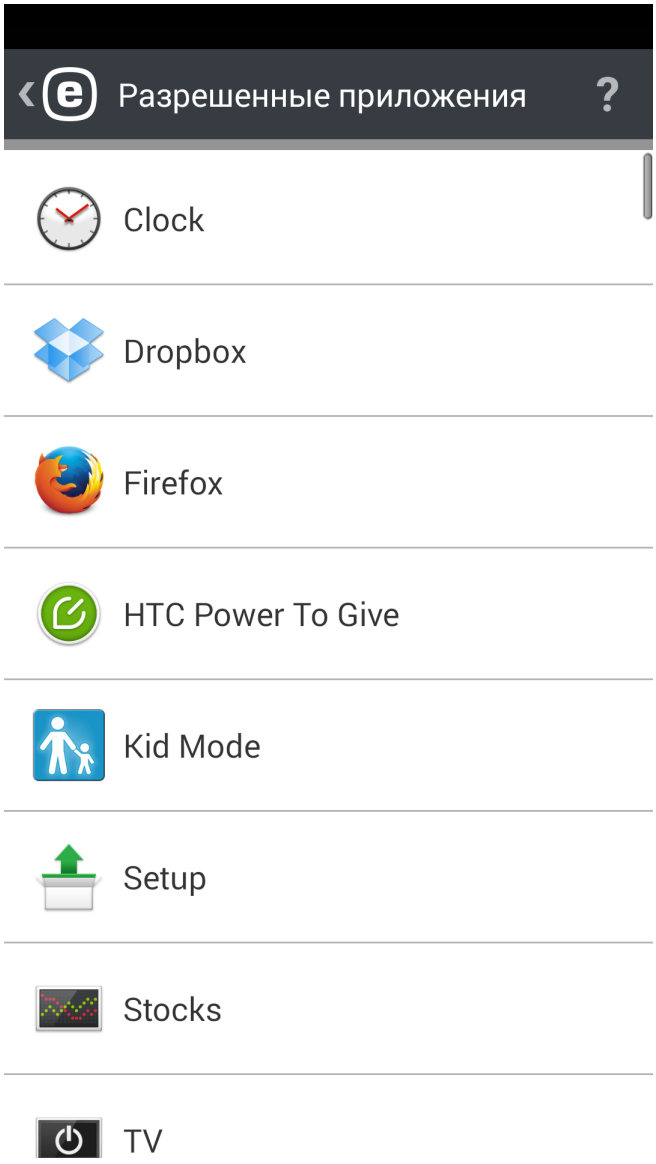
Если управление приложением ESET Endpoint Security for Android осуществляется удаленно с помощью ESET PROTECT, у пользователя есть возможность указать приложения, которые должны быть установлены на целевых устройствах. Необходимо указать следующие сведения:

- имя приложения, отображаемое для пользователя;
- уникальное имя пакета приложения, например *com.eset.ems2.gp*;
- URL-адрес, по которому пользователь может найти ссылку для загрузки. Можно также использовать ссылки Google Play, например https://play.google.com/store/apps/details?id=com.eset.ems2.gp.

Эта функция недоступна в приложении ESET Endpoint Security for Android.

Разрешенные приложения

Этот раздел содержит информацию об установленных приложениях, которые не блокируются согласно правилам блокировки.

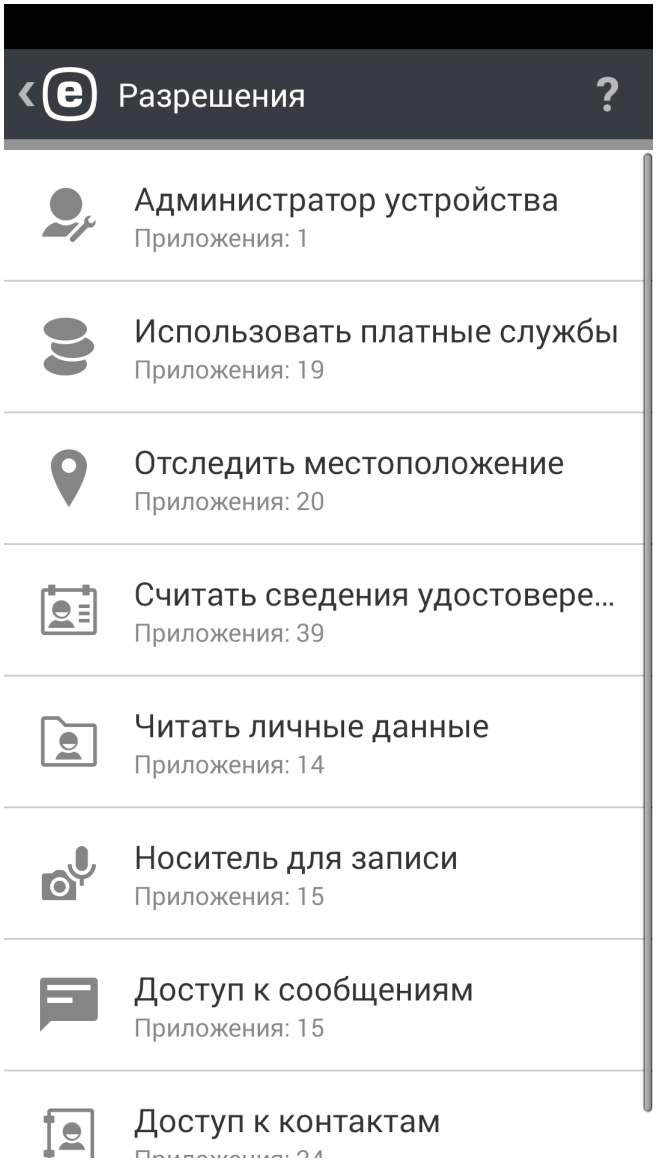


Разрешения

Эта функция отслеживает поведение приложений, у которых есть доступ к личным или корпоративным данным. Кроме того, используя предварительно заданные категории разрешений, администраторы могут контролировать, к каким данным приложения получают доступ.

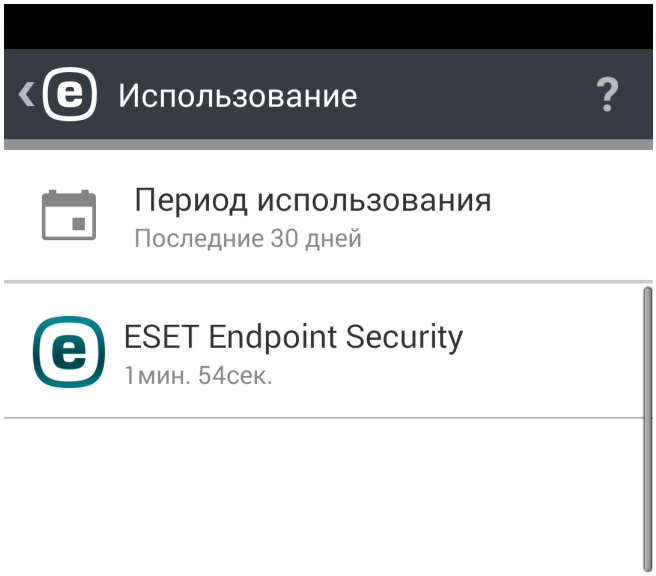
Некоторые приложения, установленные на вашем устройстве могут иметь доступ к платным услугам, отслеживать ваше местоположение либо считывать ваши идентификационные данные, контакты или текстовые сообщения. ESET Endpoint Security for Android проводит аудит таких приложений.

Этот раздел содержит список приложений, отсортированных по категориям. Выберите категорию, чтобы увидеть ее подробное описание. Сведения о разрешениях отдельного приложения можно получить, нажав на это приложение.



Использование

В этой области интерфейса администратор может отслеживать, сколько времени пользователь работает с тем или иным приложением. Чтобы отфильтровать общие сведения по периоду использования, используйте параметр **Интервал**.

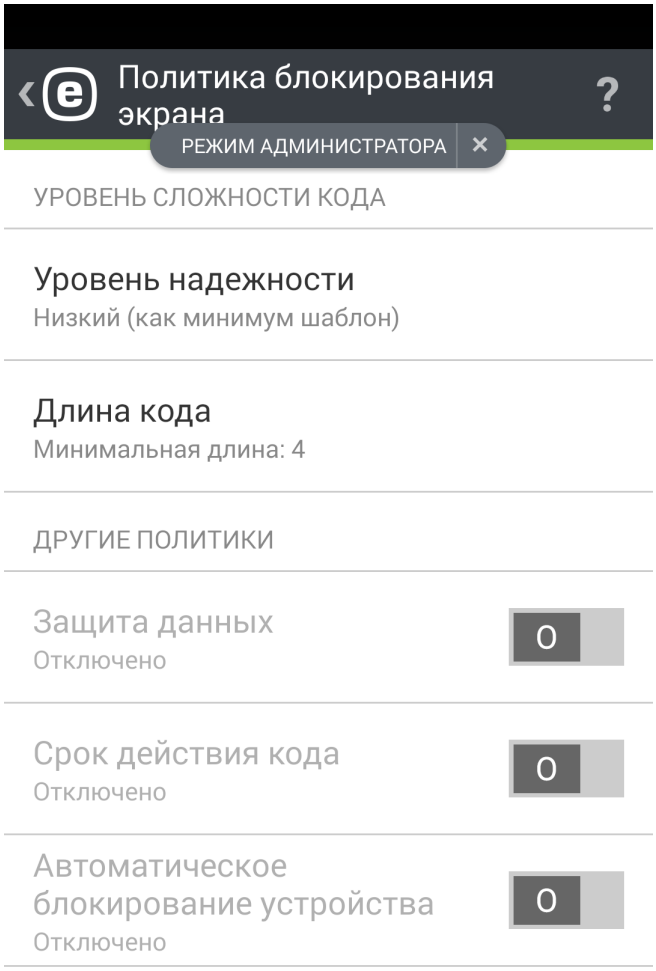


Безопасность устройства

В разделе **Безопасность устройства** администратор может:

- выполнять базовые политики безопасности на мобильных устройствах и определять политики, касающиеся важных параметров устройства;
- указывать необходимый уровень сложности разблокировки экрана;
- ограничивать использование встроенной камеры.

Политика блокирования экрана



В этой области интерфейса администратор может выполнить следующие действия:

- задать минимальный уровень безопасности (разблокировка экрана с помощью графического ключа, PIN-кода или пароля) и настроить сложность кода блокирования экрана (например, минимальную длину);
- указать максимальное количество неудачных попыток разблокировки, после которых настройки устройства будут сброшены до заводских;
- указать максимальный возраст кода блокирования экрана;
- настроить таймер блокировки экрана;

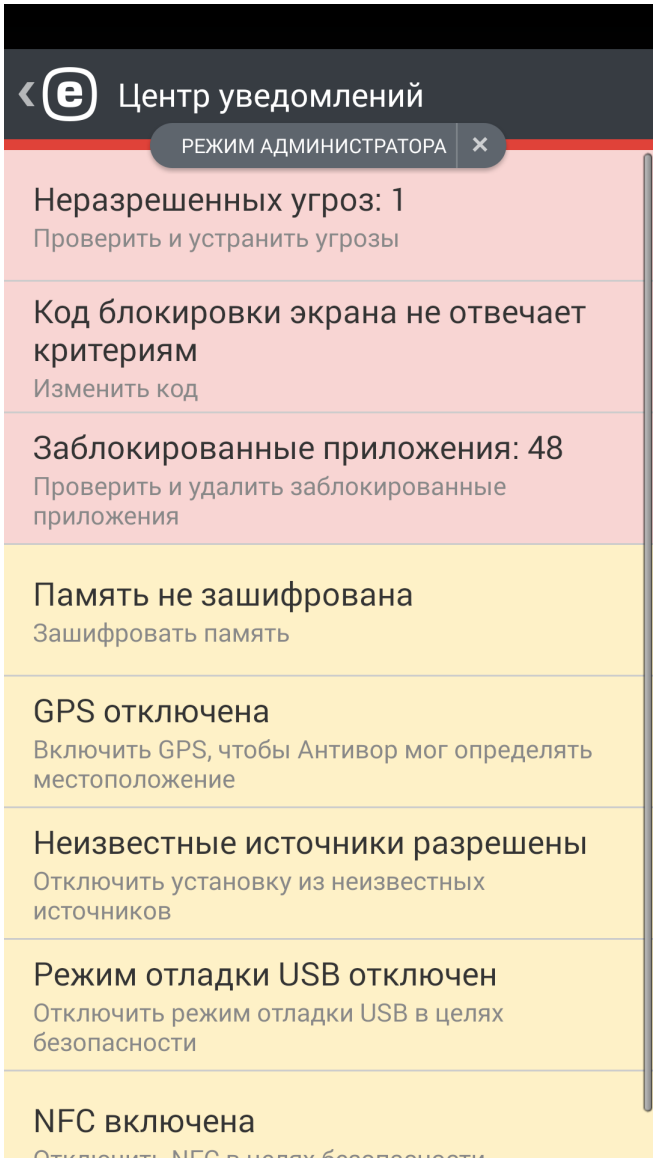
Решение ESET Endpoint Security for Android автоматически уведомляет пользователя и администратора, соответствуют ли текущие параметры устройства корпоративным политикам безопасности. Если устройство политикам не соответствует, приложение автоматически предлагает пользователю возможное решение проблемы.

Политика настроек устройства

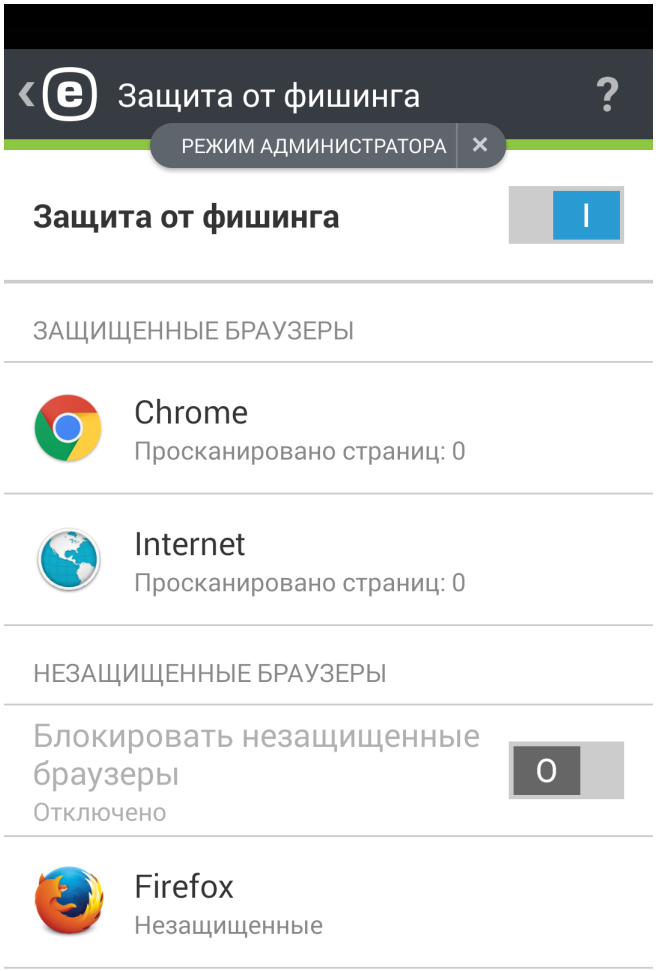
Компонент «Безопасность устройства» включает также возможность использования **политики настроек устройства** (раньше входила в компонент **«Аудит безопасности»**). С помощью этой политики системный администратор может контролировать предварительно заданные настройки устройства.

Настраивать в устройстве можно следующее:

- Wi-Fi
- спутники GPS,
- Службы определения местоположения
- Память
- передача данных в роуминге,
- вызовы в роуминге,
- неизвестные источники,
- режим отладки,
- NFC,
- шифрование памяти.
- На устройстве получены права суперпользователя root



Защита от фишинга



Фишинг — это преступная деятельность с использованием социальной инженерии (манипулирование пользователями для получения конфиденциальной информации). Фишинг часто используется для получения доступа к такой конфиденциальной информации, как номера банковских счетов, номера кредитных карт, PIN-коды или имена пользователей и пароли.

Рекомендуется оставить функцию **Защиты от фишинга** включенной. ESET Endpoint Security for Android сканирует URL-адреса — все потенциальные фишинговые атаки с веб-сайтов или доменов, занесенных компанией ESET в базу данных вредоносных объектов, блокируются, а для пользователя отображается уведомление об атаке.

ВАЖНО! Компонент защиты от фишинга интегрируется с самыми распространенными веб-браузерами, доступными в ОС Android. В большинстве случаев защита от фишинга доступна для браузеров Chrome, Firefox, Opera, Opera Mini, Dolphin, Samsung и стандартных браузеров, предварительно устанавливаемых на устройствах Android. Другие браузеры будут отображаться как незащищенные, и доступ к ним можно заблокировать с помощью переключателя O.

Чтобы функция защиты от фишинга ESET работала правильно, в настройках системы Android необходимо включить параметр **Доступность**.

Включение разрешения «Специальные возможности» для решения ESET Endpoint Security for Android, установленного с помощью APK-файла в Android 13

> **Примечание**
> Из соображений безопасности использование разрешения «Специальные возможности» в Android 13 ограничено для приложений, установленных с помощью APK-файлов. Во избежание неинформированного доступа к этим разрешениям.
>
> **Как это разрешение используется в ESET Endpoint Security for Android**
> Мы используем это разрешение для доступа к URL-адресам посещаемых вами веб-сайтов. Мы анализируем эти веб-сайты на предмет вредоносных намерений, например фишинга, вредоносных программ или других опасных действий.
> При обнаружении угрозы веб-сайт блокируется для защиты вас и вашей конфиденциальной информации.
> Данные, доступ к которым получен с помощью разрешения \"Специальные возможности\", третьим лицам не передаются.

Чтобы устранить проблему с разрешением «Специальные возможности», выполните следующие действия.

1. Откройте раздел **Настройки** > **Специальные возможности** > **Загруженные приложения**, где решение ESET Endpoint Security for Android будет отображаться неактивным.

2. Нажмите приложение ESET Endpoint Security for Android, после чего откроется диалоговое окно **Ограниченная настройка**.

3. Нажмите кнопку **OK.**

4. Перейдите в раздел **Настройки** > **Приложения** > ESET Endpoint Security for Android, чтобы открыть **информацию о приложении**.

5. Нажмите значок меню с тремя точками ⋮ в правом верхнем углу > **Разрешить ограниченные настройки**.

Теперь разрешение «Специальные возможности» включено, и вы можете начать использование приложения.

Контроль доступа в Интернет

Настроив параметры функции «Контроль доступа в Интернет», можно защитить свою компанию от возможной юридической ответственности. Например, с помощью данной функции можно управлять доступом к веб-сайтам, которые нарушают права на интеллектуальную собственность. Цель заключается в предотвращении доступа сотрудников к страницам с неприемлемым или опасным содержимым, а также к ресурсам, посещение которых отрицательно влияет на эффективность работы.

Работодатели или системные администраторы могут запрещать доступ к более чем 27 предварительно заданным категориям веб-сайтов, включая более 140 подкатегорий, а также могут регистрировать такие визиты в журнале.

Контроль доступа в Интернет — это управляемая функция. Все настройки можно изменять с помощью ESET PROTECT Cloud.

Для правильной работы функции «Контроль доступа в Интернет» управляемое устройство должно соответствовать следующим требованиям:
• ESET Endpoint Security for Android версии 3 и выше.
• Android версии 8 и выше.
• Устройство должно быть зарегистрировано в ESET PROTECT Cloud с разрешениями администратора устройства.

Защищенные браузеры

- Chrome
- Chrome Beta
- Firefox
- Firefox Beta
- Opera
- Opera Beta
- Opera Mini
- Opera Mini Beta
- Браузер Opera TV
- Samsung Internet
- Mint
- Браузер Яндекс
- DuckDuckGo
- Браузер Kiwi
- Edge
- Silk на устройствах Amazon
- Браузер Mi
- Браузер Xiaomi Mi
- Vewd в Android TV
- Кроме того, под защитой находятся приложения, в которых используются защищенные компоненты браузера для просмотра веб-страниц.

Фильтрация вызовов

Фильтр звонков блокирует входящие и исходящие звонки в соответствии с правилами, заданными пользователем.

При блокировке входящего звонка уведомление не отображается. Благодаря этому вас не будет отвлекать нежелательная информация. При этом вы всегда сможете проверить журналы на наличие звонков, которые могли быть заблокированы по ошибке.

Фильтрация вызовов не работает на планшетах, которые не поддерживают телефонные звонки.

Чтобы блокировать звонки с последнего входящего номера телефона, коснитесь элемента **Заблокировать последнего звонящего**. В результате будет создано правило.

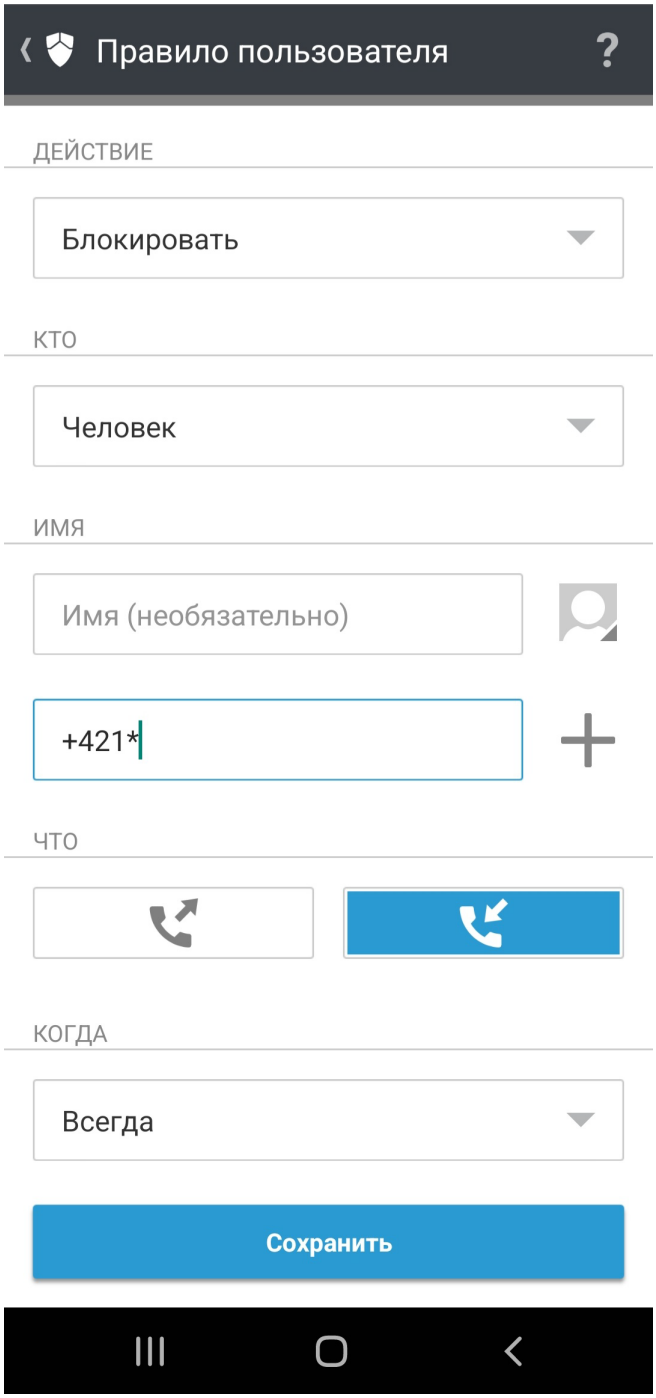
Блокировка телефонных номеров с помощью подстановочных знаков

С помощью подстановочных знаков, описанных в таблице ниже, можно заблокировать диапазон номеров.

Подстановочный знак	Описание
*	заменяет несколько символов
?	заменяет один символ

Пример

Если вы не хотите получать звонки из определенной страны, введите код страны и подстановочный знак * в поле **Номер мобильного телефона**, и все входящие звонки из страны с такой последовательностью цифр будут блокироваться. Если вы решите сделать исключение для какого-либо номера телефона из этой страны, добавьте новое правило с действием **Разрешить**. На изображении ниже показано, как заблокировать все звонки из Словакии.



Правила

Пользователь может создавать пользовательские правила, не вводя пароль администратора. Правила администратора можно создавать только в режиме администратора. Пользовательские правила переопределяются правилами администратора.

Дополнительные сведения о создании правил можно найти в этом разделе.

Если нужно удалить существующее правило из списка **Правила**, коснитесь имени правила и задержите на нем палец, а затем коснитесь значка **Удалить** .

Добавление нового правила

Чтобы добавить новое правило, нажмите **Добавить правило** или коснитесь значка ➕ в правом верхнем углу экрана **Правила**.

Выберите контакт или группу телефонных номеров. Приложение ESET Endpoint Security for Android распознает сохраненные на телефоне группы контактов (например, «Семья», «Друзья» или «Сотрудники»). Параметр **Все неизвестные номера** относится ко всем телефонным номерам, не сохраненным в списке контактов. С помощью этого параметра можно заблокировать нежелательные телефонные звонки (например, рекламные) или запретить сотрудникам звонить на неизвестные номера. Параметр **Все известные номера** относится ко всем телефонным номерам, сохраненным в списке контактов. Параметр «**Скрытые номера**» относится к абонентам, которые намеренно скрывают свои номера с помощью услуги «антиопределитель номера».

Укажите, что нужно разрешать или блокировать:

-  исходящие звонки
-  входящие звонки

Чтобы применить правило только на указанный период времени, последовательно коснитесь элементов **Всегда** > **Выборочная** и укажите дни недели и промежуток времени. По умолчанию выбраны суббота и воскресенье. Эта функция может пригодиться, например, если вы не хотите, чтобы вас беспокоили во время совещаний, командировок, ночью или на выходных.

ПРИМЕЧАНИЕ. Если вы находитесь за границей, все телефонные номера в списке должны включать международный телефонный (например, +1610100100).

Журнал

В области интерфейса **История** отображаются звонки и сообщения, которые заблокировал или разрешил фильтр звонков. Каждый журнал содержит следующие сведения: имя события, соответствующий номер телефона, дата и время события.

Если нужно изменить правило, связанное с заблокированным номером телефона или контактом, коснитесь записи в списке, чтобы выбрать ее, а затем коснитесь значка .

Чтобы удалить запись из списка, выберите ее и коснитесь значка . Чтобы удалить несколько записей, коснитесь одной из них и задержите на ней палец, выберите остальные ненужные записи и коснитесь значка .

Параметры

Язык – По умолчанию приложение ESET Endpoint Security for Android устанавливается на языке, который выбран в качестве языка системы на устройстве (настройки языка и клавиатуры в ОС Android). Чтобы изменить язык интерфейса приложения, нажмите «Язык» и сделайте свой

выбор.

Страна – Выберите страну, в которой вы работаете или находитесь в настоящий момент.

Обновление – Чтобы обеспечить максимальную защиту, важно использовать самую последнюю версию ESET Endpoint Security for Android. Чтобы узнать, доступна ли более новая версия на веб-сайте ESET, нажмите Обновление.

ИД устройства – Установите или измените идентификационное имя устройства для администратора на случай кражи или утери устройства.

Удаленное управление – Подключите устройство к решению ESET PROTECT.

Дополнительные параметры

Щелкните **Дополнительные параметры**, чтобы открыть раздел «Дополнительные параметры».

Уведомления о разрешениях — см. раздел Управление разрешениями.

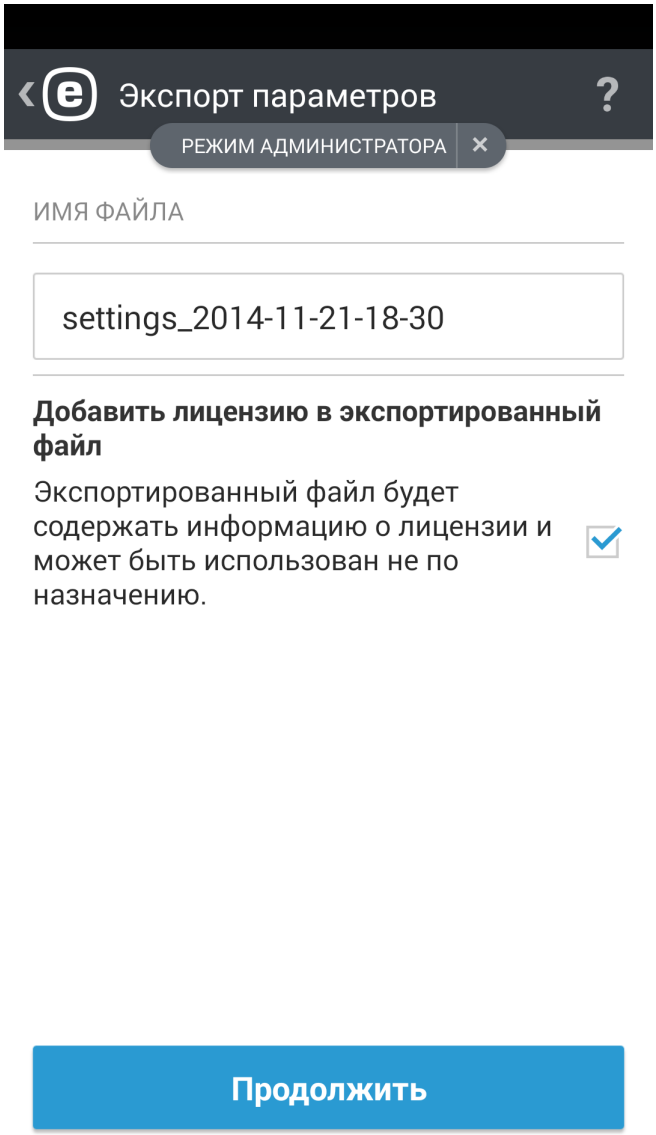
Отправить данные об использовании – Этот параметр помогает улучшать продукты ESET путем отправки анонимных данных об использовании приложения. Конфиденциальная информация не отправляется. Если этот параметр не был включен с помощью мастера начальной настройки на этапе установки, это можно сделать в разделе Параметры > Дополнительные параметры.

Пароль администратора – Этот параметр позволяет создать пароль администратора или изменить существующий. Дополнительные сведения см. в разделе Пароль администратора данного документа.

Импорт и экспорт параметров – Импорт или экспорт настроек в приложении ESET Endpoint.

Импорт и экспорт параметров

Чтобы обеспечить простую передачу настроек между двумя мобильными устройствами, которые не управляются с помощью ESET PROTECT, решение ESET Endpoint Security for Android дает возможность экспортировать и импортировать настройки программы. Администратор может вручную экспортировать настройки устройства в файл, который затем можно передать (например, по электронной почте) и импортировать на любое устройство, на котором запущено клиентское приложение. Когда пользователь принимает полученный файл с настройками, происходит автоматическое применение всех настроек и активация приложения (если в файл были добавлены сведения о лицензии). Все настройки будут защищены паролем администратора.



Экспортировать параметры

Чтобы экспортировать текущие параметры приложения ESET Endpoint Security for Android, укажите имя файла параметров (текущие дата и время будут вставлены автоматически). В экспортируемый файл можно добавить также сведения о лицензии (лицензионный ключ или адрес электронной почты и пароль к учетной записи администратора безопасности), однако помните, что эта информация не будет зашифрована и может быть использована в преступных целях.

На следующем этапе выберите способ передачи файла:

- по сети Wi-Fi,
- через Bluetooth,
- по электронной почте,
- через приложение Gmail,
- через диспетчер файлов (например, ASTRO File Manager или ES File Explorer).

Импорт параметров

Чтобы импортировать настройки из файла, который находится на устройстве, с помощью приложения для работы с файлами найдите файл настроек и выберите ESET Endpoint Security for Android.

Также параметры можно импортировать, выбрав файл в разделе **История**.

Журнал

История отображает список импортированных файлов с параметрами. Тут эти файлы можно передавать другим пользователям, импортировать и удалять.

Пароль администратора

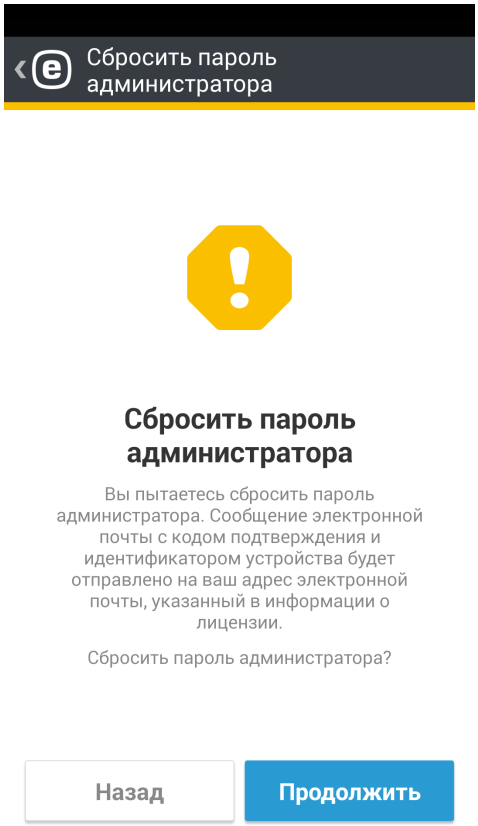
Пароль **администратора** требуется для разблокировки устройства, отправки команд модуля Антивор, доступа к защищенным паролем функциям и удаления ESET Endpoint Security for Android.

После создания **пароля администратора** блокируется возможность пользователей изменять настройки и удалять ESET Endpoint Security for Android.

Подойдите к вопросу выбора пароля со всей серьезностью. Чтобы улучшить безопасность, используйте сочетание цифр, строчных и прописных букв.

Чтобы сбросить пароль администратора на устройстве с заблокированным экраном, выполните такие действия:

1. Нажмите **Восстановление пароля** > **Продолжить** > **Запросить код проверки**. Если устройство не подключено к Интернету, вместо этого нажмите ссылку **выбрать сброс в автономном режиме** и свяжитесь со службой технической поддержки клиентов ESET.



2. На адрес электронной почты, связанный с лицензией ESET, будет отправлено электронное письмо с кодом проверки и идентификатором устройства. Код проверки будет действовать в течение семи дней. Введите код проверки и новый пароль на заблокированном экране вашего устройства.

Удаленное управление

ESET PROTECT позволяет централизовано управлять приложением ESET Endpoint Security for Android в сетевой среде.

Использование ESET PROTECT не только повышает уровень безопасности, но и упрощает администрирование всех программ ESET установленных на клиентских рабочих станциях и мобильных устройствах. Устройства, на которых установлено приложение ESET Endpoint Security for Android могут подключаться к ESET PROTECT, используя любой тип подключения к Интернету — по сети WiFi, LAN, WLAN, сети сотовой связи (3G, 4G LTE, HSDPA, GPRS) и т. д. При этом требуется, чтобы подключение к Интернету было обычным (без использования прокси-сервера или файервола) и чтобы обе конечные точки были правильно настроены.

Успешное подключение к ESET PROTECT по сотовой сети зависит от поставщика услуг мобильной связи и требует полноценного Интернет-соединения.

Чтобы подключить устройство к ESET PROTECT, добавьте устройство в список Компьютеры в веб-консоли ESET PROTECT, зарегистрируйте устройство с помощью задачи **Регистрация устройства** и введите **адрес сервера средства подключения для мобильных устройств**.

В ESET PROTECT ссылка для регистрации (адрес сервера средства подключения для мобильных устройств) имеет стандартный формат `https://MDCserver:port/token`. Ссылка содержит следующие значения:

- **MDCserver** — полное DNS-имя или общедоступный IP-адрес сервера, на котором запущено средство Mobile Device Connector (MDC). Имя хоста может использоваться только в том случае, если подключение выполняется через внутреннюю сеть Wi-Fi.

- **Port** — номер порта, который используется для подключения к средству Mobile Device Connector.

- **Маркер** — строка, содержащая набор символов, генерируемый администратором в веб-консоли ESET PROTECT

Дополнительные сведения о том, как управлять сетью с помощью решения ESET PROTECT, доступны в следующих разделах интернет-справки:

- Управление политиками

- Создание клиентских задач

- Сведения об отчетах

ИД устройства

ИД устройства поможет администратору идентифицировать устройство, если оно потеряется или его украдут.

Управление разрешениями

В ОС Android 6 (Marshmallow) компания Google представила новую систему управления разрешениями. Приложение ESET Endpoint Security for Android совместимо с этой системой. Приложения, предназначенные для Android 6.0, будут запрашивать разрешения, как только вы попытаетесь запустить их. Вместо предоставления приложению доступа во время установки пользователь получает запрос при первой попытке доступа приложения к определенной функции устройства.

ESET Endpoint Security for Android запрашивает разрешение на доступ к следующим функциям.

- **Доступность** — требуется для надлежащей работы функции Защиты от фишинга ESET.

- **Контакты** — требуется для модуля Антивор и Фильтрация вызовов

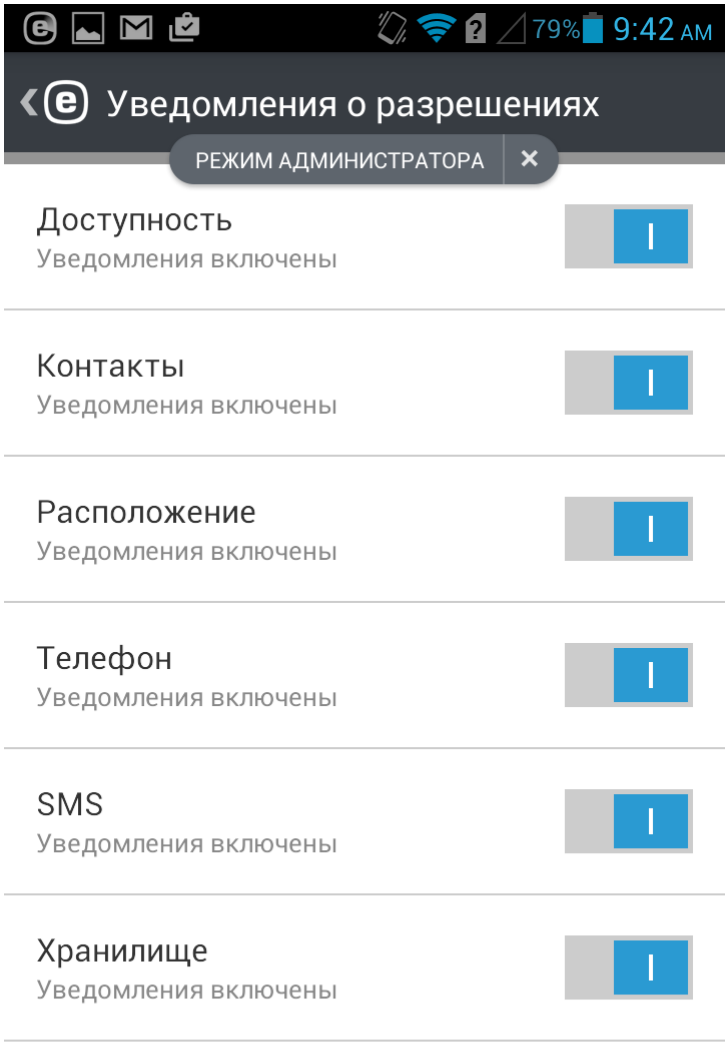
- **Расположение** — требуется для модуля Антивор.

- **Телефон** — требуется для модуля Антивор и Фильтрация вызовов

- **SMS** — требуется для модуля Антивор и Фильтрация вызовов

- **Хранилище** — требуется для функции защиты от вирусов и модуля Антивор.

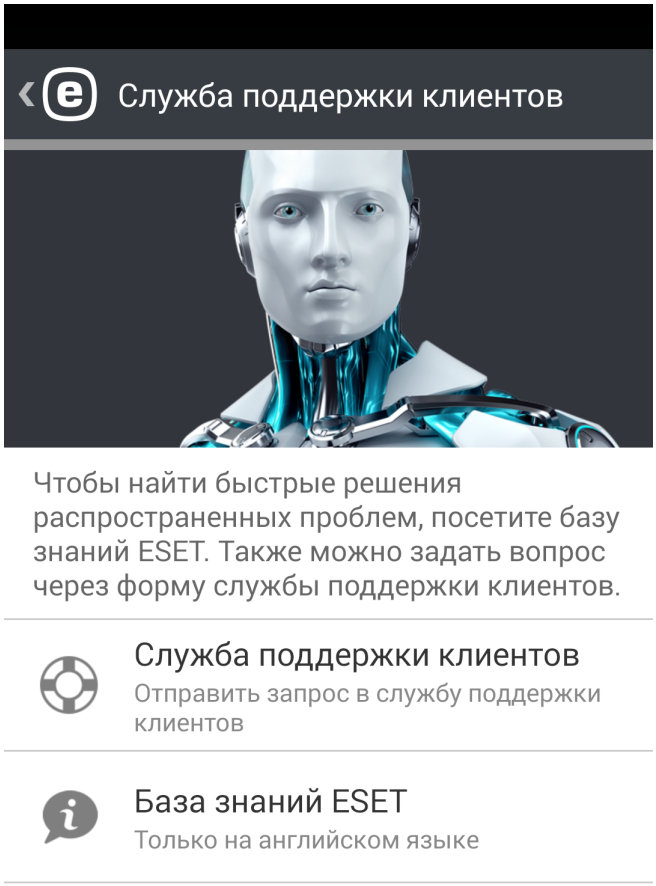
Администратор может отключить мониторинг этих разрешений в разделе **Параметры** > **Уведомления о разрешениях**.



Служба технической поддержки клиентов

Специалисты службы технической поддержки клиентов ESET окажут административную и техническую помощь по ESET Endpoint Security for Android и остальным продуктам ESET.

Чтобы отправить запрос в службу поддержки со своего устройства, коснитесь значка меню на главном экране ESET Endpoint Security for Android, последовательно выберите элементы **Служба поддержки клиентов** > **Служба технической поддержки клиентов** и заполните все обязательные поля.



В приложении ESET Endpoint Security for Android улучшены функции расширенного ведения журналов, что позволяет лучше диагностировать потенциальные технические проблемы. Для предоставления специалистам ESET подробного журнала приложения убедитесь, что выбран параметр **Отправить журнал приложения** (по умолчанию). Нажмите кнопку **Отправить**, чтобы отправить запрос. Специалист службы технической поддержки клиентов ESET свяжется с вами по указанному электронному адресу.

Программа улучшения пользовательского опыта

Присоединившись к программе улучшения пользовательского опыта, вы предоставляете компании ESET анонимные сведения об использовании наших продуктов. Дополнительные сведения об обработке данных доступны в нашей политике конфиденциальности.

Ваше согласие

Участие в программе является добровольным и зависит от вашего согласия. После присоединения вы пассивно участвуете в программе, то есть вам не нужно предпринимать

каких-либо дальнейших действий. В любой момент вы можете отозвать свое согласие, изменив настройки продукта. Сделав так, вы запретите нам обрабатывать ваши анонимные данные.

Какие виды информации мы собираем?

Данные о взаимодействии с продуктом

Эти сведения показывают нам, как используются наши продукты. Благодаря этому мы знаем, например, какие функции используются часто, какие настройки пользователи изменяют и сколько времени они тратят на использование продукта.

Данные об устройствах

Мы собираем эти сведения, чтобы понять где и на каких устройствах используются наши продукты. Типичные примеры таких сведений: модель устройства, страна, версия и имя операционной системы.

Данные диагностики ошибок

Собираются также сведения о возникновении ошибок и аварийных ситуаций. Например, какая ошибка произошла, и какие действия привели к ней.

Почему мы собираем эту информацию?

Эти анонимные сведения дают нам возможность улучшать наши продукты для вас, наших пользователей. Они помогают сделать их максимально полезными, простыми в использовании и свободными от ошибок.

Кто контролирует эту информацию?

Компания ESET, spol. s r.o. является единственным контролером данных, собираемых в рамках Программы. Эта информация не сообщается третьим лицам.

Лицензионное соглашение с конечным пользователем

Вступает в силу с 19 октября 2021 года.

ВАЖНО! Внимательно прочитайте изложенные далее условия использования программного продукта, прежде чем загружать, устанавливать, копировать или использовать его. **ЗАГРУЖАЯ, УСТАНАВЛИВАЯ, КОПИРУЯ ИЛИ ИСПОЛЬЗУЯ ЭТО ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ, ВЫ ВЫРАЖАЕТЕ СВОЕ СОГЛАСИЕ С ИЗЛОЖЕННЫМИ УСЛОВИЯМИ И С ПОЛИТИКОЙ КОНФИДЕНЦИАЛЬНОСТИ.**

Лицезионное соглашение с конечным пользователем

Согласно условиям данного Лицензионного соглашения с конечным пользователем («Соглашение»), заключенного компанией ESET, spol. s r. o., зарегистрированной по адресу Einsteinova 24, 85101 Bratislava, Slovak Republic, внесенной в коммерческий регистр окружного суда

Bratislava I, раздел Sro, запись № 3586/B, BIN 31333532 (ESET или Поставщик) и вами, физическим или юридическим лицом (Вы или Конечный пользователь), Вы получаете право использовать Программное обеспечение, указанное в статье 1 настоящего Соглашения. Программное обеспечение, указанное в статье 1 настоящего Соглашения, может храниться на носителях данных, отправляться по электронной почте, загружаться через Интернет, загружаться с серверов Поставщика или получаться из других источников, которые удовлетворяют перечисленным ниже условиям.

ЭТО СОГЛАШЕНИЕ КАСАЕТСЯ ПРАВ КОНЕЧНОГО ПОЛЬЗОВАТЕЛЯ И НЕ ЯВЛЯЕТСЯ ДОГОВОРОМ ПРОДАЖИ. Поставщик остается владельцем экземпляра Программного обеспечения и материального носителя, на котором Программное обеспечение было поставлено в торговой упаковке, а также всех копий Программного обеспечения, на которые Конечный пользователь имеет право в соответствии с настоящим Соглашением.

Выбор варианта «Принимаю» в процессе установки, загрузки, копирования или использования этого Программного обеспечения выражает Ваше согласие с условиями настоящего Соглашения и Политики конфиденциальности. Если Вы не согласны с каким-либо из условий настоящего Соглашения или Политики конфиденциальности, немедленно выберите вариант отмены, отмените установку или загрузку, уничтожьте или верните Программное обеспечение, установочные носители, сопроводительную документацию, а также квитанцию об оплате Поставщику или в организацию, в которой было приобретено Программное обеспечение.

ИСПОЛЬЗОВАНИЕ ВАМИ ЭТОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ОЗНАЧАЕТ, ЧТО ВЫ ПРОЧЛИ ДАННОЕ СОГЛАШЕНИЕ, ПОНЯЛИ ЕГО ПОЛОЖЕНИЯ И СОГЛАСНЫ СЧИТАТЬ ИХ ОБЯЗЫВАЮЩИМИ.

1. **Программное обеспечение.** Термин "Программное обеспечение" в настоящем Соглашении означает: (i) компьютерную программу, которая сопровождается настоящим Соглашением, и все ее компоненты; (ii) все содержимое на дисках, компакт-дисках, DVD-дисках, в электронных сообщениях и каких-либо вложениях или на других носителях, которые были поставлены вместе с настоящим Соглашением, в том числе форму объектного кода Программного обеспечения, поставляемую на носителе данных, по электронной почте или загружаемую через Интернет; (iii) любые пояснительные материалы или любую другую возможную документацию, связанную с Программным обеспечением, главным образом какое-либо описание Программного обеспечения, его спецификации, какое-либо описание свойств или работы Программного обеспечения, какое-либо описание рабочей среды, в которой используется Программное обеспечение, инструкции по использованию или установке Программного обеспечения или какое-либо описание использования Программного обеспечения (Документация); (iv) копии Программного обеспечения, пакеты исправления возможных ошибок Программного обеспечения, дополнения к Программному обеспечению, расширения Программного обеспечения, измененные версии Программного обеспечения и обновления компонентов Программного обеспечения (при наличии), на которые Поставщик предоставил Вам лицензию в соответствии со статьей 3 настоящего Соглашения. Программное обеспечение предоставляется исключительно в форме исполняемого объектного кода.

2. **Установка, компьютер и лицензионный ключ**. Программное обеспечение, поставляемое на носителе данных, по электронной почте, загруженное через Интернет или с серверов Поставщика или полученное из других источников, подлежит установке. Установка Программного обеспечения должна происходить на должным образом настроенном компьютере, который отвечает минимальным требованиям, изложенным в Документации. Способ установки описан в Документации. Компьютер, на котором выполняется установка, не должен содержать программное или аппаратное обеспечение, которое может негативно повлиять на работу Программного обеспечения. Компьютер означает оборудование, в том

числе, среди прочего, персональные компьютеры, ноутбуки, рабочие станции, карманные компьютеры, смартфоны, карманные или другие электронные устройства, для которых разрабатывается Программное обеспечение, на котором его будут устанавливать и/или использовать. Лицензионный ключ означает уникальную последовательность символов, букв, цифр или специальных знаков, предоставляемых конечному пользователю, чтобы разрешить законно использовать Программное обеспечение или его определенную версию либо продлить срок действия Лицензии в соответствии с настоящим Соглашением.

3. **Лицензия**. Если Вы приняли все условия, предусмотренные в настоящем Соглашении, и соблюдаете их, Поставщик предоставляет Вам следующие права (Лицензия).

a) **Установка и использование.** Вы получаете неисключительное не подлежащее передаче право установить Программное обеспечение на жесткий диск компьютера или иной носитель для хранения данных, установки и хранения Программного обеспечения в памяти компьютера, а также внедрить, хранить и отображать Программное обеспечение.

b) **Оговорка по количеству лицензий.** Право на использование Программного обеспечения ограничено определенным количеством Конечных пользователей. Под одним Конечным пользователем подразумевается (i) установка Программного обеспечения на один компьютер или (ii) в случае ограничения лицензии количеством почтовых ящиков пользователь компьютера, который принимает электронную почту через пользовательский почтовый агент («Пользовательский почтовый агент»). Если Пользовательский почтовый агент принимает электронную почту, а затем автоматически распределяет ее среди нескольких пользователей, количество Конечных пользователей должно определяться в соответствии с фактическим количеством пользователей, получающих электронную почту. Если почтовый сервер выполняет функции почтового шлюза, количество Конечных пользователей будет равняться количеству пользователей почтового сервера, которых обслуживает этот шлюз. Если один пользователь владеет несколькими адресами электронной почты (например, при использовании псевдонимов) и принимает почту по ним, а почта не распределяется автоматически клиентом другим пользователям, необходима Лицензия только для одного компьютера. Одну Лицензию нельзя использовать одновременно на нескольких компьютерах. Конечный пользователь имеет право вводить Лицензионный ключ в Программное обеспечение только в той степени, в которой Конечный пользователь имеет право использовать Программное обеспечение в соответствии с ограничением по количеству Лицензий, выданных Поставщиком. Лицензионный ключ считается конфиденциальной информацией. Вы не должны передавать Лицензию третьим сторонам или разрешать третьим сторонам использовать Лицензионный ключ, если это не разрешено настоящим Соглашением или Поставщиком. Если Ваш Лицензионный ключ взломан, немедленно сообщите об этом Поставщику.

c) **Выпуск для дома или для бизнеса.** Версия Программного обеспечения для дома должна использоваться исключительно в личной и/или некоммерческой средах и предназначена только для домашнего и семейного использования. Для использования Программного обеспечения в коммерческих средах, а также на почтовых серверах, серверах ретрансляции электронной почты, почтовых шлюзах и шлюзах Интернета необходимо приобрести версию Программного обеспечения для бизнеса.

d) **Срок Лицензии.** Ваше право на использование Программного обеспечения ограничено определенным сроком.

e) **Программное обеспечение, получаемое через изготовителей комплектного оборудования.** Программное обеспечение, классифицированное как OEM (распространяется через изготовителей комплектного оборудования), можно использовать только на том

компьютере, на котором оно было получено. Такое программное обеспечение нельзя перенести на другой компьютер.

f) **Не предназначенные для продажи и пробные версии Программного обеспечения.** Программное обеспечение, классифицированное как не предназначенная для продажи или пробная версия, не может быть связано с каким-либо платежом и должно использоваться исключительно для демонстрации или тестирования функций Программного обеспечения.

g) **Прекращение действия Лицензии.** Действие Лицензии прекращается автоматически по окончании периода, на который она была выдана. Если Вы нарушаете любое положение настоящего Соглашения, Поставщик получает право выйти из него, что никак не повлияет на его возможности воспользоваться любыми правами и средствами судебной защиты, доступными ему в таких обстоятельствах. В случае отмены Лицензии Вы обязаны незамедлительно за собственный счет удалить, уничтожить или вернуть Программное обеспечение и все его резервные копии в компанию ESET или в точку продажи, в которой оно было приобретено. В случае прекращения действия Лицензии Поставщик также имеет право запретить Конечному пользователю использовать функции Программного обеспечения, которые требуют подключения к серверам Поставщика или серверам третьих лиц.

4. **Функции, для которых необходим сбор данных и подключение к Интернету.** Для корректной работы Программного обеспечения необходимо подключение к Интернету, поскольку Программное обеспечение должно регулярно подключаться к серверам Поставщика или третьих лиц, а также собирать соответствующие данные в соответствии с документом Политика конфиденциальности. Подключение к Интернету необходимо для использования перечисленных далее функций Программного обеспечения.

a) **Обновление Программного обеспечения.** Поставщик имеет право время от времени выпускать обновления Программного обеспечения (далее — «Обновления»), но не обязан их предоставлять. Эта функция включена при использовании стандартных параметров Программного обеспечения. Это значит, что Обновления устанавливаются автоматически, если Конечный пользователь не отключит их автоматическую установку. Для предоставления обновлений необходима проверка подлинности лицензии, включая информацию о компьютере и/или платформе, на которой установлено Программное обеспечение, в соответствии с Политикой конфиденциальности.

Предоставление любых Обновлений может регулироваться политикой в отношении окончания срока службы (далее — «Политика ОСС»), которая доступна по адресу https://go.eset.com/eol_business. После наступления даты окончания срока службы, которая устанавливается политикой ОСС для Программного обеспечения или какой-либо из его функций, Обновления предоставляться не будут.

b) **Отправка зараженных файлов и информации Поставщику.** Программное обеспечение оснащено функциями, которые собирают образцы компьютерных вирусов и других вредоносных программ, а также подозрительные, проблемные, потенциально нежелательные или потенциально опасные объекты, такие как файлы, URL-адреса, IP-пакеты и кадры Ethernet («Заражения»), и отправляют их Поставщику, в том числе, среди прочего, информацию о процессе установки, о Компьютере и/или платформе, на которых установлено Программное обеспечение, а также информацию об операциях и функциональности Программного обеспечения («Информация»). Информация и Заражения могут содержать данные (в том числе случайно или непредумышленно полученные персональные данные) о Конечном пользователе или других пользователях компьютера, на котором установлено Программное обеспечение, и о файлах, пораженных Заражениями с соответствующими метаданными.

Информацию и Заражения могут собирать следующие функции Программного обеспечения:

i. Функция LiveGrid Reputation System отвечает за сбор и отправку Поставщику в одном направлении хэшей, связанных с Заражениями. Эта функция включена при использовании стандартных параметров Программного обеспечения.

ii. Система обратной связи LiveGrid отвечает за сбор и отправку Поставщику Заражений со связанными метаданными и Информации. Конечный пользователь может активировать эту функцию в процессе установки Программного обеспечения.

Поставщик обязуется использовать полученные Заражения и Информацию только для анализа и исследования Заражений, улучшения Программного обеспечения и усовершенствования проверки подлинности Лицензии, а также принять необходимые меры предосторожности по сохранению конфиденциальности Информации и Заражений. Активируя эту функцию Программного обеспечения, Вы соглашаетесь на отправку Заражений и Информации Поставщику, а также даете ему необходимое разрешение, регулируемое соответствующими правовыми нормами, на обработку полученной Информации. Данную функцию можно отключить в любой момент.

Для целей настоящего Соглашения необходимо собирать, обрабатывать и хранить данные, позволяющие Поставщику идентифицировать Вас в соответствии с документом Политика конфиденциальности. Настоящим Вы подтверждаете, что Поставщик с помощью своих средств может проверять, используете ли Вы Программное обеспечение в соответствии с положениями настоящего Соглашения. Вы соглашаетесь на передачу информации в процессе обмена данными между Программным обеспечением и компьютерными системами Поставщика или его коммерческих партнеров, входящих в сеть распространения и поддержки Поставщика, с целью обеспечения работы и проверки возможности использования Программного обеспечения и защиты прав Поставщика.

После заключения этого Соглашения Поставщик или любой из его коммерческих партнеров, входящих в сеть распространения и поддержки Поставщика, получат право передавать, обрабатывать и хранить важные данные, позволяющие идентифицировать Вашу личность, в целях оплаты и исполнения настоящего Соглашения, а также для отправки уведомлений на Ваш компьютер.

Сведения о конфиденциальности, защите персональных данных и Ваших правах как субъекта персональных данных приведены в Политике конфиденциальности, которая доступна на веб-сайте Поставщика, а также непосредственно в процессе установки. Вы также можете открыть ее из справки Программного обеспечения.

5. **Использование прав Конечного пользователя**. Права Конечного пользователя необходимо использовать лично, либо их могут использовать Ваши сотрудники. Вы имеете право на использование Программного обеспечения только для защиты своих действий и компьютеров или компьютерных систем, на которые приобретена Лицензия.

6. **Ограничения прав.** Не разрешается копировать, распространять Программное обеспечение, извлекать его компоненты и создавать производные работы на его основе. При использовании Программного обеспечения Вы обязаны соблюдать перечисленные далее ограничения.

a) Вы можете создать одну резервную копию Программного обеспечения на носителе постоянного хранения данных при условии, что эта резервная копия не установлена и не используется ни на каком компьютере. Создание любых иных копий Программного

обеспечения является нарушением этого Соглашения.

b) Вы не должны использовать, изменять, переводить или воспроизводить Программное обеспечение и передавать права на использование Программного обеспечения или копии Программного обеспечения любым способом, отличным от описанного в настоящем Соглашении.

c) Вы не должны продавать, передавать на условиях сублицензии, сдавать в аренду или передавать во временное пользование Программное обеспечение, а также использовать Программное обеспечение для предоставления коммерческих услуг.

d) Запрещается вскрывать технологию, декомпилировать или разбирать код Программного обеспечения и иными способами пытаться получить исходный код Программного обеспечения за исключением того, в чем данное ограничение противоречит действующему законодательству.

e) Вы соглашаетесь использовать Программное обеспечение только способом, соответствующим всем действующим законодательным нормам страны, в которой используется Программное обеспечение, в том числе применимым ограничениям относительно авторского права, других прав на интеллектуальную собственность и так далее.

f) Вы соглашаетесь использовать Программное обеспечение и его функции только способом, который не ограничивает возможности доступа к этим услугам других Конечных пользователей. Поставщик оставляет за собой право ограничить объем услуг, предоставляемых отдельным Конечным пользователям, чтобы обеспечить использование услуг максимально возможным числом Конечных пользователей. Ограничение объема услуг должно также означать полное прекращение возможности использовать любую из функций Программного обеспечения, а также удаление Данных и информации на серверах Поставщика или сторонних серверах, относящихся к определенной функции Программного обеспечения.

g) Вы обязуетесь не предпринимать действий, связанных с использованием Лицензионного ключа, которые противоречат условиям настоящего Соглашения или приводят к предоставлению Лицензионного ключа лицу, не имеющему права использовать Программное обеспечение, например передачу использованного или неиспользованного Лицензионного ключа в любой форме, а также несанкционированное воспроизведение или распространение дублированных или сгенерированных лицензионных ключей или использование Программного обеспечения с помощью Лицензионного ключа, полученного не от Поставщика.

7. **Авторское право**. Программное обеспечение и все права на него, в том числе, среди прочего, право собственности и права на объекты интеллектуальной собственности, принадлежат компании ESET и/или ее лицензиарам. Эти права защищены международными соглашениями и всеми прочими применимыми законодательными нормами страны, в которой используется Программное обеспечение. Внутренняя структура, устройство и код Программного обеспечения являются ценной коммерческой тайной и конфиденциальной информацией, принадлежащими компании ESET и/или ее лицензиарам. Запрещается копировать Программное обеспечение кроме случаев, описанных в статье 6(a). Любые копии, которые разрешено создать в соответствии с Соглашением, должны содержать оригинальные отметки о защите авторских прав и другие уведомления о правах интеллектуальной собственности, которые присутствуют в самом Программном обеспечении. Если Вы вскрываете технологию, декомпилируете, разбираете исходный код Программного обеспечения или иным способом пытаетесь получить исходный код Программного обеспечения в нарушение положений этого Соглашения, любая полученная таким образом информация автоматически и

безоговорочно должна считаться подлежащей передаче Поставщику и принадлежащей ему полностью с момента создания вне зависимости от прав Поставщика в отношении нарушения этого Соглашения.

8. **Сохранение прав**. Настоящим Поставщик сохраняет за собой все права на Программное обеспечение, за исключением прав, явно предоставленных Вам как Конечному пользователю Программного обеспечения в соответствии с условиями настоящего Соглашения.

9. **Несколько языковых версий, программное обеспечение на носителях двух типов, несколько копий**. Если Программное обеспечение поддерживает несколько платформ или языков или если Вы получили несколько экземпляров программного обеспечения, разрешается использовать Программное обеспечение только на том количестве компьютеров и в тех версиях, на которые была приобретена Лицензия. Запрещается продавать, передавать на условиях сублицензии, сдавать в аренду, передавать во временное или постоянное пользование версии или копии Программного обеспечения, которые не используются Вами.

10. **Момент вступления в силу и прекращение действия Соглашения.** Настоящее Соглашение вступает в законную силу с дня, когда Вы согласились с его условиями. Завершить действие Соглашения можно в любой момент, необратимо удалив, разрушив или вернув за свой счет Программное обеспечение, все резервные копии и любые относящиеся к нему материалы, предоставленные Поставщиком или одним из его коммерческих партнеров. Ваше право на использование Программного обеспечения и любых его функций может регулироваться политикой в отношении окончания срока службы. После наступления даты окончания срока службы, которая устанавливается политикой в отношении окончания срока службы для Программного обеспечения или какой-либо из его функций, ваше право на использование Программного обеспечения прекратится. Независимо от способа прекращения действия этого Соглашения положения статей 7, 8, 11, 13, 19 и 21 остаются действительными без ограничения по времени.

11. **ГАРАНТИИ КОНЕЧНОГО ПОЛЬЗОВАТЕЛЯ**. ВЫСТУПАЯ В КАЧЕСТВЕ КОНЕЧНОГО ПОЛЬЗОВАТЕЛЯ, ВЫ ПОДТВЕРЖДАЕТЕ СВОЮ ОСВЕДОМЛЕННОСТЬ В ТОМ, ЧТО ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ПОСТАВЛЯЕТСЯ НА УСЛОВИЯХ «КАК ЕСТЬ» БЕЗ КАКИХ-ЛИБО ПРЯМЫХ ИЛИ ВМЕНЕННЫХ ГАРАНТИЙ ЛЮБОГО ТИПА, НАСКОЛЬКО ЭТО ПОЗВОЛЯЮТ СООТВЕТСТВУЮЩИЕ ЗАКОНОДАТЕЛЬНЫЕ НОРМЫ. НИ ПОСТАВЩИК, НИ ЕГО ПАРТНЕРЫ, ВЫСТУПАЮЩИЕ В КАЧЕСТВЕ ЛИЦЕНЗИАРОВ ИЛИ АФФИЛИРОВАННЫХ ЛИЦ, НИ ПРАВООБЛАДАТЕЛИ НЕ ДЕЛАЮТ НИКАКИХ ЗАЯВЛЕНИЙ И НЕ ПРЕДОСТАВЛЯЮТ НИКАКИХ ПРЯМЫХ ИЛИ ВМЕНЕННЫХ ОБЯЗАТЕЛЬСТВ ИЛИ ГАРАНТИЙ, В ЧАСТНОСТИ ГАРАНТИЙ ПРОДАЖ ИЛИ ГАРАНТИЙ ПРИГОДНОСТИ ДЛЯ ОПРЕДЕЛЕННОГО ИСПОЛЬЗОВАНИЯ, А ТАКЖЕ ГАРАНТИЙ ТОГО, ЧТО ЭТО ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ НЕ НАРУШАЕТ НИКАКИХ ПАТЕНТОВ, АВТОРСКИХ ПРАВ, ПРАВ НА ТОВАРНЫЕ ЗНАКИ И ДРУГИХ ПРАВ ТРЕТЬИХ ЛИЦ. ПОСТАВЩИК И ЛЮБЫЕ ДРУГИЕ ЛИЦА НЕ ГАРАНТИРУЮТ, ЧТО ФУНКЦИИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ БУДУТ СООТВЕТСТВОВАТЬ ВАШИМ ТРЕБОВАНИЯМ ИЛИ ЧТО ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ БУДЕТ РАБОТАТЬ БЕЗ СБОЕВ И ОШИБОК. РИСК ПРИ ВЫБОРЕ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДЛЯ ДОСТИЖЕНИЯ НУЖНЫХ РЕЗУЛЬТАТОВ, А ТАКЖЕ ПРИ УСТАНОВКЕ, ИСПОЛЬЗОВАНИИ И ПОЛУЧЕНИИ РЕЗУЛЬТАТОВ, КОТОРЫХ ВЫ БУДЕТЕ ДОСТИГАТЬ С ПОМОЩЬЮ ЭТОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, ЛЕЖИТ НА ВАС.

12. **Отказ от других обязательств**. Настоящее Соглашение не предусматривает никаких обязательств для Поставщика и его лицензиаров за исключением тех, которые изложены в настоящем Соглашении.

13. **ОГРАНИЧЕНИЕ ОТВЕТСТВЕННОСТИ**. В ТОЙ СТЕПЕНИ, В КОТОРОЙ ЭТО РАЗРЕШЕНО ПРИМЕНИМЫМ ЗАКОНОДАТЕЛЬСТВОМ, НИ ПРИ КАКИХ ОБСТОЯТЕЛЬСТВАХ ПОСТАВЩИК, ЕГО

СОТРУДНИКИ ИЛИ ЛИЦЕНЗИАРЫ НЕ НЕСУТ ОТВЕТСТВЕННОСТИ ЗА КАКУЮ-ЛИБО УПУЩЕННУЮ ПРИБЫЛЬ, ВЫРУЧКУ, ПРОДАЖИ, ДАННЫЕ ИЛИ РАСХОДЫ НА ЗАКУПКУ ВЗАИМОЗАМЕНЯЕМЫХ ТОВАРОВ ИЛИ УСЛУГ, ПОВРЕЖДЕНИЕ ИМУЩЕСТВА, ТЕЛЕСНЫЕ ПОВРЕЖДЕНИЯ, ПРИОСТАНОВКУ РАБОТЫ, ПОТЕРЮ КОММЕРЧЕСКОЙ ИНФОРМАЦИИ ИЛИ ЗА КАКИЕ-ЛИБО ФАКТИЧЕСКИЕ, ПРЯМЫЕ, НЕПРЯМЫЕ, ПОБОЧНЫЕ, ЭКОНОМИЧЕСКИЕ, КОМПЕНСИРУЕМЫЕ, ШТРАФНЫЕ, КОСВЕННЫЕ ИЛИ ПРЕДСКАЗУЕМЫЕ КОСВЕННЫЕ УБЫТКИ, НАНЕСЕННЫЕ В РЕЗУЛЬТАТЕ ВЫПОЛНЕНИЯ СОГЛАШЕНИЯ, ГРАЖДАНСКОГО ПРАВОНАРУШЕНИЯ ИЛИ НЕБРЕЖНОСТИ, НЕЗАВИСИМО ОТ ПРИЧИНЫ И ВИДА ОТВЕТСТВЕННОСТИ, ВОЗНИКАЮЩИЕ В РЕЗУЛЬТАТЕ УСТАНОВКИ, ИСПОЛЬЗОВАНИЯ ИЛИ ОТСУТСТВИЯ ВОЗМОЖНОСТИ ИСПОЛЬЗОВАНИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, ДАЖЕ ЕСЛИ ПОСТАВЩИК, ЕГО ЛИЦЕНЗИАРЫ ИЛИ АФФИЛИРОВАННЫЕ ЛИЦА ОСВЕДОМЛЕНЫ О ВОЗМОЖНОСТИ ВОЗНИКНОВЕНИЯ ТАКОГО УЩЕРБА. ПОСКОЛЬКУ ЗАКОНОДАТЕЛЬСТВО НЕКОТОРЫХ СТРАН И ОТДЕЛЬНЫЕ ЗАКОНЫ НЕ РАЗРЕШАЮТ ИСКЛЮЧАТЬ ТАКУЮ ОТВЕТСТВЕННОСТЬ, НО ПОЗВОЛЯЮТ ОГРАНИЧИВАТЬ ЕЕ, В ТАКИХ СЛУЧАЯХ ОТВЕТСТВЕННОСТЬ ПОСТАВЩИКА, ЕГО СОТРУДНИКОВ, ЛИЦЕНЗИАРОВ ИЛИ АФФИЛИРОВАННЫХ ЛИЦ ОГРАНИЧИВАЕТСЯ СУММОЙ, ВЫПЛАЧЕННОЙ ВАМИ ЗА ЛИЦЕНЗИЮ.

14. Ни одно из положений настоящего Соглашения не затрагивает законные права любой стороны, выступающей в качестве потребителя, даже если они противоречат таким правам.

15. **Техническая поддержка**. ESET или привлеченные компанией ESET третьи лица предоставляют техническую поддержку по собственному усмотрению без каких-либо гарантий или заявлений. После наступления даты окончания срока службы, которая устанавливается политикой ОСС для Программного обеспечения или какой-либо из его функций, техническая поддержка предоставляться не будет. Конечный пользователь обязан создать резервную копию всех существующих данных, программного обеспечения или программных средств, прежде чем обратиться за технической поддержкой. ESET и (или) третьи лица, привлеченные ESET, не могут принять на себя ответственность за повреждение или потерю данных, собственности, программного обеспечения или оборудования, а также за упущенную прибыль, которые связаны с предоставлением технической поддержки. ESET и (или) привлеченные ESET третьи лица оставляют за собой право принять решение о том, что устранить конкретную проблему невозможно в рамках технической поддержки. ESET оставляет за собой право отказать в предоставлении технической поддержки, приостановить или прекратить ее оказание по своему собственному усмотрению. Сведения о лицензии, Информация и другие данные в соответствии с Политикой конфиденциальности могут потребоваться для предоставления технической поддержки.

16. **Передача лицензии**. Программное обеспечение может быть перенесено с одного компьютера на другой, если это не противоречит условиям настоящего Соглашения. Если это не противоречит условиям Соглашения, Конечный пользователь может только перманентно передать Лицензию и все права по настоящему Соглашению другому Конечному пользователю с согласия Поставщика, если соблюдаются следующие условия: (i) у первого Конечного пользователя не остается никаких экземпляров Программного обеспечения; (ii) передача прав должна быть непосредственной, т. е. от исходного Конечного пользователя к новому; (iii) новый Конечный пользователь должен принять все права и обязательства исходного Конечного пользователя по настоящему Соглашению; (iv) исходный Конечный пользователь должен предоставить новому Конечному пользователю документацию, позволяющую проверить подлинность Программного обеспечения в соответствии со статьей 17.

17. **Проверка подлинности Программного обеспечения.** Конечный пользователь может продемонстрировать наличие у него прав на использование Программного обеспечения одним из следующих способов: (i) с помощью лицензионного сертификата, выданного Поставщиком

или третьим лицом, которое назначено Поставщиком; (ii) письменным лицензионным соглашением, если таковое было заключено; (iii) путем предоставления отправленного Поставщиком сообщения электронной почты, в котором содержатся сведения о лицензии (имя пользователя и пароль). Сведения о лицензии и идентификационные данные Конечного пользователя в соответствии с Политикой конфиденциальности могут потребоваться для проверки подлинности программного обеспечения.

18. **Предоставление лицензии органам власти и правительству США**. Программное обеспечение будет предоставлено органам власти, в том числе правительству Соединенных Штатов Америки, в соответствии с правами и ограничениями, описанными в настоящем Соглашении.

19. **Соответствие нормам регулирования внешней торговли**.

a) Вы не будете прямо или косвенно экспортировать, реэкспортировать, передавать или иным образом предоставлять Программное обеспечение кому-либо, а также не будете использовать его каким-либо образом либо иметь отношение к каким-либо действиям, в результате чего компания ESET или ее холдинговые компании, ее филиалы, филиалы ее холдинговых компаний, прочие субъекты, находящиеся под управлением ее холдинговых компаний («Аффилированные лица»), может стать нарушителем Законодательства по регулированию внешней торговли либо получить негативные последствия в связи с его применением. К законодательству по регулированию внешней торговли относится:

i. Любое законодательство, которое предназначено для регулирования, ограничения или введения лицензионных требований в сфере экспорта, реэкспорта или передачи товаров, программного обеспечения, технологий, услуг и которое принимается любыми правительственными, государственными или регулятивными органами Соединенных Штатов Америки, Сингапура, Великобритании, Европейского Союза или любого входящего в него государства, а также любой страны, в которой должны выполняться обязательства согласно настоящему Соглашению или в которой зарегистрирована либо действует компания ESET или какие-либо ее Аффилированные лица

ii. Любые экономические, финансовые, торговые и прочие санкции, ограничения, эмбарго, запреты на импорт или экспорт, запреты на перевод денежных средств или активов либо на предоставление услуг, а также эквивалентные меры, которые вводятся в действие любыми правительственными, государственными или регулятивными органами Соединенных Штатов Америки, Сингапура, Великобритании, Европейского Союза или любого входящего в него государства, а также любой страны, в которой должны выполняться обязательства согласно настоящему Соглашению или в которой зарегистрирована либо действует компания ESET или какие-либо ее Аффилированные лица.

(Законодательные акты, упомянутые в пунктах i и ii выше, совместно именуются «Законодательство по регулированию внешней торговли».)

b) Компания ESET имеет право приостановить выполнение своих обязательств согласно настоящим Условиям либо незамедлительно прекратить действие настоящих Условий в следующих случаях:

i. В случае, если компания ESET устанавливает, что по ее обоснованному мнению Пользователь нарушил или может нарушить положения Статьи 19 a) настоящего Соглашения.

ii. В случае, если Конечный пользователь и/или Программное обеспечение попадут под

действие Законодательства по регулированию внешней торговли, и, как результат, компания ESET установит, что по ее обоснованному мнению продолжение выполнения своих обязательств согласно настоящему Соглашению может привести к тому, что компания ESET или ее Аффилированные лица может стать нарушителем Законодательства по регулированию внешней торговли либо получить негативные последствия в связи с его применением.

c) Ни одна часть настоящего Соглашения не предназначена, не может интерпретироваться или истолковываться так, чтобы побуждать либо обязывать любую его сторону действовать или воздерживаться от действий (или согласиться действовать или воздерживаться от действий) каким-либо образом, который противоречит любому применимому Законодательству по регулированию внешней торговли, преследуется или запрещается им.

20. **Уведомления**. Все уведомления, возвращаемые Программное обеспечение и документация должны быть доставлены по адресу: ESET, spol. s r. o., Einsteinova 24, 85101 Bratislava, Slovak Republic, что не ограничивает право ESET сообщать Вам о любых изменениях в настоящем Соглашении, политиках конфиденциальности, политике в отношении окончания срока службы и документации в соответствии со статьей 22 настоящего Соглашения. ESET может отправлять Вам письма по электронной почте и уведомления в Программном обеспечении, а также публиковать сообщения на нашем веб-сайте. Вы соглашаетесь получать юридически значимые сообщения от компании ESET в электронной форме, в том числе любые сообщения об изменении Условий, Специальных условий или Политик конфиденциальности, любые предложения и принятие условий договоров, приглашения вести переговоры о заключении договора, уведомления или другие юридически значимые сообщения. Такие электронные сообщения считаются полученными в письменной форме, если только действующее законодательство не требует другого формата коммуникации.

21. **Применимое законодательство**. Данное Соглашение регулируется и толкуется в соответствии с законодательством Словацкой Республики. Конечный пользователь и Поставщик согласны, что принципы коллизионного права и Конвенция Организации Объединенных Наций о договорах международной купли-продажи товаров не применяются. Вы явным образом соглашаетесь с тем, что эксклюзивная юрисдикция по решению любых споров и вопросов с Поставщиком или относительно способа использования Программного обеспечения принадлежит окружному суду I в Братиславе.

22. **Общие положения**. Если любое положение настоящего Соглашения оказывается недействительным или невыполнимым, это не отражается на действительности остальных положений Соглашения, которые по-прежнему будут действительными и выполнимыми в соответствии с указанными здесь условиями. Настоящее Соглашение составлено на английском языке. В случае подготовки перевода настоящего Соглашения для удобства или любой иной цели либо при наличии любых расхождений между разными языковыми версиями настоящего Соглашения преимуществом обладает версия на английском языке.

Компания ESET оставляет за собой право вносить изменения в Программное обеспечение и пересматривать условия настоящего Соглашения, приложений и дополнений к нему, Политики конфиденциальности, Политики ОСС и документации или какой-либо их части в любое время путем обновления соответствующего документа (a) для отображения изменений в Программном обеспечении либо в способе осуществления деятельности компанией ESET, (б) для соблюдения нормативно-правовых норм или из соображений безопасности либо (в) для недопущения нарушений или нанесения вреда. В случае изменения настоящего Соглашения Вы будете уведомлены с помощью электронной почты, уведомления в приложении или другими электронными средствами. Если Вы не согласны с предлагаемыми изменениями к настоящему Соглашению, Вы можете расторгнуть его в соответствии со статьей 10 в течение

30 дней после получения уведомления об изменении. Если Вы не расторгнете настоящее Соглашение в течение этого срока, предлагаемые изменения будут считаться принятыми и вступят в силу в отношении Вас с даты получения Вами уведомления об изменении.

Это полное Соглашение между Поставщиком и Вами относительно использования Программного обеспечения, которое заменяет все предыдущие заверения, обсуждения, гарантии или уведомления или рекламные материалы в отношении Программного обеспечения.

EULAID: EULA-PRODUCT-LG; 3537.0

Политика конфиденциальности

Компания ESET, spol. s r. o., зарегистрированная по адресу Einsteinova 24, 851 01 Bratislava, Словацкая Республика, внесенная в реестр юридических лиц окружного суда I в Братиславе, раздел Sro, запись № 3586/B, регистрационный номер предприятия 31333532, в качестве оператора данных (далее — «ESET» или «Мы») стремится обеспечить прозрачность своих действий, связанных с обработкой личных данных и обеспечением конфиденциальности клиентов. Поэтому Мы публикуем Политику конфиденциальности, исключительно чтобы уведомить клиента (далее — «Конечный пользователь» или «Вы») о нижеследующем:

- Обработка персональных данных,
- Конфиденциальность данных,
- права субъекта данных.

Обработка персональных данных

Услуги, предоставляемые ESET и реализованные в нашем продукте, предоставляются в соответствии с Лицензионным соглашением с конечным пользователем (далее — «Лицензионное соглашение»), но некоторые из них могут потребовать особого внимания. Мы хотим рассказать Вам подробнее о сборе данных, связанных с предоставлением наших служб. Мы предоставляем различные услуги, описанные в Лицензионном соглашении и документации, например услугу обновления, систему ESET LiveGrid®, защиту от ненадлежащего использования данных, поддержку и т. д. Чтобы все это работало, нам необходимо собирать следующую информацию.

- обновления и другую статистику, содержащую данные о процессе установки и Вашем компьютере, в том числе тип платформы, операции и функции Наших программ, например версию ОС, характеристики оборудования, идентификаторы инсталляций и лицензий, IP- и MAC-адреса, конфигурации программ;
- Однонаправленные хеш-функции, связанные с заражениями и входящие в систему репутации ESET LiveGrid®, которая повышает эффективность решений для защиты от вредоносных программ и благодаря которой сканируемые файлы сопоставляются с элементами белого и черного списков в облаке.
- Подозрительные образцы метаданных из внешних источников в рамках системы обратной связи ESET LiveGrid®, благодаря которой ESET может мгновенно реагировать на нужды пользователей и своевременно адаптироваться под новейшие угрозы. Мы рассчитываем на то, что вы будете присылать нам:

- зараженные элементы, такие как потенциальные образцы вирусов и прочих вредоносных программ; подозрительные, проблемные, потенциально нежелательные и небезопасные объекты, такие как исполняемые файлы, сообщения электронной почты, про которые сообщили вы как про спам или которые выявил наш продукт;
- информацию об устройствах в локальной сети, например тип, производитель, модель и/или название;
- сведения о пользовании Интернетом, например IP-адрес, географическое расположение, пакеты IP, URL-адреса и кадры Ethernet;
- файлы аварийных дампов и их содержимое.

Мы не стремимся собирать какие-либо данные, кроме обозначенных выше, но иногда этого невозможно избежать. Случайно собранные данные могут входить в состав вредоносных программ (будучи собранными без вашего ведома и одобрения) либо входить в имена файлов и URL-адреса, и Мы не намерены делать их частью наших систем или обрабатывать их для целей, указанных в настоящей Политике конфиденциальности.

• Сведения о лицензиях, например идентификаторы лицензий, и личные данные, например имя, фамилия, адрес, электронная почта, необходимые для выставления счетов, проверки подлинности лицензий и предоставления наших услуг.

• Для обслуживания и предоставления поддержки может потребоваться контактная информация и данные, указанные в Ваших запросах на поддержку. Исходя из выбранного способа общения, Мы можем фиксировать Ваш электронный адрес, номер телефона, информацию о лицензии, сведения о программах и описание Вашего инцидента. Возможно, служба поддержки попросит Вас предоставить дополнительную информацию, чтобы упростить решение проблемы.

Конфиденциальность данных

ESET — это международная компания. Наша сеть распространения, обслуживания и поддержки состоит из аффилированных лиц и партнеров. Мы можем обмениваться информацией, которую обрабатывает ESET, с аффилированными лицами для выполнения соглашений EULA, например для предоставления поддержки или выставления счетов. В зависимости от Вашего расположения и выбранной услуги Нам, возможно, потребуется передать Ваши данные в страну, в которой не действуют нормативы Европейской Комиссии. Даже в этом случае сведения передаются лишь при необходимости и в соответствии с законодательством в сфере защиты данных. Во всех случаях без исключения должны применяться стандартные контрактные условия, обязательные корпоративные правила или другие соответствующие средства защиты.

Мы стремимся хранить данные не дольше, чем это необходимо для предоставления услуг в соответствии с Лицензионным соглашением. Длительность нашего периода хранения может превышать срок действия вашей лицензии — это дает Вам возможность простого и удобного продления. Сведенная к минимуму и анонимизированная статистика, а также прочие данные системы ESET LiveGrid® могут в дальнейшем обрабатываться в статистических целях.

ESET проводит соответствующие технические и организационные мероприятия, чтобы гарантировать уровень безопасности согласно возможным рискам. Мы делаем все возможное для непрерывного обеспечения конфиденциальности, целостности, доступности и устойчивости систем и служб обработки. Однако, если произойдет утечка данных, которая

будет угрожать Вашим правам и свободам, Мы готовы уведомить органы по надзору, а также субъекты данных. Как субъект данных Вы имеете право подать жалобу в наблюдательный орган.

Права субъекта данных

ESET действует согласно словацким законам и законам о защите данных ЕС. Согласно условиям, которые определены действующим законодательством по защите данных, Вы как субъект данных имеете следующие права:

- запросить доступ к своим персональным данным, которыми располагает ESET;
- запросить исправление неточных данных (у Вас также есть право на дополнение неполных данных);
- запросить уничтожение своих персональных данных;
- запросить ограничение обработки своих персональных данных;
- право на запрет обработки данных;
- право на подачу жалобы, а также
- запросить переносимость данных.

Если Вы хотите воспользоваться своими правами субъекта данных или у Вас возникнет вопрос или проблема, отправьте нам письмо по адресу:

ESET, spol. s r.o.
Data Protection Officer
Einsteinova 24
85101 Bratislava
Slovak Republic
dpo@eset.sk