

kaspersky

Kaspersky Endpoint Security for Aurora

Руководство Администратора

Уважаемый пользователь!

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

Внимание! Права на этот документ являются собственностью АО "Лаборатория Касперского" (далее также "Лаборатория Касперского") и защищены законодательством Российской Федерации об авторском праве и международными договорами. За незаконное копирование и распространение документа и его отдельных частей нарушитель несет гражданскую, административную или уголовную ответственность в соответствии с применимым законодательством.

Копирование в любой форме, распространение, в том числе в переводе, любых материалов возможны только с письменного разрешения "Лаборатории Касперского".

Документ и связанные с ним графические изображения могут быть использованы только в информационных, некоммерческих или личных целях.

Документ может быть изменен без предварительного уведомления.

За содержание, качество, актуальность и достоверность используемых в документе материалов, права на которые принадлежат другим правообладателям, а также за возможный ущерб, связанный с использованием этих материалов, "Лаборатория Касперского" ответственности не несет.

В этом документе используются зарегистрированные товарные знаки и знаки обслуживания, которые являются собственностью соответствующих правообладателей.

Дата редакции документа: 8/24/2020

Обозначение документа:

643.46856491.00109-02 99 01

© 2020 АО "Лаборатория Касперского"

<https://www.kaspersky.ru>

<https://help.kaspersky.com/u>

<https://support.kaspersky.ru>

О "Лаборатории Касперского": <https://www.kaspersky.ru/about/company>

Оглавление

| | |
|--|----|
| Об этом документе | 4 |
| О программе..... | 5 |
| Требования | 6 |
| Аппаратные и программные требования..... | 6 |
| Указания по эксплуатации и требования к среде | 6 |
| Подготовка к установке программы | 7 |
| Установка программы | 8 |
| Подготовка программы к работе | 9 |
| Процедура приемки..... | 10 |
| Безопасное состояние | 10 |
| Проверка работоспособности. EICAR..... | 12 |
| Разделение доступа к функциям программы по пользовательским ролям | 15 |
| Антивирусная проверка | 16 |
| Обновление антивирусных баз | 18 |
| Мониторинг работы программы | 20 |
| Обновление антивирусных баз в ручном режиме | 20 |
| Устранение уязвимостей и установка критических обновлений в программе..... | 21 |
| Действия после сбоя или неустранимой ошибки в работе программы..... | 22 |
| Удаление программы | 23 |
| Техническая поддержка | 23 |
| Информация о стороннем коде..... | 24 |
| Уведомления товарных знаках..... | 25 |
| Соответствие терминов | 26 |
| Приложение. Значения параметров программы в сертифицированной конфигурации | 26 |

Об этом документе

Настоящий документ представляет собой подготовительные процедуры и руководство по эксплуатации программного изделия "Kaspersky Endpoint Security for Aurora" (далее также "Kaspersky Endpoint Security", "программа").

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

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

В документе также содержатся разделы с дополнительной информацией о программе.

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

О программе

Программное изделие "Kaspersky Endpoint Security for Aurora" представляет собой средство антивирусной защиты типа "В" четвертого класса защиты и предназначено для применения на мобильных автоматизированных рабочих местах информационных систем.

В программе реализованы следующие функции безопасности:

- разграничение доступа к управлению программой;
- управление работой программы;
- управление параметрами программы;
- управление установкой обновлений (актуализации) базы данных признаков вредоносных компьютерных программ (вирусов) (БД ПКВ);
- аудит безопасности программы;
- выполнение проверок объектов воздействия;
- обработка объектов воздействия.

Требования

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

В этом разделе

| | |
|---|-------------------|
| Аппаратные и программные требования | 6 |
| Указания по эксплуатации и требования к среде | 6 |

Аппаратные и программные требования

Kaspersky Endpoint Security for Aurora имеет следующие минимальные аппаратные и программные требования:

- смартфон или планшет с разрешением экрана от 540x960 пикселей;
- оперативная память 1 ГБ ОЗУ;
- 20 МБ свободного места в основной памяти устройства;
- операционная система Aurora OS 3.2.2.21;
- процессор ARM Contex-A7, 1.26 ГГц, 4 ядра.

Указания по эксплуатации и требования к среде

Для работы Kaspersky Endpoint Security for Aurora должны быть выполнены следующие условия:

1. Установка, конфигурирование и управление программой должны осуществляться в соответствии с эксплуатационной документацией.
2. Программа должна эксплуатироваться на мобильных устройствах, отвечающих минимальным требованиям (см. раздел "Аппаратные и программные требования" на стр. [6](#)).
3. Программа должна эксплуатироваться на мобильных устройствах, на которых у пользователей отсутствуют root-права.
4. Перед установкой и началом эксплуатации программы необходимо установить все доступные обновления для используемых версий ПО среды функционирования.

5. Должна быть обеспечена совместимость программы с контролируруемыми ресурсами информационной системы.
6. Персонал, ответственный за функционирование программы, должен обеспечивать надлежащее функционирование программы, руководствуясь эксплуатационной документацией.
7. Должен быть обеспечен доверенный канал получения обновлений БД ПКВ.
8. Должна быть обеспечена защищенная область для выполнения функций безопасности программы.
9. Управление атрибутами безопасности, связанными с доступом к функциям и данным программы, должно предоставляться только уполномоченным ролям (администраторам программы и информационной системы).

Подготовка к установке программы

Перед установкой программы убедитесь, что программные и аппаратные ресурсы мобильного устройства, на который будет произведена установка, удовлетворяют требованиям, приведенным в разделе "Аппаратные и программные требования".

Также нужно убедиться, что для операционной системы и программных средств, необходимых для установки (если таковые имеются), установлены самые последние пакеты обновлений, выпускаемые производителями операционной системы и программного обеспечения.

Для удаленной установки Kaspersky Endpoint Security через Аврора Центр необходимо опубликовать программу в консоли разработчика Аврора Центр и добавить мобильное устройство в консоль управления Аврора Центр. Подробнее см. в документации компании "Открытая мобильная платформа"

<https://omprussia.ru/>.

Установка программы

Установка Kaspersky Endpoint Security доступна только администратору. Установить программу через приложение Аврора Маркет невозможно.

Вы можете установить Kaspersky Endpoint Security следующими способами:

- удаленно с помощью Аврора Центр;
- локально через приложение Терминал.

Установка с помощью Аврора Центр

Установка программы через Аврора Центр выполняет администратор. Установка выполняется обычным способом, принятым для платформы Аврора. Подробнее об установке программ с помощью Аврора Центр см. в документации компании "Открытая мобильная платформа" <https://omprussia.ru/>. Установка будет выполнена в тихом режиме.


Установка через приложение Терминал

Установку Kaspersky Endpoint Security выполняют инструменты операционной системы. Скопируйте RPM-пакет в память мобильного устройства любым доступным способом. Например, вы можете подключить мобильное устройство к компьютеру с помощью USB. RPM-пакет входит в комплект поставки программы.

Для установки Kaspersky Endpoint Security через приложение Терминал учетная запись должна обладать правами суперпользователя (`devel-su`).

► Чтобы установить Kaspersky Endpoint Security, выполните следующую команду:

```
rpm -i <имя RPM-пакета>
```

В результате инструменты операционной системы установят Kaspersky Endpoint Security в тихом режиме. После завершения установки операционная система покажет уведомление с результатами установки. В сетке программ будет добавлен значок .

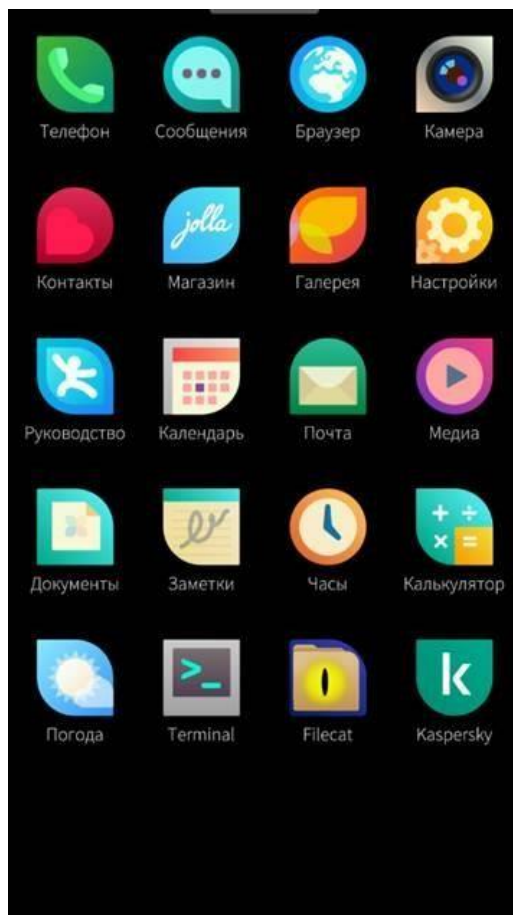



Рисунок 1. Сетка программ

Подготовка программы к работе

Запустите Kaspersky Endpoint Security после установки программы на мобильное устройство. Для этого коснитесь значка  в сетке программ или на домашнем экране. В результате запустится мастер первоначальной настройки программы. Следуйте его указаниям.

Шаг 1. Просмотр Лицензионного соглашения

На этом шаге мастера первоначальной настройки нужно ознакомиться с Лицензионным соглашением, которое заключается между вами и "Лабораторией Касперского".

Внимательно прочитайте Лицензионное соглашение. Если вы согласны со всеми пунктами Лицензионного соглашения, нажмите **Принять**.

Если вы не согласны с Лицензионным соглашением, нажмите **Отказаться** и удалите программу.

Шаг 2. Создание пароля администратора

На этом шаге мастера первоначальной настройки нужно задать пароль администратора. *Администратор* имеет следующие права:

- настройка параметров программы;

- просмотр всех отчетов о работе программы (пользователь может просматривать только отчеты о проверке и обновлении баз).

Пароль должен удовлетворять требованиям надежности, например, пароль должен содержать не менее восьми символов. В пароле запрещается использовать символы "точка", "запятая", "пробел".

Вы можете установить пароль администратора только в мастере первоначальной настройки. Изменить или восстановить пароль невозможно. Если вы забыли пароль, сбросьте устройство к заводским настройкам.

Задайте и подтвердите пароль администратора. Нажмите **Установить**.

Шаг 3. Завершение работы мастера

На этом шаге мастер первоначальной настройки завершает свою работу. Kaspersky Endpoint Security автоматически запускает обновление антивирусных баз программы. После обновления баз Kaspersky Endpoint Security автоматически запускает антивирусную проверку устройства. Если Kaspersky Endpoint Security обнаружит угрозы, программа автоматически их удалит и добавит запись в отчеты.

После завершения работы мастера первоначальной настройки Kaspersky Endpoint Security работает в фоновом режиме. В фоновом режиме Kaspersky Endpoint Security запускает обновление антивирусных баз и антивирусную проверку по расписанию. После перезапуска мобильного устройства Kaspersky Endpoint Security начинает работу в фоновом режиме автоматически.

Процедура приемки

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

В этом разделе

| | |
|---|--------------------|
| Безопасное состояние | 11 |
| Проверка работоспособности. EICAR | |

[12](#)

Безопасное состояние

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

- На главном окне Kaspersky Endpoint Security отображается сообщение **Угроз не обнаружено** (см. рис. ниже).
- Антивирусные базы программы обновлены (см. раздел "Обновление антивирусных баз" на стр. [20](#)).

На главном окне Kaspersky Endpoint Security отсутствует сообщение **Базы давно не обновлялись**.

- Настроено расписание антивирусной проверки всей файловой системы мобильного устройства (см. раздел "Антивирусная проверка" на стр. [18](#)).
- Настроено расписание обновления антивирусных баз (см. раздел "Обновление антивирусных баз" на стр. [20](#)).
- Параметры программы находятся в рамках допустимых значений, приведенных в приложении к этому документу (см. раздел "Приложение. Значения параметров программы в сертифицированной конфигурации" на стр. [31](#)).

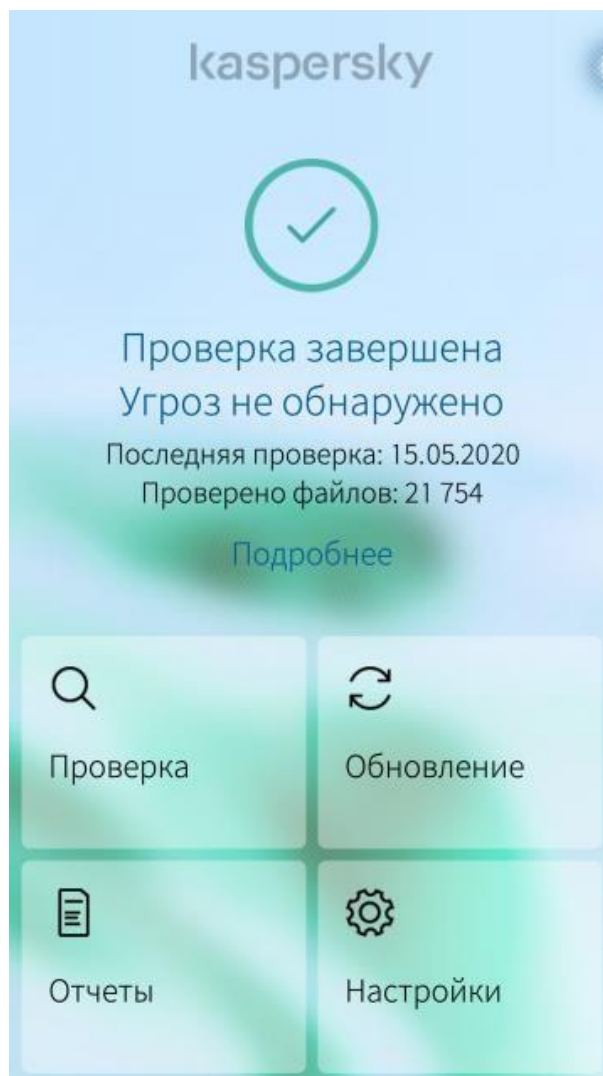


Рисунок 2. Главное окно программы

Проверка работоспособности. EICAR

Чтобы проверить работоспособность программы, вы можете использовать тестовый файл EICAR. Тестовый файл EICAR предназначен для проверки работы антивирусных программ. Он разработан организацией The European Institute for Computer Antivirus Research (EICAR).

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

Вы можете загрузить тестовый файл EICAR со страницы веб-сайта организации EICAR http://www.eicar.org/anti_virus_test_file.htm.

► *Чтобы проверить работоспособность программы, выполните следующие действия:*

1. Откройте в браузере сайт EICAR http://www.eicar.org/anti_virus_test_file.htm.
2. Выберите на сайте раздел **Download**.
3. Найдите файл тестового "вируса" eicar.com.txt и загрузите файл на устройство.
Тестовый файл EICAR будет загружен в память мобильного устройства.
4. Откройте программу Kaspersky Endpoint Security.
5. В главном окне программы нажмите **Проверка**.

Kaspersky Endpoint Security обнаружит вредоносный файл и удалит его. Вы можете просмотреть результаты работы Kaspersky Endpoint Security в отчетах. Для этого нужно нажать **Подробнее**.

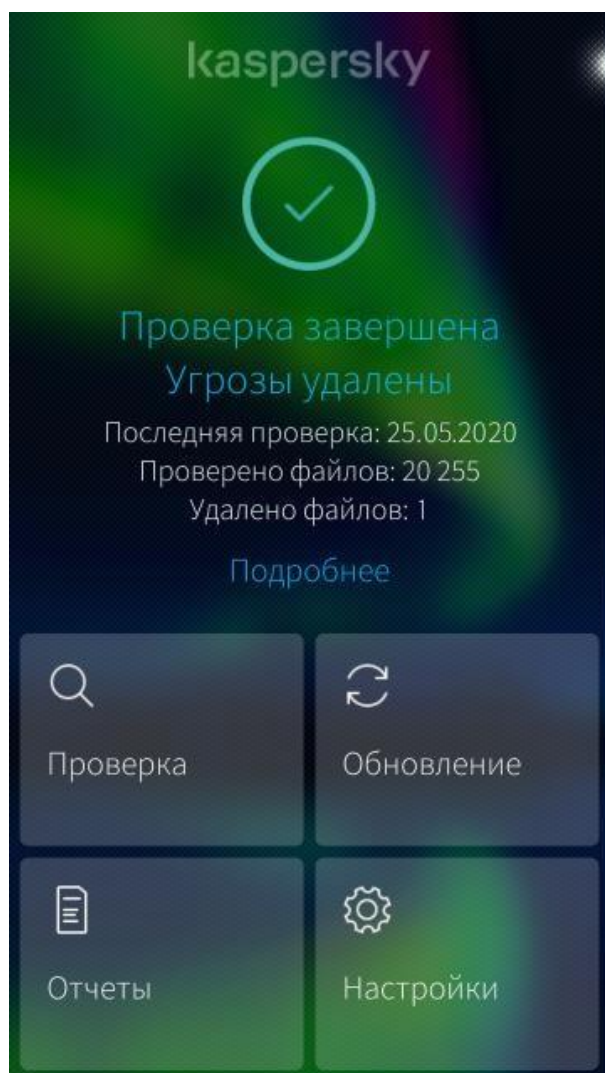


Рисунок 3. Обнаружение угрозы

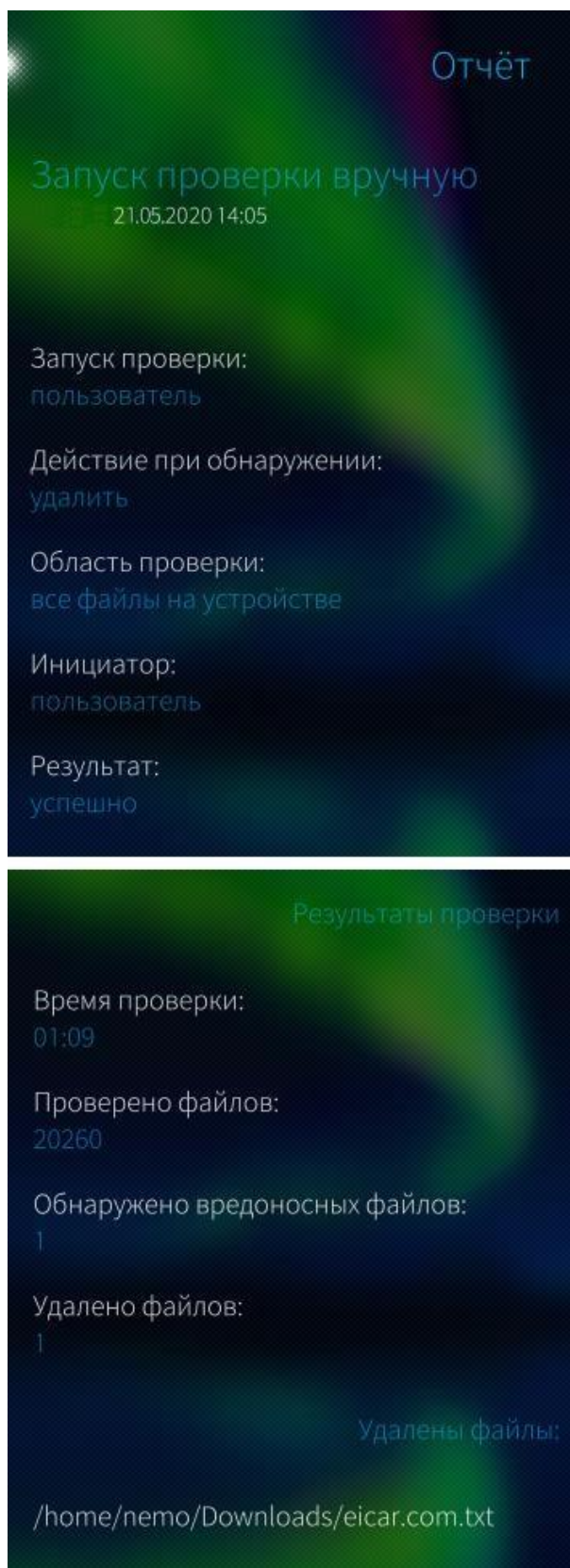


Рисунок 4. Отчет об обнаружении угрозы

Разделение доступа к функциям программы по пользовательским ролям

В Kaspersky Endpoint Security предусмотрены следующие роли:

- Администратор.
- Пользователь.

Kaspersky Endpoint Security разделяет доступ к функциям программы с помощью пароля. По умолчанию с программой работает пользователь. При попытке пользователя получить доступ к функциям, которые доступны только администратору, Kaspersky Endpoint Security запрашивает пароль. После успешной авторизации Kaspersky Endpoint Security продолжает работу с администратором. При этом администратор получает полный доступ ко всем функциям программы до закрытия программы. Если вы откроете программу заново, для авторизации администратора нужно ввести пароль повторно.

Администратор Kaspersky Endpoint Security

Роль администратора предназначена для настройки программы в соответствии с требованиями корпоративной безопасности и мониторинга работы программы. Вы можете добавить администратора только при первоначальной настройке программы (см. раздел "Подготовка программы к работе" на стр. [10](#)). Добавить несколько администраторов программы невозможно. Администратор имеет полный доступ ко всем функциям программы. Для получения доступа к функциям, запрещенным для пользователя, нужно ввести пароль.

Пользователь Kaspersky Endpoint Security

Роль пользователя предназначена для управления Kaspersky Endpoint Security. Пользователь может запускать антивирусную проверку и обновлять антивирусные базы.

Таблица 1. Разделение доступа к функциям программы по пользовательским ролям

| Функция | Пользователь | Администратор |
|--|--------------|---------------|
| Установка программы | Недоступно | ✓ |
| Обновление программы | Недоступно | ✓ |
| Антивирусная проверка | ✓ | ✓ |
| Обновление антивирусных баз | ✓ | ✓ |
| Просмотр отчетов о проверке и обновлении баз, запущенных вручную | ✓ | ✓ |
| Просмотр всех отчетов | Недоступно | ✓ |

| | | |
|--|------------|---|
| <p>Настройка программы:</p> <ul style="list-style-type: none"> • Расписание антивирусной проверки. • Расписание обновления антивирусных баз. • Источник обновления антивирусных баз | Недоступно | ✓ |
| Удаление программы | Недоступно | ✓ |

Антивирусная проверка


Для обнаружения угроз, поиска вирусов, а также других вредоносных программ следует запускать антивирусную проверку. Kaspersky Endpoint Security проверяет все устройство, включая установленные программы и внешнюю память устройства (например, SD-карту). Kaspersky Endpoint Security проверяет файлы всех форматов, в том числе содержимое архивов.

Вы можете запускать антивирусную проверку вручную или автоматически (по расписанию). Запустить проверку вручную может любой пользователь. Настроить автоматический запуск антивирусной проверки может только администратор.

Kaspersky Endpoint Security имеет следующие ограничения:


- Kaspersky Endpoint Security не может проверять файлы размером 4 ГБ и более. Во время проверки программа пропускает такие файлы и не уведомляет вас, если такие файлы были пропущены.
- У Kaspersky Endpoint Security отсутствуют права на удаление файлов в системном разделе диска. При обнаружении угроз в системном разделе диска Kaspersky Endpoint Security добавит информацию об обнаружении угрозы в отчеты программы и системный журнал устройства.

► *Чтобы запустить антивирусную проверку вручную, выполните следующие действия:*

1. Коснитесь значка  в сетке программ или на домашнем экране.
2. Нажмите **Проверка**.

Kaspersky Endpoint Security проверит все устройство. При обнаружении угроз программа удалит вредоносные файлы автоматически. Для просмотра подробного отчета о проверке нажмите **Подробнее**.

► *Чтобы настроить запуск антивирусной проверки по расписанию, выполните следующие действия:*

1. Коснитесь значка  в сетке программ или на домашнем экране.
2. Нажмите **Настройки**.
3. Введите пароль администратора и перейдите к настройкам программы.
4. Нажмите **Расписание проверки**.

5. Настройте расписание антивирусной проверки. Рекомендуется запускать антивирусную проверку раз в день.
6. Настройте дополнительные условия запуска антивирусной проверки по расписанию:
 - **Запускать проверку, только если уровень заряда батареи не менее 50%.**
 - **Запускать проверку только при зарядке батареи.**

Дополнительные условия запуска антивирусной проверки позволяют экономить заряд батареи во время работы программы. Вы можете запретить запуск антивирусной проверки при низком уровне заряда батареи и, таким образом, уменьшить потребление заряда батареи программой. Если вы настроили дополнительные условия, Kaspersky Endpoint Security запустит проверку по расписанию, только если все условия выполнены. Если, например, уровень заряда батареи слишком низкий, Kaspersky Endpoint Security отложит запуск антивирусной проверки и будет контролировать уровень заряда батареи. Когда все условия запуска антивирусной проверки будут выполнены, Kaspersky Endpoint Security запустит антивирусную проверку.

В результате Kaspersky Endpoint Security будет запускать антивирусную проверку в фоновом режиме. При обнаружении угроз программа удалит вредоносные файлы автоматически без уведомления пользователя. Администратор может просмотреть результаты проверки в отчетах (см. раздел "Мониторинг работы программы" на стр. [22](#)).

Проверка по расписанию может быть пропущена, если в это время пользователь запустил проверку вручную.

Обновление антивирусных баз


Защита мобильного устройства обеспечивается на основании баз данных, содержащих сигнатуры вирусов и других программ, представляющих угрозу, и информацию о способах борьбы с ними. Kaspersky Endpoint Security использует эту информацию при поиске и обезвреживании зараженных файлов на мобильном устройстве. Базы регулярно пополняются записями о появляющихся угрозах и способах борьбы с ними. Чтобы своевременно обнаруживать угрозы, вам нужно регулярно обновлять антивирусные базы программы.

Основным источником обновлений Kaspersky Endpoint Security служат серверы обновлений "Лаборатории Касперского". Для успешной загрузки пакета обновлений с серверов обновлений "Лаборатории Касперского" мобильное устройство должно быть подключено к интернету. Вы можете изменить источник обновлений и указать корпоративный сервер обновлений (см. инструкцию ниже).

Если базы устарели, Kaspersky Endpoint Security показывает сообщение **Базы давно не обновлялись** на главном экране программы.


Вы можете запустить обновление антивирусных баз вручную или автоматически (по расписанию). Запустить обновление антивирусных баз вручную может любой пользователь. Настроить автоматический запуск обновления антивирусных баз может только администратор.

► *Чтобы обновить антивирусные базы вручную, выполните следующие действия:*

1. Коснитесь значка  в сетке программ или на домашнем экране.
2. Нажмите **Обновление баз**.

Kaspersky Endpoint Security обновит антивирусные базы устройства. Вы можете просмотреть результаты обновления баз в отчетах.


► *Чтобы настроить запуск обновления антивирусных баз по расписанию, выполните следующие действия:*

1. Коснитесь значка  в сетке программ или на домашнем экране.
2. Нажмите **Настройки**.
3. Введите пароль администратора и перейдите к настройкам программы.
4. Нажмите **Расписание обновления**.
5. Настройте расписание обновления баз. Рекомендуется обновлять антивирусные базы раз в день.

Kaspersky Endpoint Security будет запускать обновление антивирусных баз в фоновом режиме. Администратор может просмотреть результаты обновления баз в отчетах (см. раздел "Мониторинг работы программы" на стр. [22](#)).

Обновление антивирусных баз по расписанию может быть пропущено, если в это время пользователь запустил обновление вручную.

► *Чтобы выбрать источник обновлений, выполните следующие действия:*

1. Коснитесь значка  в сетке программ или на домашнем экране.
2. Нажмите **Настройки**.
3. Введите пароль администратора и перейдите к настройкам программы.
4. Нажмите **Источник обновления баз**.
5. Выберите источник обновления:
 - **Серверы "Лаборатории Касперского"**.
 - **Другой источник**. Задайте источник обновления: FQDN (`yourcompany.address`) или IP-адрес (`192.168.1.1`).

Проверьте обновление антивирусных баз. Вы можете просмотреть результаты обновления баз в отчетах.


Мониторинг работы программы

Kaspersky Endpoint Security записывает в отчеты информацию о работе каждого компонента. Программа записывает в отчеты информацию о следующих событиях:

- Запуск и остановка Kaspersky Endpoint Security.
- Запуск и остановка аудита программы.
- Обновление антивирусных баз.
- Антивирусная проверка.
- Устранение угрозы.
- Устройство продолжительное время офлайн.
- Сбой в работе программы.

Отчеты о проверке и обновлении баз доступны всем пользователям. Отчеты о всех событиях доступны только администратору после ввода пароля.

► *Чтобы просмотреть все отчеты, выполните следующие действия:*

1. Коснитесь значка  в сетке программ или на домашнем экране.

2. Нажмите **Отчеты**.

Kaspersky Endpoint Security покажет отчеты о проверке и обновлении баз. Нажмите на отчет для получения подробной информации.


3. Если вы хотите просмотреть все отчеты, нажмите **Все отчеты**.


4. Введите пароль администратора. Kaspersky Endpoint Security покажет все отчеты. Вы можете отфильтровать события. Kaspersky

Endpoint Security хранит события шесть месяцев. По истечении срока хранения событий, программа удалит устаревшие данные.

Обновление антивирусных баз в ручном режиме

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

1. Скопируйте антивирусные базы на сервер, который находится внутри изолированного сегмента сети.
2. В Kaspersky Endpoint Security выберите источник обновления, находящийся в изолированном сегменте сети:
 - a. Коснитесь  значка в сетке программ или на домашнем экране.
 - b. Нажмите **Настройки**.

- c. Введите пароль администратора и перейдите к настройкам программы.
- d. Нажмите **Источник обновления баз** → **Другой источник**.
- e. Введите адрес сервера, который находится внутри изолированного сегмента сети.
3. Убедитесь, что мобильное устройство и источник обновления находятся в одном сегменте сети. Проверьте наличие связи между мобильным устройством и сервером.
4. Обновите антивирусные базы вручную или дождитесь обновления баз по расписанию:
 - a. Коснитесь значка  в сетке программ или на домашнем экране.
 - b. Нажмите **Обновление баз**.
5. Посмотрите результаты обновления баз в отчетах.

Устранение уязвимостей и установка критических обновлений в программе

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

Программу необходимо периодически (не реже одного раза в полгода) подвергать анализу уязвимостей: организация, осуществляющая эксплуатацию программы, должна проводить такой анализ с помощью открытых источников, содержащих базу уязвимостей, в том числе с веб-сайта "Лаборатории Касперского" (<http://www.bdu.fstec.ru>, <https://support.kaspersky.ru/vulnerability>).

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

- Через веб-форму на веб-сайте Службы технической поддержки (<https://support.kaspersky.ru/vulnerability.aspx?el=12429>).
- По адресу электронной почты vulnerability@kaspersky.com.
- В сообществе пользователей "Лаборатории Касперского" (<https://community.kaspersky.com/>).

Действия после сбоя или неустраняемой ошибки в работе программы

Программа автоматически восстанавливает свою работу после сбоев, участие пользователя не требуется. В случае, когда программа не может восстановить свою работу, вам требуется переустановить программу или ее компонент. Вы также можете обратиться за помощью в Службу технической поддержки.

Удаление программы

Удаление Kaspersky Endpoint Security доступно только администратору. Удалить программу обычным способом, принятым для операционной системы Aurora OS, невозможно.

Вы можете удалить Kaspersky Endpoint Security следующими способами:

- удаленно с помощью Аврора Центр;
- локально через приложение Терминал.

Удаление с помощью Аврора Центр

Удаление программы через Аврора Центр выполняет администратор. Удаление выполняется обычным способом, принятым для платформы Аврора. Подробнее об удалении программ с помощью Аврора Центр см. в документации компании "Открытая мобильная платформа" <https://omprussia.ru/>.

Удаление через приложение Терминал

Для удаления Kaspersky Endpoint Security через приложение Терминал учетная запись должна обладать правами суперпользователя (`devel-su`).

► Чтобы удалить Kaspersky Endpoint Security, выполните следующую команду: `rpm`

```
-e kaspersky-kes
```

В результате инструменты операционной системы удалят Kaspersky Endpoint Security. Также будут удалены все файлы, которые были созданы в результате работы программы.

Техническая поддержка

Если вы не нашли решения вашей проблемы в документации, рекомендуется обратиться в Службу технической поддержки. Сотрудники Службы технической поддержки ответят на ваши вопросы об установке и использовании программы.

Вы можете связаться со специалистами Службы технической поддержки по телефону. Вы можете найти информацию о способах получения технической поддержки в вашем регионе и контакты Службы технической поддержки на веб-сайте Службы технической поддержки "Лаборатории Касперского" (<https://support.kaspersky.ru/b2b>). Перед обращением в Службу технической поддержки ознакомьтесь с правилами предоставления технической поддержки (https://support.kaspersky.ru/support/rules#ru_ru).

Информация о стороннем коде

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

Уведомления товарных знаков

Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.

ARM – товарный знак или зарегистрированный товарный знак ARM Ltd. или дочерних компаний.

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

Соответствие терминов

В этом разделе приведено соответствие терминов, используемых в документации, и терминов, используемых в требованиях ФСТЭК.

Таблица 2. Соответствие терминов

| Термин в документации | Термин в требованиях ФСТЭК |
|--|--|
| программа | продукт, объект оценки, программное изделие |
| вирус, программа, представляющая угрозу, вредоносная программа | КВ, компьютерный вирус |
| антивирусные базы, базы программы | базы данных признаков компьютерных вирусов (БД ПКВ) |
| антивирусная проверка | поиск вирусов |
| события | данные аудита |
| администратор | администратор безопасности, уполномоченный субъект информационной системы, уполномоченный пользователь |

Приложение. Значения параметров программы в сертифицированной конфигурации

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

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

Таблица 3. Параметры и их безопасные значения для программы в сертифицированной конфигурации

| Сущность, к которой относится параметр | Название параметра | Безопасное значение или диапазон значений параметра (сертифицированная конфигурация) |
|--|--------------------|--|
|--|--------------------|--|

| | | |
|-----------------------------|-------------------------|---|
| Антивирусная проверка | Расписание проверки | Раз в час – Раз в неделю |
| Обновление антивирусных баз | Источник обновления баз | Серверы "Лаборатории Касперского" или другой источник |
| | Расписание обновления | Раз в час – Раз в неделю |