002.11.6

# Kaspersky Endpoint Security and Management

## Часть II. Управление защитой

kaspersky

Учебный курс

# Содержание

# 1. Как Kaspersky Endpoint Security защищает компьютер

## 1.1 Как злоумышленники атакуют компьютер

### Как вредоносные программы попадают на компьютер


Вредоносные программы попадают не компьютер через все, что связывает компьютер с внешним миром. В частности, через сетевые соединения и через внешние носители. Рассмотрим типичные сценарии, как вредоносные программы проникают на компьютер, и как этому помешать.

#### Через браузер

##### Уязвимый веб-браузер

У пользователя установлен уязвимый браузер. Используя уязвимость, веб-страница может заставить браузер загрузить и запустить на компьютере любую программу. Пользователь заходит на сомнительный веб-сайт — веб-сайт запускает на компьютере пользователя вредоносную программу. Вредоносный код может быть не на основных страницах веб-сайта, а в рекламных блоках, которые веб-сайт получает с других ресурсов.

Чтобы защититься от такой атаки:

— Устанавливайте обновления для веб-браузеров
— Не давайте пользователям запускать какие угодно браузеры
— Не давайте пользователям заходить на какие угодно веб-страницы
— Не давайте пользователям заходить известные зараженные сайты
— Не давайте веб-браузерам запускать дочерние процессы

#### Зараженный файл

Пользователь ищет в Интернете бесплатную программу. Например, бесплатную утилиту, которая делает что-то полезное для пользователя, или пиратскую версию платной программы, или генератор ключей для платной программы. Находит, загружает на компьютер и запускает. Программа оказывается вредоносной.

Может быть пользователь не разобрался и загрузил файл с подходящим названием с «интернет-помойки». Может быть злоумышленники подменили код у бесплатной программы или взломали страницу загрузки и подменили программу.

Чтобы защититься от такой атаки:

- Не давайте пользователям заходить на какие угодно веб-страницы
- Не давайте пользователям заходить известные сайты с вредоносными программами
- Проверяйте файлы, которые пользователь загружает из Интернет, средством защиты от угроз

### Через почту

Пользователь получает по почте письмо, которое выглядит как письмо из банка, магазина, службы доставки, от партнера, знакомого и т.п. Текст письма просит перейти по ссылке или открыть вложение. По ссылке находится вредоносный или фишинговый веб-сайт. Во вложении — вредоносная программа или документ с вложенной вредоносной программой.

Чтобы защититься от такой атаки:

- Фильтруйте почту средствами защиты от спама (массовых анонимных рассылок)
- Проверяйте файлы, вложенные в электронные письма, средством защиты от угроз
- Не давайте пользователям сохранять на диск исполняемые файлы из электронных писем
- От ссылок в письмах защищайтесь как от атак через веб-браузер

### С других компьютеров по сети

#### Из общей папки

Пользователь скопировал из общей папки на другом компьютере программу и запустил ее. Программа оказалась вредоносной.

Пользователь открыл документ из общей папки на другом компьютере. В документе был вредоносный код.

Чтобы защититься от такой атаки:

- Установите средства защиты на все компьютеры
- Проверяйте файлы, которые пользователи копируют, открывают или запускают

#### Атака по сети

В операционной системе на компьютере пользователя есть уязвимость. Если послать на определенный порт специальную последовательность пакетов, можно заставить уязвимую службу выполнить код, который содержится в этих пакетах. Зараженный компьютер в сети атакует уязвимую службу на всех окрестных компьютерах и заражает их.

Чтобы защититься от такой атаки:

- Устанавливайте обновления безопасности для операционной системы
- Запрещайте соединения с портами, которые не нужны для работы пользователя
- Проверяйте пакеты, которые принимает компьютер, на предмет сетевых атак средством защиты от угроз

## С внешних носителей

### Своя «флешка»

Пользователь подключил к компьютеру флешку, скопировать на нее или с нее документы. На флешке есть вредоносная программа, которая использовала уязвимость в операционной системе, чтобы автоматически запуститься на компьютере.

Либо пользователь подключил флешку, чтобы посмотреть, что на ней. Обнаружил документ или исполняемый файл с интригующим названием и решил открыть его. Файл оказался зараженным.

Чтобы защититься от такой атаки:

- Не разрешайте пользователям подключать к компьютеру неизвестные (или все) флешки
- Проверяйте файлы на флешках средством защиты от угроз
- Устанавливайте обновления безопасности для операционной системы

### BadUSB

Пользователь подключил к компьютеру USB-устройство, которое выглядит как флешка. Устройство зарегистрировалось в операционной системе как флешка, и как клавиатура. Через некоторое время устройство начало давать компьютеру команды, посылая сигналы нажатия клавиш.

Чтобы защититься от такой атаки, используйте средства защиты от атак BadUSB

## Как защищаться от угроз

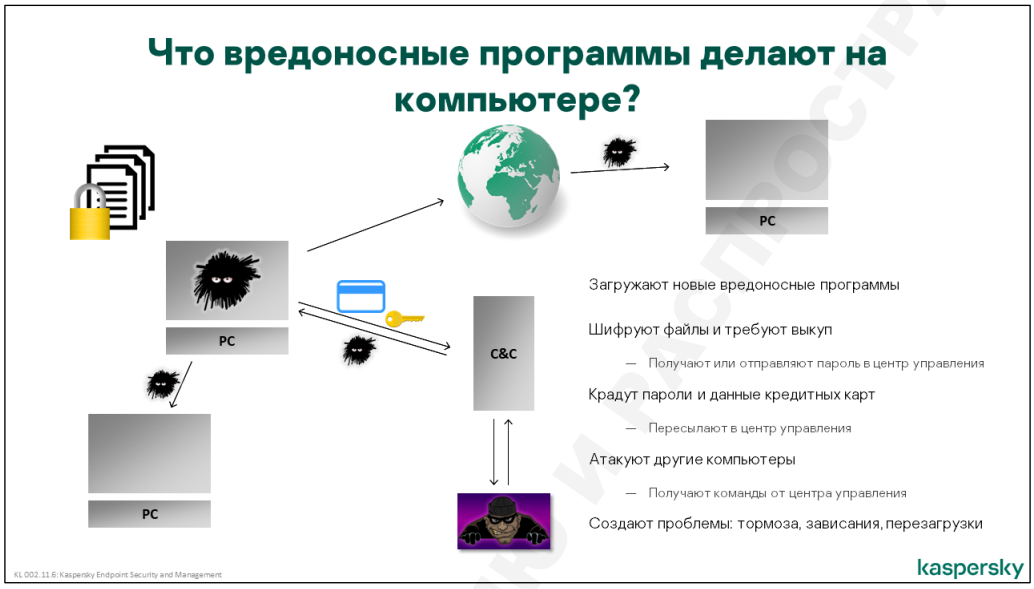
Все способы, как защититься от угроз, можно разделить на:

| Устраните потенциальные цели атак |
|---|
| Устанавливайте обновления безопасности для операционной системы |
| Устанавливайте обновления для веб-браузеров и других программ |
| Не давайте пользователям запускать какие угодно браузеры |
| Не давайте пользователям заходить на какие угодно веб-страницы |
| Не давайте веб-браузерам запускать дочерние процессы |
| Не давайте пользователям сохранять на диск исполняемые файлы из электронных писем |
| Запрещайте соединения с портами, которые не нужны для работы пользователя |
| Не разрешайте пользователям подключать к компьютеру неизвестные (или все) флешки |
| **Используйте средства защиты, чтобы обнаруживать атаки** |
| Установите средства защиты на все компьютеры |
| Проверяйте файлы, которые пользователи копируют, открывают или запускают |
| Проверяйте файлы на флешках средством защиты от угроз |
| Проверяйте файлы, вложенные в электронные письма, средством защиты от угроз |
| Проверяйте файлы, которые пользователь загружает из Интернет, средством защиты от угроз |
| Не давайте пользователям заходить известные зараженные сайты |
| Не давайте пользователям заходить известные сайты с вредоносными программами |

Проверяйте пакеты, которые принимает компьютер, на предмет сетевых атак средством защиты от угроз

Используйте средства защиты от атак BadUSB

## Как вредоносные программы наносят вред




Ни одно средство защиты не защищает от 100% угроз. Злоумышленники всегда могут оказаться на полшага впереди, за счет того, что они

- Регистрируют новые домены и веб-сайты
- Пишут новые вредоносные программы
- Используют уязвимости нулевого дня, для которых еще нет обновлений

Даже если средства защиты работают, как положено, есть риск, что компьютер будет заражен новой вредоносной программой. Если защита установлена не на всех компьютерах, если на компьютерах старые базы, если выключены важные компоненты защиты — риск возрастает.

Рассмотрим, какой вред несут вредоносные программы и как можно его уменьшить.

### Вымогатели

Вредоносная программа вымогатель шифрует документы и другие файлы на компьютере и в общих папках, и просит деньги за то, чтобы дать ключ шифрования. Ключ хранится на сервере злоумышленников. Вредоносная программа или загружает ключ с сервера, шифрует файлы и удаляет ключ; или формирует случайный ключ, посылает его на сервер, шифрует файлы и ключ удаляет. В любом случае программа-вымогатель связывается со своим сервером по сети.

Чтобы защититься от такой атаки:

- Регулярно делайте резервные копии всех важных файлов
- Не давайте неизвестным программам устанавливать и принимать сетевые соединения
- Используйте средства защиты, которые эвристически обнаруживают шифрование

### Шпионы

Вредоносная программа ищет незашифрованные или слабо зашифрованные пароли в настройках программ и в файлах на диске. Вредоносная программа перехватывает все, что вводит пользователь с клавиатуры, делает скриншоты экрана и снимки через веб-камеру. Все это программа оправляет на сервер злоумышленникам.

Чтобы защититься от такой атаки:

- Не давайте неизвестным программам устанавливать и принимать сетевые соединения
- Используйте средства защиты, которые эвристически обнаруживают шпионские действия

### Сетевые вредоносные программы

Вредоносная программа записывает себя на подключенные к компьютеру флешки и в общие папки по сети. Вредоносная программа заражает соседние компьютеры через уязвимые службы. Вредоносная программа по команде из центра рассылает спам и участвует в DDOS-атаках.

Чтобы защититься от такой атаки:

- Не давайте неизвестным программам устанавливать и принимать сетевые соединения
- Используйте средства защиты, которые эвристически обнаруживают опасные действия

### Загрузчики

Часто, чтобы заразить обойти средства защиты и заразить компьютер, злоумышленники используют очень простые файлы, которые не несут никакого прямого ущерба. Но эти файлы могут загрузить дополнительные вредоносные файлы, которые уже могут шифровать документы, воровать пароли и т.д.

Чтобы защититься от такой атаки, не давайте неизвестным программам устанавливать и принимать сетевые соединения

### Некачественные вредоносные программы

Вредоносная программа приводит к тому, что другие программы зависают или работают с ошибками, компьютер тормозит, спонтанно перезагружается и выводит синий экран.

Чтобы защититься от такой атаки, регулярно проверяйте файлы на компьютере средством защиты от угроз

### Как уменьшить урон

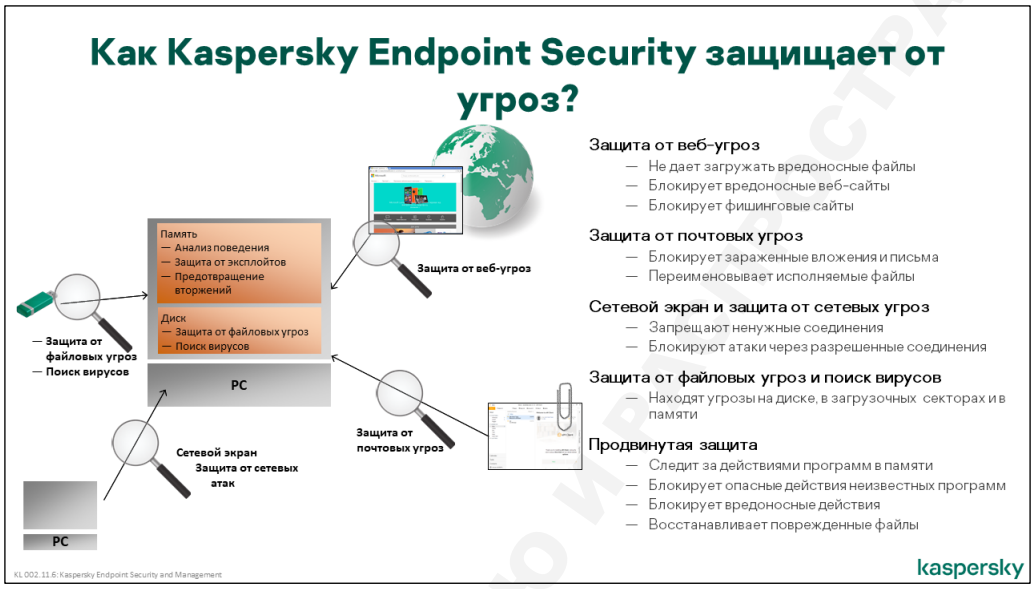
Способы уменьшить урон можно разделить так же, как и способы защититься от атаки:

| **Устраните потенциальные цели атак** |
| --- |
| Не давайте неизвестным программам устанавливать и принимать сетевые соединения |
| **Используйте средства защиты, чтобы обнаруживать атаки** |
| Используйте средства защиты, которые эвристически обнаруживают опасные действия |

Регулярно проверяйте файлы на компьютере средством защиты от угроз

# 1.2 Как Kaspersky Endpoint Security противостоит атакам

## Как Kaspersky Endpoint Security защищает от угроз




Компоненты Kaspersky Endpoint Security и Kaspersky Security Center делают все, чтобы защитить от атак и предотвратить ущерб.

| Устраните потенциальные цели атак | |
|---|---|
| Устанавливайте обновления безопасности для операционной системы | Kaspersky Security Center (см. курс KL 009) |
| Устанавливайте обновления для веб-браузеров и других программ | Kaspersky Security Center (см. курс KL 009) |
| Не давайте пользователям запускать какие угодно браузеры | Контроль программ |
| Не давайте пользователям заходить на какие угодно веб-страницы | Веб-контроль |
| Не давайте веб-браузерам запускать дочерние процессы | Анализ поведения<br>Защита от эксплойтов |
| Не давайте пользователям сохранять на диск исполняемые файлы из электронных писем | Защита от почтовых угроз |
| Запрещайте соединения с портами, которые не нужны для работы пользователя | Сетевой экран |
| Не разрешайте пользователям подключать к компьютеру неизвестные (или все) флешки | Контроль устройств |
| Не давайте неизвестным программам устанавливать и принимать сетевые соединения | Сетевой экран |

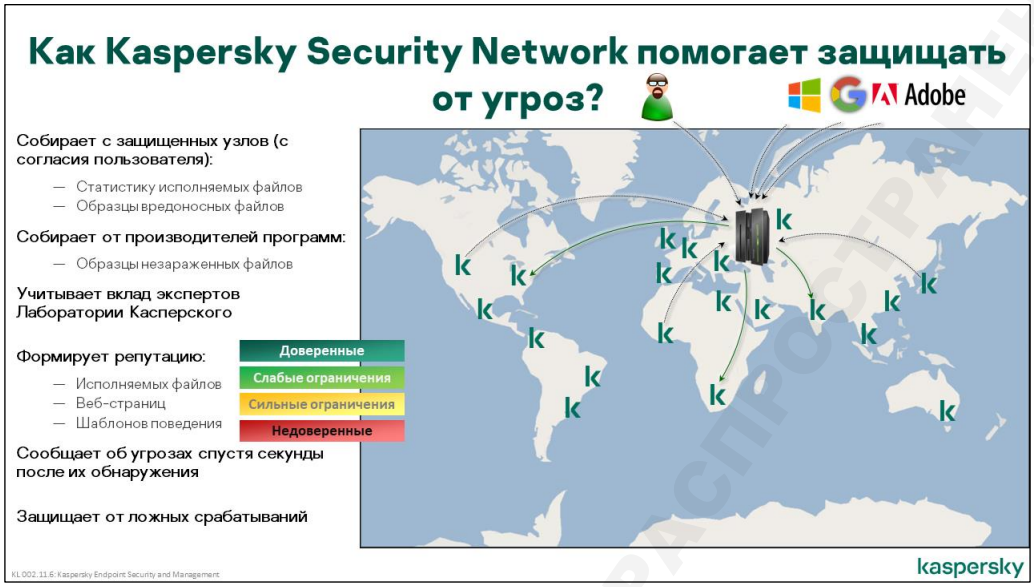
| Используйте средства защиты, чтобы обнаруживать атаки | |
|---|---|
| Установите средства защиты на все компьютеры | Kaspersky Security Center (см. Часть 1) |
| Проверяйте файлы, которые пользователи копируют, открывают или запускают | Защита от файловых угроз<br>Предотвращение вторжений |
| Проверяйте файлы на флешках средством защиты от угроз | Поиск вирусов |
| Проверяйте файлы, вложенные в электронные письма, средством защиты от угроз | Защита от почтовых угроз |
| Проверяйте файлы, которые пользователь загружает из Интернет, средством защиты от угроз | Защита от веб-угроз |
| Не давайте пользователям заходить известные зараженные и фишинговые сайты | Защита от веб-угроз |
| Не давайте пользователям заходить известные сайты с вредоносными программами | Защита от веб-угроз |
| Проверяйте пакеты, которые принимает компьютер, на предмет сетевых атак средством защиты от угроз | Защита от сетевых угроз |
| Не давайте пользователям возможность автоматически подключать любые USB устройства в качестве клавиатуры | Защита от атак BadUSB |
| Используйте средства защиты, которые эвристически обнаруживают опасные действия | Анализ поведения<br>Предотвращение вторжений |
| Регулярно проверяйте файлы на компьютере средством защиты от угроз | Поиск вирусов |

В этом списке есть все компоненты Kaspersky Endpoint Security. Все они либо уменьшают поверхность атаки, либо активно ищут, обнаруживают и блокируют угрозы.

Kaspersky Endpoint Security не делает резервные копии файлов на компьютерах, и не защищает от спама. От спама защищают продукты Лаборатории Касперского для почтовых систем, такие как:

— Kaspersky Security для Microsoft Exchange Server
— Kaspersky Secure Mail Gateway

# Как Kaspersky Security Network помогает защищать от угроз




Чтобы компоненты Kaspersky Endpoint Security защищали от угроз, важно регулярно обновлять базы сигнатур.

Не менее важно разрешить Kaspersky Endpoint Security использовать Kaspersky Security Network.

Kaspersky Security Network (KSN) — это «облачная» технология, которая повышает точность вердиктов всех компонентов защиты.

Сервера Kaspersky Security Network собирают информацию о файлах на защищенных компьютерах, анализирует их с помощью технологий машинного обучения, учитывает, когда файл был впервые обнаружен, как широко он распространен, в каких регионах, доверяют ли файлу пользователи персональных версий Kaspersky Security, подписан ли файл сертификатом и каким и т.п. Подозрительные файлы дополнительно анализируют эксперты Лаборатории Касперского.

После всего этого Kaspersky Security Network присваивает файлу группу доверия:

— Доверенные
— Слабые ограничения
— Сильные ограничения
— Недоверенные

Для каждой группы доверия аналитиками Лаборатории Касперского, разработаны сценарии, в которых описано, что можно и что нельзя делать файлам в зависимости от присвоенной им группы доверия (репутации).

Именно так компоненты Kaspersky Endpoint Security знают, каким программам можно выходить в сеть, а каким нельзя, каким программам можно устанавливать драйверы, а каким не стоит, и какие доверенные программы нужно проверять особенно тщательно, потому что в них могут быть уязвимости.

Kaspersky Security Network содержит огромную базу контрольных сумм заведомо хороших файлов. Лаборатория Касперского получает контрольные суммы эталонных файлов от многих известных производителей программ, таких как Microsoft, Adobe, Google и др. За счет этого компоненты Kaspersky Endpoint Security знают, какие файлы точно не заражены и мешают работе программ.

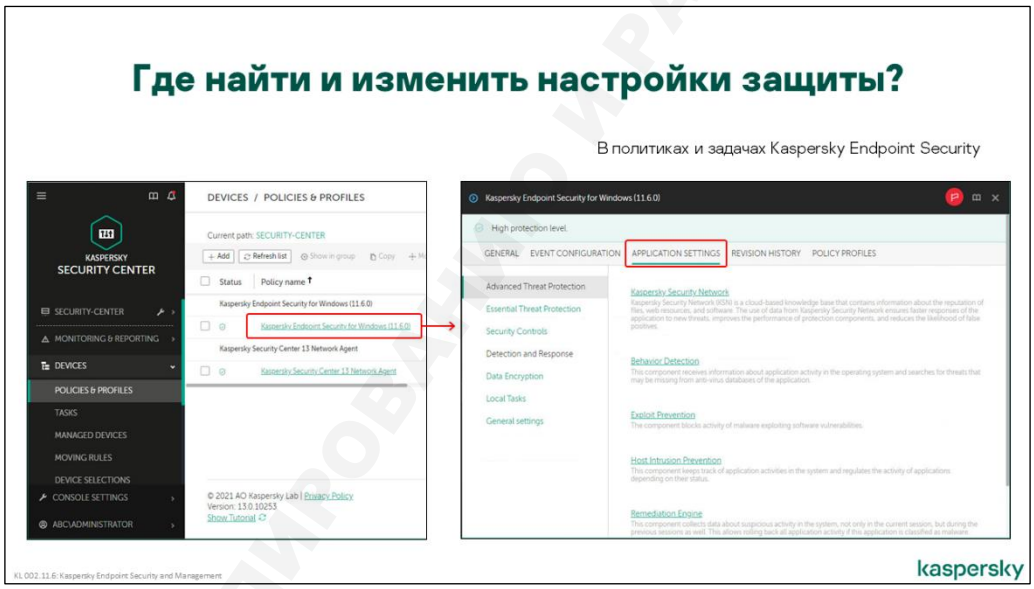
Кроме файлов Kaspersky Security Network формирует репутацию веб-страниц и шаблонов поведения программ.

Если Лаборатория Касперского обнаруживает новую угрозу, контрольные суммы всех вредоносных файлов и веб-страниц оказываются в Kaspersky Security Network через доли секунды и доступны всем продуктам, которые используют Kaspersky Security Network. Через Kaspersky Security Network продукты узнают о новых угрозах на несколько часов раньше, чем сигнатуры угроз поступают с обновлениями.

Данные, которые Kaspersky Endpoint Security посылает в Kaspersky Security Network, обезличены и анонимны. Полный список можно найти в соглашении Kaspersky Security Network, которое администратор обязан принять, чтобы включить Kaspersky Security Network в политике Kaspersky Endpoint Security.

Чтобы использовать Kaspersky Security Network, но ничего не посылать в Лабораторию Касперского, существует услуга Kaspersky Private Security Network.

## Где находятся настройки Kaspersky Endpoint Security



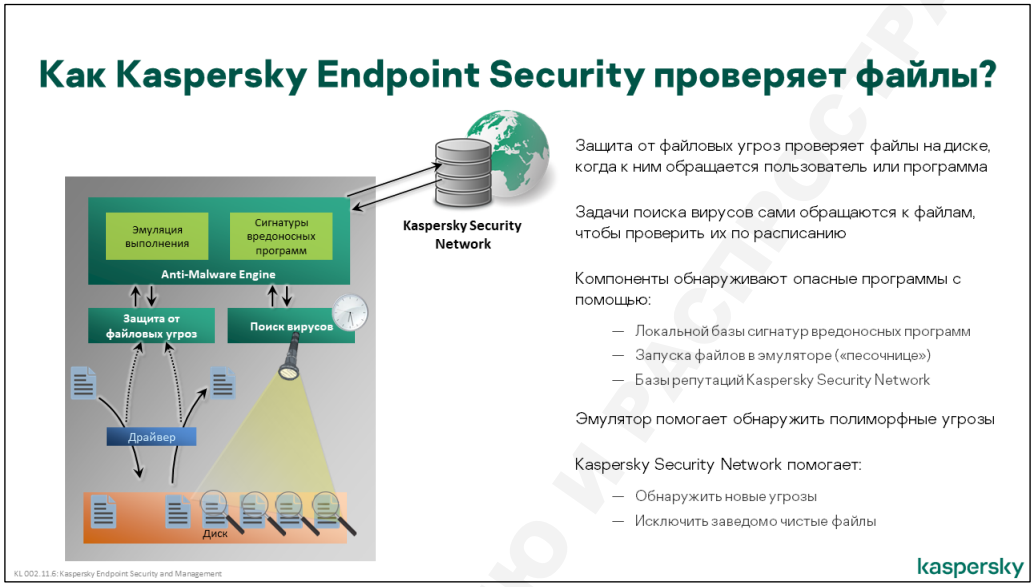

В этой части курса мы изучим:

- Какие настройки есть у компонентов Kaspersky Endpoint Security
- Какие у них значения по умолчанию
- Как разные параметры меняют поведение компонентов
- Когда и как менять настройки, чтобы улучшить защиту компьютера или комфорт пользователей

Большинство настроек Kaspersky Endpoint Security находятся в политике. Часть настроек, например, настройки поиска вирусов по расписанию, настройки обновления или настройки удаления данных, находятся в задачах.

# 2. Как настроить защиту файлов

## 2.1 Как Kaspersky Endpoint Security защищает файлы?




С помощью драйвера **klif.sys** Защита от файловых угроз перехватывает все файловые операции (такие как, чтение, копирование, выполнение) и проверяет файлы, с которыми выполняются действия. В случае если файл заражен, операция блокируется, а сам файл лечится или удаляется.

Если не считать уязвимости, которые позволяют вредоносным программам загрузить код в память, все атаки сохраняют вредоносные файлы на диск компьютера. И даже те атаки, которые начинаются с выполнения кода в памяти, могут загрузить только код небольшого размера и используют его как первую ступень атаки, которая загружает дополнительные модули в виде файлов и сохраняет на их диск.

Можно отключить Защиту от почтовых угроз и Защиту от веб-угроз, но пользователь все равно не сможет запустить зараженный файл, полученный по почте или из сети Интернет. В момент сохранения файла на диск его обнаружит и заблокирует Защита от файловых угроз. А запустить файл из вложения или веб-страницы без сохранения на диск нельзя.

Поэтому Защита от файловых угроз — один из важных компонентов Kaspersky Endpoint Security.

Защита от файловых угроз ищет вредоносные программы с помощью:

— Сигнатур вредоносных программ — база сигнатур — это «стоп-лист» известных вредоносных файлов. Если файл не соответствует ни одной записи в базе, значит он не вредоносный. Полноценный список, где у каждого известного вредоносного или зараженного файла есть отдельная запись, требует слишком много места, поэтому база сигнатур — это оптимизированный список, уменьшенный до размера, который можно загрузить на компьютер. Каждая запись идентифицирует семейство похожих угроз.

— Эвристического анализа (эмуляции выполнения) — помогает обнаруживать полиморфные вредоносные файлы, которые меняют свой код во время выполнения, и которые из-за этого сложно обнаружить по сигнатурам. Защита от файловых угроз запускает

исполняемые файлы в специальной изолированной среде и ждет, не изменится ли код в памяти так, что начнет соответствовать сигнатуре.

— Проверки по KSN — Защита от файловых угроз посылает в KSN контрольную сумму файла и получает ответ: есть ли такой файл в базе KSN, и какая у него репутация. База KSN это и есть огромный список всех известных Лаборатории Касперского файлов (вернее, их контрольных сумм). В этом списке есть файлы с репутацией *недоверенные*. Это черный список, такие файлы Защита от файловых угроз блокирует. Есть файлы с репутацией *доверенные*. Это белый список, куда входят известные невредоносные файлы операционных систем и распространенных программ. Эти файлы Защита от файловых угроз не блокирует, даже если по сигнатурам они вредоносные. Вердикт KSN имеет больший приоритет, потому что KSN содержит больше информации, чем локальная база сигнатур.

Чтобы получить вердикт из KSN, компьютеру нужна связь с Интернет, которая может быть ненадежной. Именно поэтому Kaspersky Endpoint Security не полагается исключительно на KSN, а использует базу сигнатур и эмуляцию.

Вердикты KSN могут меняться со временем. У файла, который недавно появился в сети Интернет, сначала нет никакой репутации. Со временем, когда KSN накапливает данные о том, кто, где и как использует этот файл, его репутация меняется и может стать как доверенной, так и недоверенной. Для наилучшей защиты, Kaspersky Endpoint Security мог бы уточнять вердикт KSN при каждой файловой операции. Но это бы сильно увеличило сетевой трафик компьютера. И к тому же, на то, чтобы отправить запрос и получить ответ, уходит время, которое зависит от качества связи.

Чтобы не создавать лишний трафик и не задерживать операции с файлами, Kaspersky Endpoint Security сохраняет вердикты KSN в локальный кэш. У каждого вердикта есть время хранения. Для новых файлов оно короткое, и заставляет Kaspersky Endpoint Security часто уточнять вердикт. Для файлов, которые известны давно, это время большое.

Чтобы не замедлять компьютер, Защита от файловых угроз проверяет не все файлы, а только те файлы, которые могут заразить компьютер. Например, Защита от файловых угроз не проверяет архивы, потому что, чтобы запустить файл из архива, этот файл нужно извлечь. Если пользователь сам не извлек файл из архива, это делает операционная система незаметно для пользователя. В любом случае Защита от файловых угроз проверит и, если нужно, заблокирует извлеченные файлы.

Файлы, которые не проверила Защита от файловых угроз, проверяйте задачами поиска вирусов. Поиск вирусов проверяет файлы в указанной области и применяет те же методы, что и Защита от файловых угроз.

## Как Kaspersky Endpoint Security защищает файлы в Windows Subsystem for Linux?

Подсистема Windows для Linux (WSL) – это слой совместимости, который позволяет запускать собственные средства командной строки Linux непосредственно в Windows 10 или Windows Server 2016. Как и контейнеры Docker, основной задачей, которую решает WSL является предоставление кроссплатформенного инструмента для разработчиков, особенно для веб разработчиков, и для тех, кто работает с открытым исходным кодом.

Преимуществом WSL перед стандартной виртуализацией являются: простота установки, меньшее потребление ресурсов по сравнению с гипервизором, или виртуальной машиной.

В Windows Server 2016 администратор может развернуть следующие Linux системы: Ubuntu, openSUSE Leap42, SUSE Linux Enterprise Server.

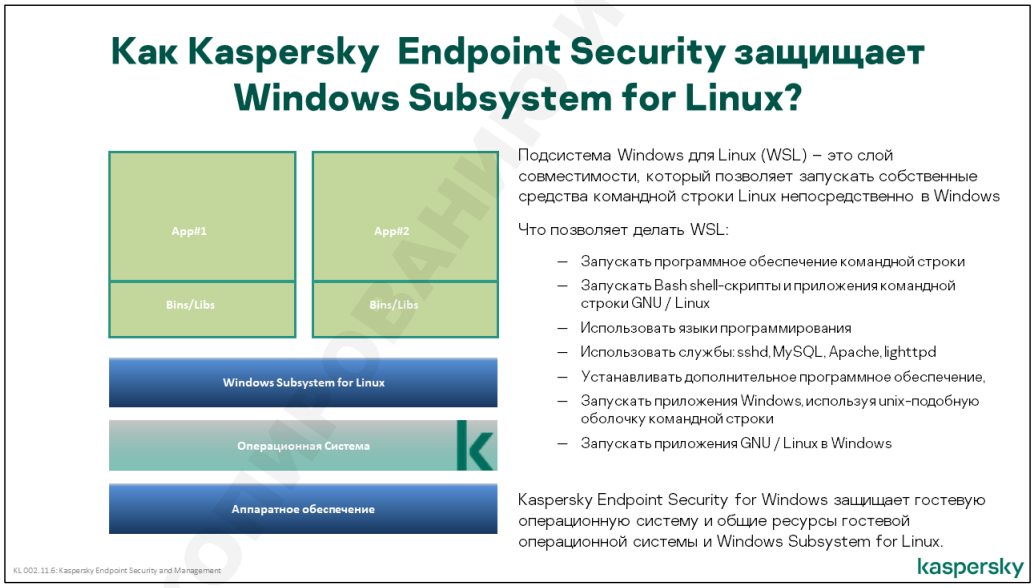
Windows Subsystem for Linux представляет собой приложение под названием wsl.exe (в старых версиях Windows bash.exe), которое возможно запустить через командную строку Windows

(cmd.exe). После запуска Bash.exe будет инициализирована ранее выбранная и установленная версия Linux: Ubuntu, openSUSE Leap42, или SUSE Linux Enterprise Server.

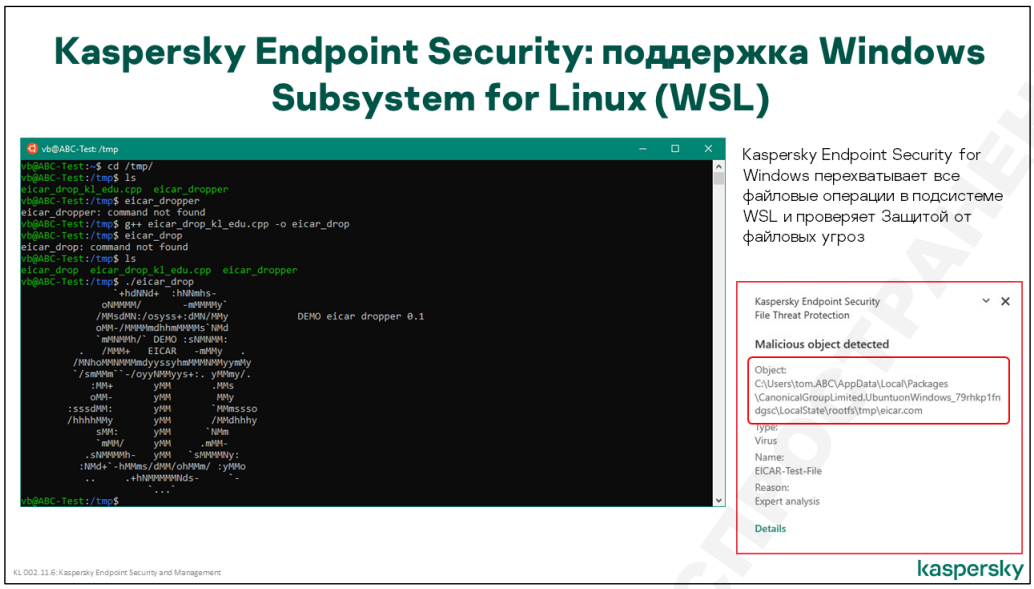
Windows Subsystem for Linux транслирует системные вызовы Linux в системные вызовы Windows, что позволяет развернуть в основном окружении Windows полноценный инструментарий Linux без эмуляции и виртуализации.

Что позволяет делать WSL:

- Запускать программное обеспечение командной строки, такое как grep, sed, awk
- Запускать Bash shell-скрипты и приложения командной строки GNU / Linux, включая vim, emacs, tmux
- Использовать языки программирования: Javascript / node.js, Ruby, Python, C / C ++, C #, Go и т.д.
- Использовать службы: sshd, MySQL, Apache, lighttpd
- Устанавливать дополнительное программное обеспечение, используя собственный менеджер пакетов дистрибутива GNU / Linux.
- Запускать приложения Windows, используя unix-подобную оболочку командной строки,
- Запускать приложения GNU / Linux в Windows.

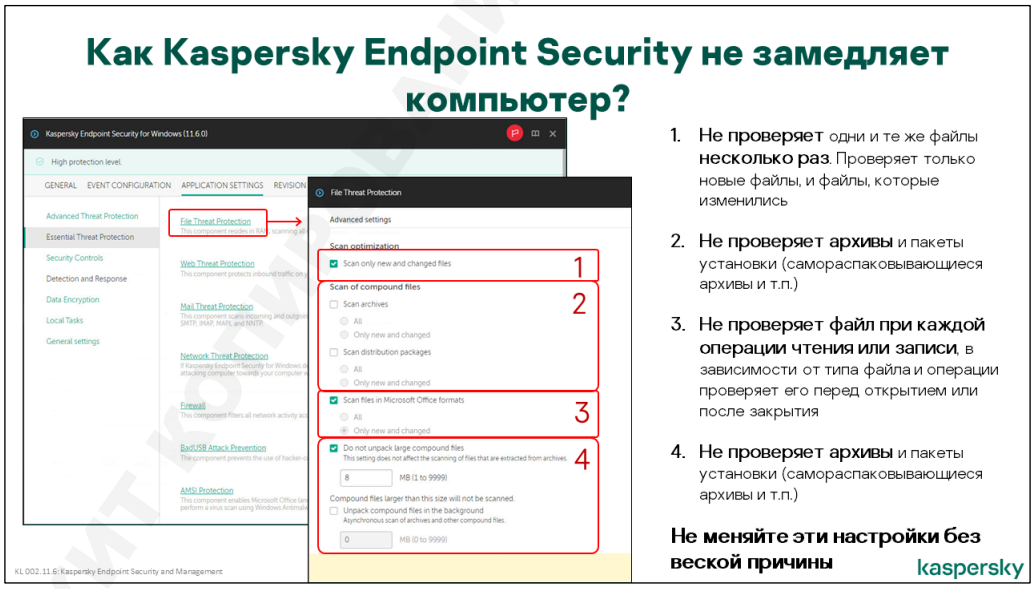



Слой совместимости Windows Subsystem for Linux совместно использует файловую систему основной операционной системы, на которую установлен. Таким образом все файловые операции, выполняемые в подсистеме Linux, будут перехвачены Защитой от файловых угроз.




Если вредоносный файл будет скомпилирован или запущен в Linux среде данное действие будет обнаружено и устранено Защитой от файловых угроз Kaspersky Endpoint Security.

# 2.2 Что и как настроить в Защите от файловых угроз




## Настройки Защиты от файловых угроз

Защита от файловых угроз, как и Kaspersky Endpoint Security в целом, решает две задачи:

— Не дать вредоносным программам нанести ущерб
— Не мешать работать пользователю и программам

Чем больше файлов проверяет Защита от файловых угроз, тем лучше он решает первую задачу, и тем хуже вторую. И наоборот. Настройки по умолчанию обеспечивают баланс между защитой и

производительностью. Меняя настройки, администратор может сместить баланс в ту или другую сторону.

Администратор меняет настройки Kaspersky Endpoint Security в политике. Настройки всех компонентов находятся в одноименных областях: настройки Защиты от файловых угроз в разделе **Базовая защита | Защита от файловых угроз** на вкладке **Параметры программы**.

Рассмотрим сначала параметры, которые не нужно менять и почему.

## Защита от файловых угроз проверяет не все типы файлов

Файлы, которые могут нанести вред компьютеру, это в основном исполняемые файлы, но не только. Документы Microsoft Office могут содержать исполняемый код (макросы), который может быть вредоносным. Даже документы без кода, некоторые графические файлы, могут использовать уязвимости в программах, которые их открывают, и заставить эти программы выполнить часть файла как код.

По умолчанию Защита от файловых угроз проверяет файлы по формату. Так Kaspersky Endpoint Security надежно защищает компьютер, поскольку *проверяет все опасные файлы*, но меньше загружает компьютер, поскольку *проверяет не все файлы*.

Проверять файлы только по расширению опасно. Например, вредоносный документ Word может иметь расширение *.123*, которое не входит в список проверяемых, но пользователь все равно может его открыть через контекстное меню *Открыть с помощью*. К тому же, проверять по расширению не намного быстрее, чем проверять по формату. Пользователь не заметит разницы в производительности.

Если администратор хочет улучшить производительность медленных компьютеров, лучше начать с исключений для программ, с которыми работают пользователи. Как создавать исключения, рассказывается в конце этого раздела.

Список проверяемых расширений:

| | |
|---|---|
| **com** | исполняемый файл программы размером не более 64 КБ |
| **exe** | исполняемый файл, самораспаковывающийся архив |
| **sys** | системный файл Microsoft Windows |
| **prg** | текст программы dBase™, Clipper или Microsoft Visual FoxPro®, программа пакета WAVmaker |
| **bin** | бинарный файл |
| **bat** | файл пакетного задания |
| **cmd** | командный файл Microsoft Windows NT (аналогичен bat-файлу для DOS), OS/2 |
| **dpl** | упакованная библиотека Borland Delphi |
| **dll** | библиотека динамической загрузки |
| **scr** | файл-заставка экрана Microsoft Windows |
| **cpl** | модуль панели управления (control panel) в Microsoft Windows |
| **ocx** | объект Microsoft OLE (Object Linking and Embedding) |
| **tsp** | программа, работающая в режиме разделения времени |
| **drv** | драйвер некоторого устройства |

| | |
|---|---|
| **vxd** | драйвер виртуального устройства Microsoft Windows |
| **pif** | файл с информацией о программе |
| **lnk** | файл-ссылка в Microsoft Windows |
| **reg** | файл регистрации ключей системного реестра Microsoft Windows |
| **ini** | файл конфигурации, который содержит данные настроек для Microsoft Windows, Windows NT и некоторых программ |
| **cla** | класс Java |
| **vbs** | скрипт Visual Basic |
| **vbe** | видеорасширение BIOS |
| **js, jse** | исходный текст JavaScript |
| **htm** | гипертекстовый документ |
| **htt** | гипертекстовая заготовка Microsoft Windows |
| **hta** | гипертекстовая программа для Microsoft Internet Explorer |
| **asp** | скрипт Active Server Pages |
| **chm** | скомпилированный HTML-файл |
| **pht** | HTML-файл со встроенными скриптами PHP |
| **php** | скрипт, встраиваемый в HTML-файлы |
| **wsh** | файл Microsoft Windows Script Host |
| **wsf** | скрипт Microsoft Windows |
| **the** | файл заставки для рабочего стола Microsoft Windows 95 |
| **hlp** | файл справки формата Win Help |
| **eml** | сообщение Microsoft Outlook Express |
| **nws** | новое сообщение электронной почты Microsoft Outlook Express |
| **msg** | сообщение электронной почты Microsoft Mail |
| **plg** | сообщение электронной почты |
| **mbx** | расширение для сохраненного сообщения Microsoft Office Outlook |
| **doc*** | документы Microsoft Office Word, такие как: |
| **doc** | документ Microsoft Office Word |
| **docx** | документ Microsoft Office Word 2007 с поддержкой языка XML |
| **docm** | документ Microsoft Office Word 2007 с поддержкой макросов |
| **dot*** | шаблоны документа Microsoft Office Word, такие как: |
| **dot** | шаблон документа Microsoft Office Word |
| **dotx** | шаблон документа Microsoft Office Word 2007 |

| | |
|---|---|
| **dotm** | шаблон документа Microsoft Office Word 2007 с поддержкой макросов |
| **fpm** | программа баз данных, стартовый файл Microsoft Visual FoxPro |
| **rtf** | документ в формате Rich Text Format |
| **shs** | фрагмент Windows Shell Scrap Object Handler |
| **dwg** | база данных чертежей AutoCAD |
| **msi** | пакет Microsoft Windows Installer |
| **otm** | VBA-проект для Microsoft Office Outlook |
| **pdf** | документ Adobe Acrobat |
| **swf** | объект пакета Shockwave Flash |
| **jpg, jpeg** | файл графического формата хранения сжатых изображений |
| **emf** | файл формата Enhanced Metafile. Следующее поколение метафайла операционной системы Microsoft Windows. Файлы EMF не поддерживаются 16-разрядной Microsoft Windows |
| **ico** | файл значка объекта |
| **ov?** | исполняемые файлы Microsoft Office Word |
| **xl*** | документы и файлы Microsoft Office Excel, такие как: |
| **xla** | расширение Microsoft Office Excel |
| **xlc** | диаграмма Microsoft Office Excel |
| **xlt** | шаблон документа Microsoft Office Excel |
| **xlsx** | xlsx – рабочая книга Microsoft Office Excel 2007 |
| **xltm** | рабочая книга Microsoft Office Excel 2007 с поддержкой макросов |
| **xlsb** | рабочая книга Microsoft Office Excel 2007 в бинарном (не XML) формате |
| **xltx** | шаблон Microsoft Office Excel 2007 |
| **xlsm** | шаблон Microsoft Office Excel 2007 с поддержкой макросов |
| **xlam** | xlam – надстройка Microsoft Office Excel 2007 с поддержкой макросов |
| **pp*** | pp* – документы и файлы Microsoft Office PowerPoint, такие как: |
| **pps** | слайд Microsoft Office PowerPoint |
| **ppt** | презентация Microsoft Office PowerPoint |
| **pptx** | презентация Microsoft Office PowerPoint 2007 |
| **pptm** | презентация Microsoft Office PowerPoint 2007 с поддержкой макросов |
| **potx** | шаблон презентации Microsoft Office PowerPoint 2007 |
| **potm** | шаблон презентации Microsoft Office PowerPoint 2007 с поддержкой макросов |
| **ppsx** | слайд-шоу Microsoft Office PowerPoint 2007 |
| **ppsm** | слайд-шоу Microsoft Office PowerPoint 2007 с поддержкой макросов |

| | |
|---|---|
| **ppam** | надстройка Microsoft Office PowerPoint 2007 с поддержкой макросов |
| **md*** | документы и файлы Microsoft Office Access, такие как: |
| **mda** | рабочая группа Microsoft Office Access |
| **mdb** | база данных Microsoft Office Access |
| **sldx** | слайд Microsoft Office PowerPoint 2007 |
| **sldm** | слайд Microsoft Office PowerPoint 2007 с поддержкой макросов |
| **thmx** | тема Microsoft Office 2007 |

Эвристический анализ в Kaspersky Endpoint Security запускает исполняемый программы в изолированной среде и смотрит, что они делают. В первую очередь эвристический анализ помогает обнаруживать полиморфные вредоносные программы, которые меняют свой код во время выполнения.

Когда злоумышленники рассылают новую вредоносную программу по почте, или загружают новую версию вредоносного модуля на зараженный компьютер, они могут генерировать файл с уникальной контрольной суммой для каждого компьютера или адресата. Сигнатуры и даже Kaspersky Security Network в этом случае не помогут. Но эвристический анализ как раз и позволит увидеть, что все эти варианты после запуска восстанавливают одинаковый вредоносный код.

## Защита от файловых угроз не проверяет файлы, которые уже проверяла

Большая часть файлов на компьютере меняется редко, поэтому проверяя только новые и измененные файлы, Защита от файловых угроз почти не загружает компьютер. В первые несколько дней, пока все файлы для Kaspersky Endpoint Security новые, пользователь может ощущать, что компьютер работает медленнее. Но довольно скоро Защита от файловых угроз перестает заметно влиять на производительность.

Не выключайте опцию **Проверять только новые и измененные файлы** в Защите от файловых угроз, это замедлит компьютер.

### Как Kaspersky Endpoint Security узнает, какие файлы менялись, а какие нет?

Файловая система NTFS (и ее наследник ReFS) записывает, когда файлы меняются, и гарантирует целостность этих записей. Поэтому на дисках с файловой системой NTFS Kaspersky Endpoint Security просто смотрит на дату изменения файла.

Файловая система FAT32 может не записывать дату изменения, и не защищает саму дату изменения от изменений. Вредоносная программа может изменить файл, а потом записать ему какую угодно дату изменения. Поэтому на дисках с файловой системой FAT32 Kaspersky Endpoint Security сохраняет в специальную базу контрольные суммы проверенных файлов. При следующем обращении Kaspersky Endpoint Security заново вычисляет контрольную сумму и сравнивает ее с сохраненной. Если суммы отличаются, значит файл изменился, и Защита от файловых угроз его проверяет.

Проверять новые файлы только один раз опасно. Если вредоносная программа попала на компьютер до того, как Kaspersky Endpoint Security получил ее сигнатуры, Защита от файловых угроз ее проверит, посчитает чистой, и не будет проверять при следующих запусках.

Чтобы так не случилось, даже когда опция **Проверять только новые и измененные файлы** включена, Защита от файловых угроз проверяет все новые файлы не один раз, а как минимум два раза или даже несколько раз.

Для этого Kaspersky Endpoint Security хранит время выпуска сигнатур, которыми проверял файл первый раз и последний раз. Если файл проверялся только один раз или если текущая версия сигнатур отличается от той, которой файл был проверен первый раз, меньше, чем на 24 часа, Защита от файловых угроз проверяет файл еще раз.

Что если сигнатуры для новой угрозы не появятся за 24 часа? Такого почти никогда не бывает. Тем более, кроме сигнатур, Kaspersky Endpoint Security использует информацию из Kaspersky Security Network, куда сведения об угрозах попадают без задержек.

Чтобы еще снизить риск, используйте поиск вирусов, чтобы проверять все файлы на компьютере, в том числе и те, которые не менялись, и которые Защита от файловых угроз уже проверяла.

## Защита от файловых угроз не проверяет составные файлы (архивы и пр.)

| Параметры программы \| Базовая защита \| Защита от файловых угроз \| Проверять архивы | |
|---|---|
| **Включено** | Защита от файловых угроз проверяет файлы внутри архивов форматов RAR, ARJ, ZIP, CAB, LHA, JAR, ICE. Для этого Защита от файловых угроз распаковывает файлы из архива во временную папку или в память |
| **Выключено (по умолчанию)** | Защита от файловых угроз не распаковывает архивы и не проверяет файлы в них |

Чтобы проверить файлы в архиве, Защита от файловых угроз распаковывает архив, и на это уходит много ресурсов компьютера. Сами по себе архивы не опасны. Даже если в архиве есть вредоносный файл, его нельзя запустить из архива. Пользователь либо сам распакует архив, либо это сделает операционная система незаметно для пользователя. В любом случае вредоносный файл попадает на диск, и Защита от файловых угроз проверяет его как обычный файл.

Не включайте опцию **Проверять архивы** в Защите от файловых угроз. Это замедлит компьютер и не повлияет на защиту

| Параметры программы \| Базовая защита \| Защита от файловых угроз \| Проверять дистрибутивы | |
|---|---|
| **Включено** | Защита от файловых угроз проверяет файлы внутри самораспаковывающихся архивов и установочных пакетов, таких, как MSI. Для этого Защита от файловых угроз извлекает файлы из пакета во временную папку или в память |
| **Выключено (по умолчанию)** | Защита от файловых угроз не проверяет самораспаковывающиеся архивы и установочные пакеты |

Установочные пакеты — это исполняемые файлы. И Защита от файловых угроз в любом случае проверяет их исполняемую часть. Но большая часть информации внутри установочного пакета — это заархивированные файлы программы, которую устанавливает пакет. Чтобы проверить их, Защита от файловых угроз извлекает их из пакета, и это ничем не отличается от проверки архивов.

Установочные пакеты Защитой от файловых угроз проверять не нужно. Если пользователь копирует пакет, он не может заразить компьютер. Если пользователь запускает пакет, пакет сам извлекает из себя файлы и сохраняет их на диск, где их и проверяет Защита от файловых угроз.

| Параметры программы \| Базовая защита \| Защита от файловых угроз \| Проверять файлы офисных форматов | |
|---|---|
| **Включено (по умолчанию)** | Защита от файловых угроз проверяет исполняемые куски не только в самих документах Microsoft Office, но и в объектах, вложенных в документы Microsoft Office |
| **Выключено** | Защита от файловых угроз проверяет исполняемые куски только непосредственно в документах Microsoft Office, но не во вложенных в них объектах |

У файлов Microsoft Office сложная структура. Можно сказать, что внутри у документа Microsoft Office своя собственная файловая система с дополнительными файлами. Когда пользователь вставляет в документ Word график, который он подготовил в Excel, Microsoft Office может добавить в документ Word весь документ Excel, со всеми данными, формулами и макросами.

Не отключайте проверку документов офисных форматов. Не проверять объекты, вложенные в офисные документы опасно. В них могут быть вредоносные макросы, которые программы Office запускают, не сохраняя предварительно на диск.

### Параметры проверки архивов

Если администратор включил проверять архивы, и пользователь попробует скопировать или открыть архив, операция не начнется, пока Защита от файловых угроз не распакует архив и не проверит в нем все файлы. Все это время пользователь ничего не сможет делать с архивом.

Если администратор хочет проверять архивы, он может сделать жизнь пользователей легче, изменив дополнительные параметры проверки архивов.

| | |
|---|---|
| **Не распаковывать составные файлы большого размера** | Защита от файловых угроз будет проверять только архивы, которые меньше чем *Максимальный размер файла* |
| **Максимальный размер файла** | По умолчанию равен 8 МБ. |
| **Распаковывать составные файлы в фоновом режиме** | Защита от файловых угроз будет задерживать только операции с небольшими архивами. Если пользователь обращается к большому архиву, Защита от файловых угроз разрешит доступ, но параллельно начнет распаковывать файлы архива и проверять их. И пользователю не придется ждать. Большие архивы — это те, которые больше, чем *Минимальный размер файла* |
| **Минимальный размер файла** | По умолчанию не задан. Т.е. если включить распаковывать составные файлы в фоновом режиме, Защита от файловых угроз будет проверять в фоновом режиме все архивы |

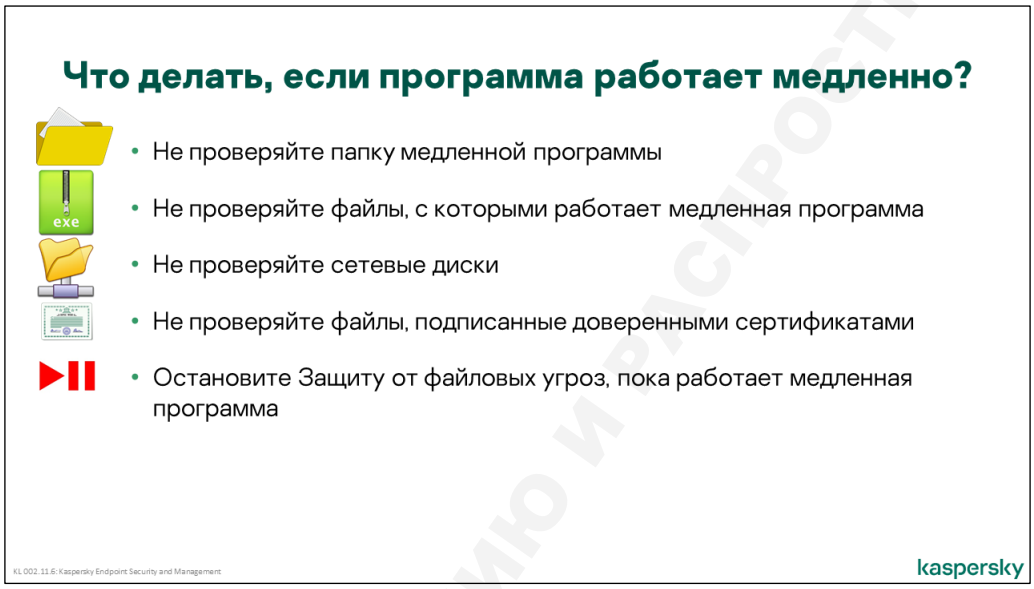
## Защита от файловых угроз удаляет вредоносные программы

Вредоносные программы, обнаруженные Защитой от файловых угроз, нельзя оставлять необработанными. Поэтому настройки действий Защиты от файловых угроз должны быть обязательными. Оптимальным выбором будет пытаться лечить, а если лечение невозможно, удалять зараженные файлы. Большинство вредоносных файлов неизлечимы, потому что не содержат ничего кроме вредоносного кода.

Перед лечением или удалением файла его копия помещается в резервное хранилище. Это делается на случай, если файл понадобится восстановить. Например, если в нем была критично важная информация, или если файл был удален в результате ложного срабатывания.

Если включен компонент Откат вредоносных действий (из Расширенной защиты), для объектов, которые в результате проверки удаляются, будет выполнен откат действий[1].

## 2.3 Что делать если Защита от файловых угроз замедляет компьютер




Во-первых, выясните, действительно ли Защита от файловых угроз замедляет компьютер (или программу):

- Найдите компьютер, который работает медленно
- Отключите на нем политику (см. раздел Как защитить Kaspersky Endpoint Security от пользователя)
- Остановите (выключите) Защиту от файловых угроз
- Проверьте, стал ли компьютер (программа) работать быстрее

Даже если без Защиты от файловых угроз программы на компьютере работают быстрее, не выключайте Защиту от файловых угроз. Настройте исключения для программ. Попробуйте разные виды исключений:

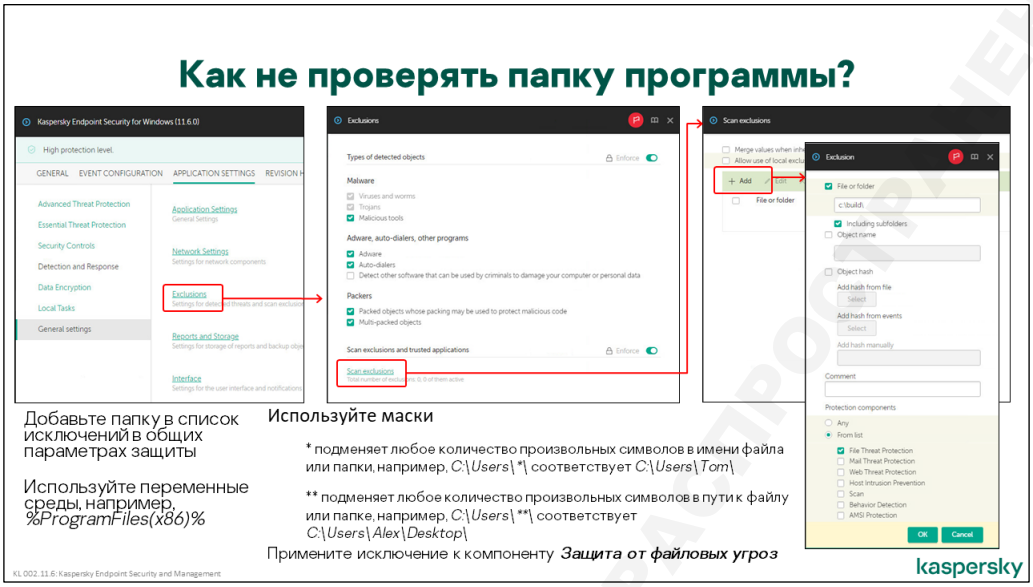
- Если все файлы программы в одной папке, исключите из проверки папку программы
- Если программа работает с файлами в разных папках или во временной папке, сделайте исполняемый файл программы доверенным

  Не исключайте из проверки временную папку операционной системы. Вредоносные программы часто запускаются именно из нее

- Если программа работает с файлами в сетевых папках, попробуйте отключить проверку сетевых дисков
- Для программ, которые работают по расписанию в нерабочее время, приостанавливайте Защиту от файловых угроз на время работы программы

[1] О процедуре отката действий рассказывается в 4 главе этой части

# Как исключить папку программы




Исключения настраиваются в политике Kaspersky Endpoint Security: откройте раздел **Параметры программы | Общие настройки** и нажмите ссылку *Исключения*.

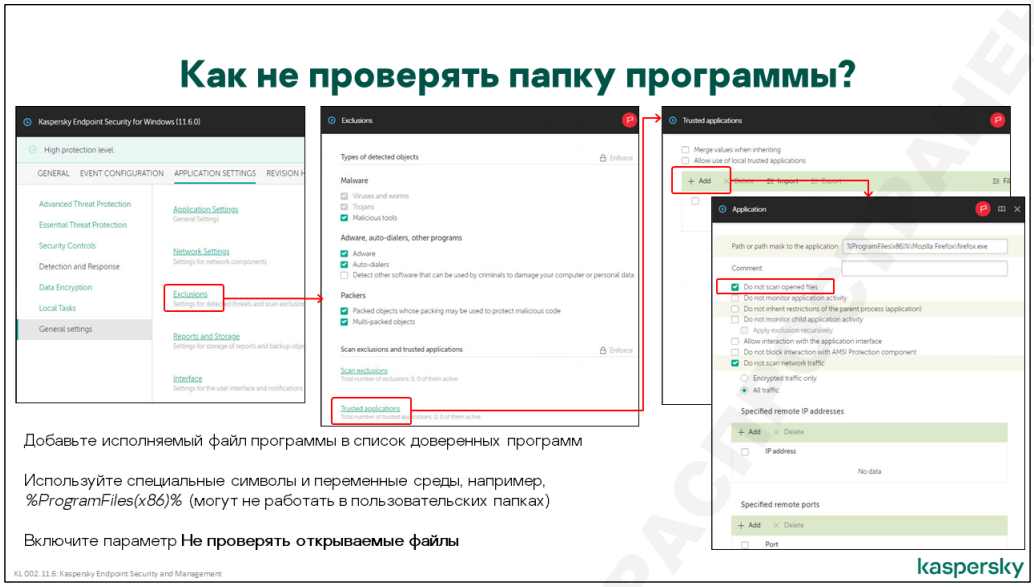
Исключения для папок доступны по ссылке *Исключения из проверки* и применяются ко всем компонентам защиты. Исключения из проверки состоят из трех атрибутов:

- **Файл или папка** — имя файла или каталога, на который распространяется исключение. В имени объекта можно использовать переменные окружения (*%systemroot%*, *%userprofile%* и другие) и спецсимволы «*» и «?»
- **Название объекта** — имя игнорируемой угрозы (как правило, имя вредоносной программы), которое тоже можно задать с использованием спецсимволов
- **Хеш объекта** — контрольная сумма файла (SHA-256), на который распространяется исключение.
- **Компоненты защиты**— перечень компонентов защиты, на которые распространяется правило

Из четырех атрибутов, обязательными являются любой из первых трех и четвертый. Можно создать полноценное правило исключения для отдельного файла или каталога, не указывая тип угроз — выбранные компоненты будут игнорировать любые угрозы в указанных объектах. И наоборот, можно создать правило исключения для некоторого типа угроз, например, для средства удаленного управления UltraVNC, так что выбранные компоненты не будут реагировать на эту угрозу независимо от того, где она обнаружена.

Нередко используются три атрибута. Так, в списке исключений сразу имеется набор правил для распространенных средств удаленного управления: UltraVNC, RAdmin и пр. В них задан и тип угроз, и объект — расположение исполняемого файла при типичной установке средства управления. Такое правило не будет реагировать на средства управления, запускаемые из **Program Files**, но если пользователь запустит UltraVNC из своего домашнего каталога, Kaspersky Endpoint Security воспримет это как угрозу.

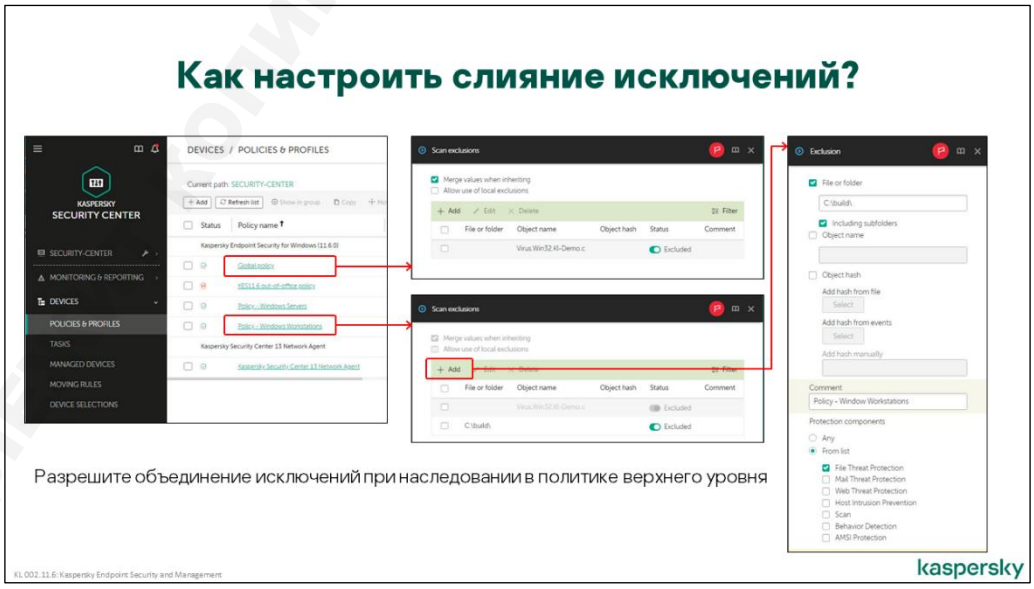
# Как исключить файлы, к которым обращается процесс




Если на компьютере запускаются особенно ресурсоемкие приложения, их работа может замедляться Защитой от файловых угроз. Особенно это касается программ, выполняющих много операций с файлами, например, резервного копирования или дефрагментации. Чтобы избежать замедления во время работы таких приложений, сделайте их доверенными.

Для этого в окне настройки исключений добавьте исполняемый файл в список **Доверенные программы**. В окне **Программа** укажите путь к исполняемому файлу, и выберите тип разрешенных действий **— Не проверять открываемые файлы**. Путь может содержать переменные среды и символов “*” и “?”

# Как объединить исключения политик



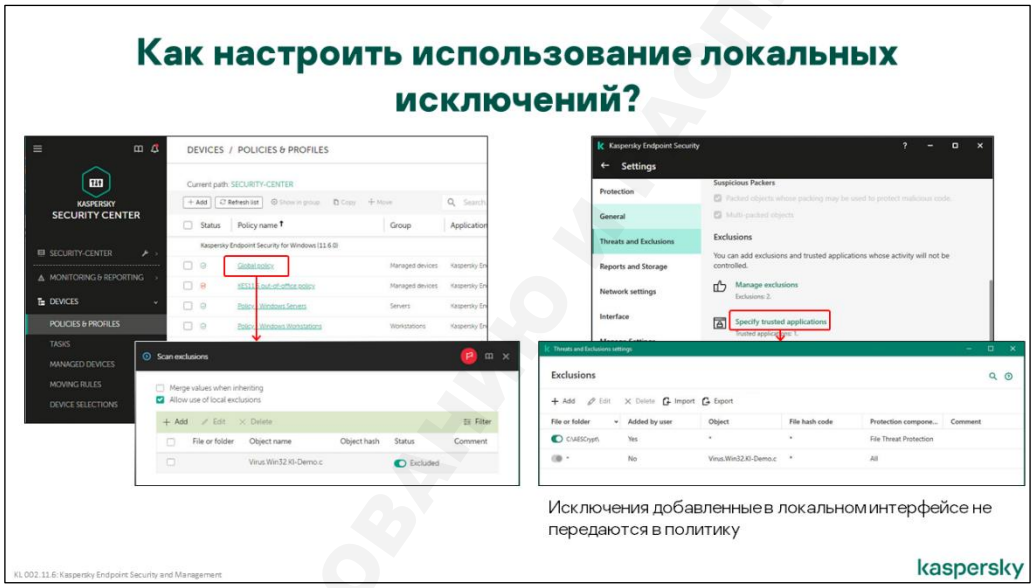

Список исключений из проверки и список доверенных программ можно объединять при наследовании в нижестоящей политике или профиле политик. Для этого в политике верхнего

уровня – родительской политике – в окне настройки исключения из проверки включите параметр **Объединять значения при наследовании**. При этом параметр **Наследовать параметры родительской политики** должен быть включен в нижестоящей политике.

В результате в нижестоящей политике или профиле политик появится возможность дополнить исключения, унаследованные из вышестоящей политики другими исключениями. Это позволит гибко настроить исключения для определенной группы или набора устройств.

Унаследованные исключения нельзя удалить или изменить в нижестоящей политике, их можно только дополнить новыми исключениями. Если отключить параметр **Объединять значения при наследовании** в родительской политике, то унаследованные исключения не будут автоматически удалены из нижестоящей политики, но станут доступными для удаления и редактирования.

## Как использовать локальные исключения

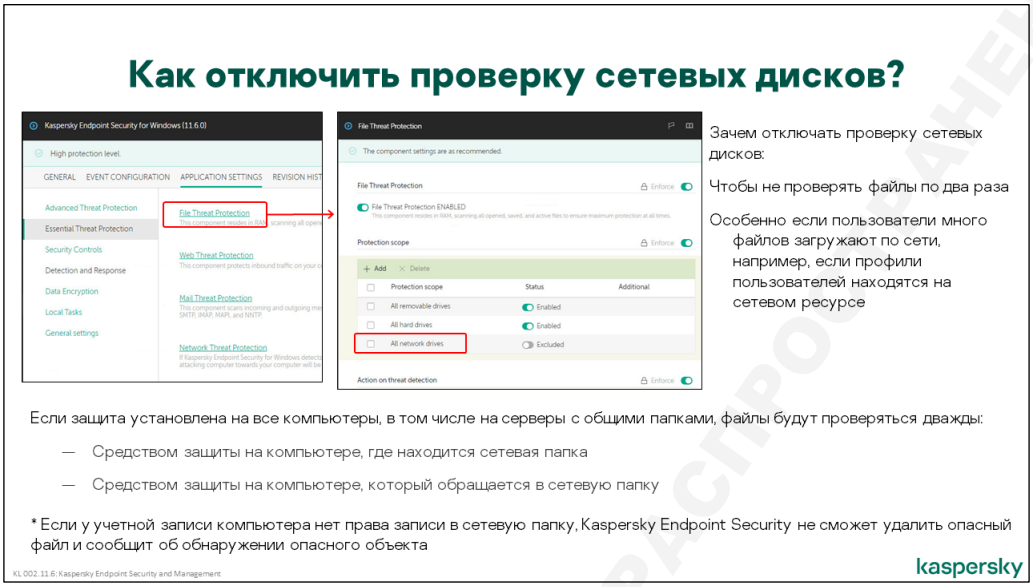



В ряде случаев исключения для доверенных программ гораздо легче и быстрее настроить по месту, т.е. в локальном интерфейсе Kaspersky Endpoint Security. Для этого в политике в окне настройки исключения из проверки включите параметр **Разрешить использование локальных доверенных программ**.

Основным недостатком этого способа настройки исключений является то, что исключения, добавленные с помощью локального интерфейса, не передаются в политику, и соответственно работают только на том компьютере, на котором они были сделаны.

Локальные исключения можно экспортировать в файл, а затем импортировать их в политику. Механизм импорта исключений в политику пока доступен только в mmc-консоли администрирования.

# Как не проверять сетевые диски




Не проверять сетевые диски опасно. Перед тем, как выключить проверку сетевых дисков, будьте уверены, что на всех компьютерах сети установлены средства защиты. Не отключайте проверку сетевых дисков «на всякий случай», а только если это решает проблему пользователей

Чтобы не проверять сетевые диски, измените область защиты в настройках защиты от файловых угроз.

**Область защиты** в Защите от файловых угроз по умолчанию включает:

— Все съемные диски
— Все жесткие диски
— Все сетевые диски

Иными словами — любые диски, с которых может быть произведен запуск вредоносных объектов. Область защиты допускает добавление отдельных дисков или каталогов, вместо групп дисков. Однако отключение любой из стандартных областей проверки существенно понижает уровень защиты.

# Как применить настройки к компьютерам

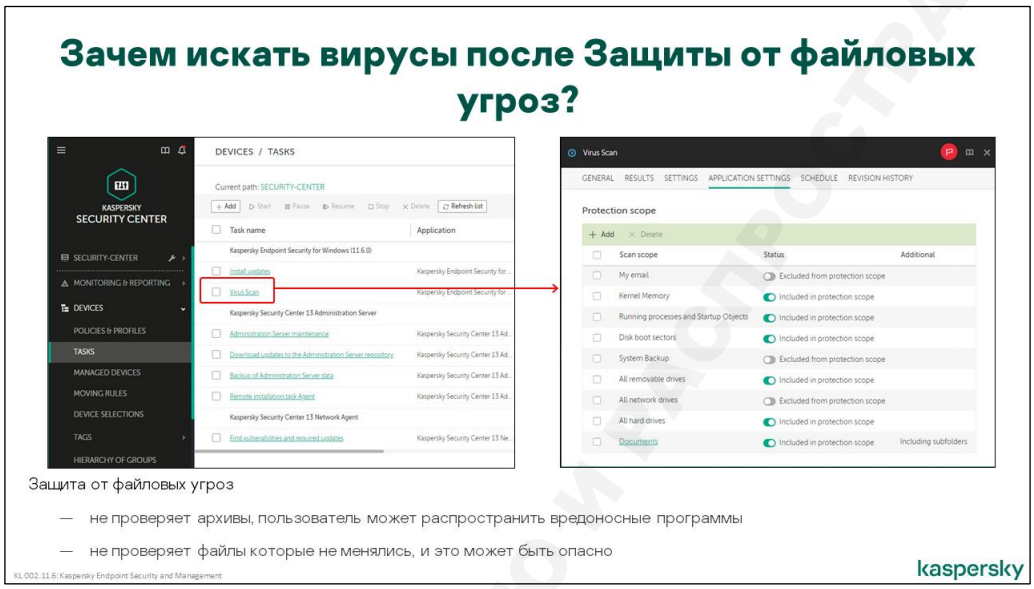
Настройки политики должны быть обязательными, т.е. с закрытым замком. Настройки с незакрытым замком не применяются к компьютерам.

Из-за того, что в политике по умолчанию все замки закрыты, администратор может вообще не обращать на них внимания. Пока он меняет настройки и не трогает замки, все настройки остаются обязательными и применяются к компьютерам.

Но все равно помните, что без закрытых замков настройки не применяются. Если вы изменили настройки в политике, а на компьютерах они не изменились, проверьте замки в политике.

# 2.4 Как и зачем проверять файлы по расписанию

## Зачем искать вредоносные программы после Защиты от файловых угроз




Чем помогает поиск вирусов, если Защита от файловых угроз все равно проверяет все опасные файлы? Поиск вирусов:

- Не дает пользователям распространять вредоносные программы в архивах
- Обновляет кэши KSN, обновляет данные о контрольных суммах файлов, после чего Защита от файловых угроз может проверять меньше файлов
- Проверяет файлы, которые не менялись. Защита от файловых угроз не проверяет такие файлы и иногда это может быть опасно

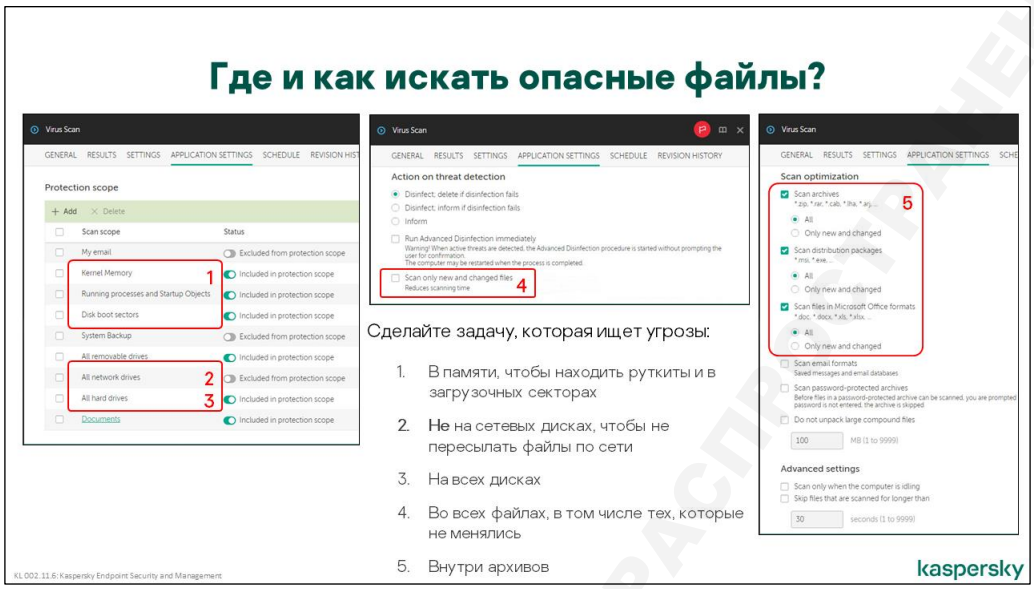
Задачи поиска вирусов выполняют проверку теми же способами, что и Защита от файловых угроз — используя сигнатурный и эвристический анализ, а также KSN. Разница в том, что Защита от файловых угроз проверяет файлы на лету, когда к ним происходит обращение, а задачи поиска вирусов проверяют файлы по расписанию или по запросу.

Защита от файловых угроз работает тогда же, когда и пользователь. Причем, чем активнее работают пользовательские приложения, тем больше файлов проверяет Защита от файловых угроз, тратя больше ресурсов. Из-за этого настройки Защиты от файловых угроз оптимизированы так, чтобы защищать только от немедленных угроз. Если пользователь копирует архив, немедленной угрозы заражения нет, и архив можно не проверять.

Задачи поиска вирусов можно запускать в нерабочее время. В таком случае нет необходимости слишком уж экономить ресурсы и можно выполнять проверку более тщательно. Поэтому, задача поиска будет ожидать ответа из KSN для вынесения окончательного вердикта, независимо от результатов проверки с помощью сигнатур и эвристики. Кроме того, поиском вирусов можно проверить объекты, исключенные из проверки в Защите от файловых угроз — архивы, инсталляционные пакеты, прочие файлы незаражаемых форматов.

Задача поиска вирусов может проверять процессы, находящиеся в памяти и ее можно запланировать для выполнения после каждого результативного обновления баз.

# Где и как искать опасные файлы




Настройки поиска вредоносных файлов задавайте в задачах поиска вирусов. Администратору необходимо самостоятельно создать задачу поиска вирусов в группе **Управляемые устройства.**

Начиная с одиннадцатой версии Kaspersky Security Center, мастер первоначальной настройки сервера администрирования больше не создает задачу **Быстрого поиска вируса**. По умолчанию, поиск вирусов на компьютерах осуществляется специальной локальной задачей **Scan_IdleScan.**

Задача **Scan_IdleScan** требует меньше ресурсов, по сравнению с обычной задачей поиска вирусов. Выполняется при простое компьютера, не отображает уведомления пользователю и не сбрасывает статус *Давно не выполнялся поиск вирусов.* Параметры проверки и область проверки данной задачи изменить нельзя.

Если вы решили использовать собственную задачу поиска вирусов, рекомендуется отключить задачу **Scan_IdleScan.** Чтобы отключить задачу **Scan_IdleScan,** в свойствах политики Kaspersky Endpoint Security**,** перейдите в раздел **Параметры программы | Локальные задачи | Фоновая проверка** и снимите отметку с опции **Включить фоновую проверку.**

## Область проверки

Область проверки представляет собой список путей к папкам и файлам, которые проверяются во время работы задачи. При указании пути допускается использование переменных среды (например, *%systemroot%*), а также символов ***** и **?** в имени файла или папки. Для папок, можно дополнительно выбрать: проверять все содержимое, включая подпапки, или только файлы, расположенные непосредственно в каталоге. В случае если подпапки не проверяются, иконка объекта помечается небольшим красным значком "минус".

Помимо файлов или каталогов в качестве объекта проверки можно указать:

- **Моя почта** — файлы данных Outlook (**.pst** и **.ost**)
- **Память ядра** —область памяти ядра операционной системы
- **Запущенные программы и объекты автозапуска** — область памяти, занятая процессами, и исполняемые файлы программ, которые запускаются при старте системы. Дополнительно, если в свойствах задачи выбран этот объект, в ходе поиска будет выполняться проверка на наличие руткитов (скрытых объектов файловой системы)
- **Загрузочные секторы** — проверяются загрузочные секторы жестких и съемных дисков

- **Системное резервное хранилище** — проверка папок **System Volume Information**
- **Все съемные диски** — съемные диски, подключенные в данный момент к компьютеру
- **Все жесткие диски** — жесткие диски компьютера
- **Все сетевые диски** — все сетевые диски, подключенные к компьютеру

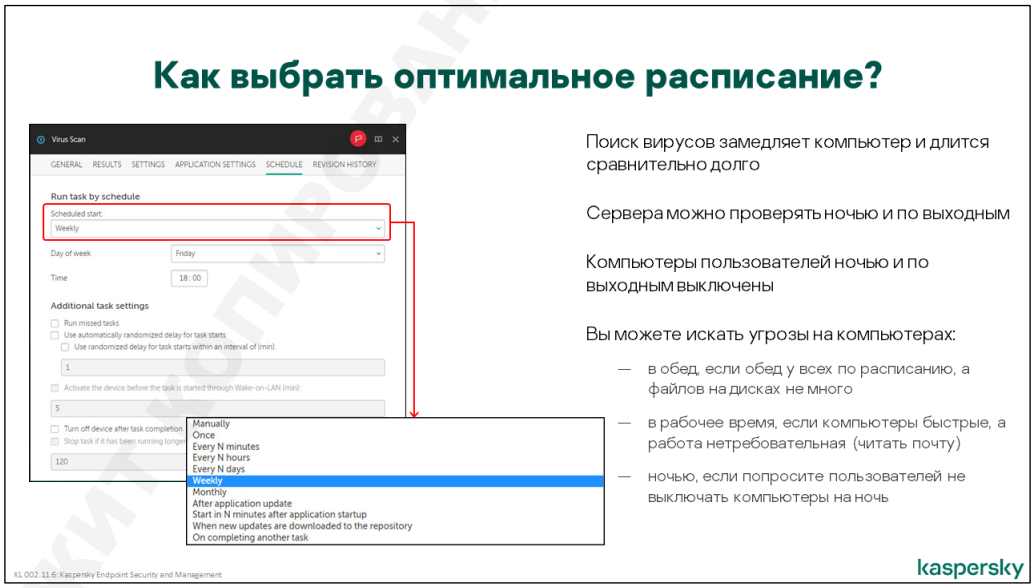
Сделайте задачу, которая проверяет весь компьютер раз в неделю или раз в две недели. Если для такой задачи нет времени, когда ее можно выполнить, проверяйте хотя бы критические области:

- Память ядра
- Запущенные процессы и объекты автозапуска
- Загрузочные секторы
- %systemroot%\
- %systemroot%\system\
- %systemroot%\system32\
- %systemroot%\system32\drivers\
- %systemroot%\syswow64\
- %systemroot%\syswow64\drivers\

### Учетная запись

По умолчанию задачи поиска запускаются на клиентских компьютерах с правами учетной записи локальной системы. В случае если в область проверки задачи входят сетевые диски или другие объекты, доступ к которым открыт не для всех пользователей, задача проверки не сможет их просканировать. Чтобы решить проблему, укажите в свойствах задачи учетную запись, обладающую необходимыми правами.

## Как выбрать оптимальное расписание




Задачи поиска вирусов могут иметь любое периодическое расписание: каждый N день, еженедельно, ежемесячно. Их можно запускать один раз в указанное время, или просто вручную.

Кроме этого, доступны специальные расписания:

- **После обновления программы** — т.е. после загрузки и применения новых сигнатур угроз. Такое расписание хорошо использовать для проверки памяти и других мест, где могут располагаться активные угрозы
- **Запуск через N (мин) после запуска программы** — т.е. сразу после включения Kaspersky Endpoint Security (или спустя несколько минут). Это тоже хороший момент для проверки наиболее уязвимых областей компьютера
- **По завершении другой задачи** — универсальное расписание, позволяющее организовать цепочку запусков. С практической точки зрения наиболее разумно увязывать поиск вирусов с завершением обновления, но для этого уже есть специальное расписание

Имеется возможность запускать пропущенные задачи. Если в запланированный момент поиска вирусов компьютер был выключен, задача запустится при его включении. Используйте эту опцию осторожно. Если поиск вирусов запустится утром, когда пользователь включил компьютер, проверка будет мешать пользователю.

Режим **Использовать автоматическое определение случайного интервала между запусками задачи** полезнее для задач обновления, чем для задач поиска вирусов. Читайте о нем в Части 4.

В области **Дополнительные свойства задачи** есть еще несколько полезных настроек:

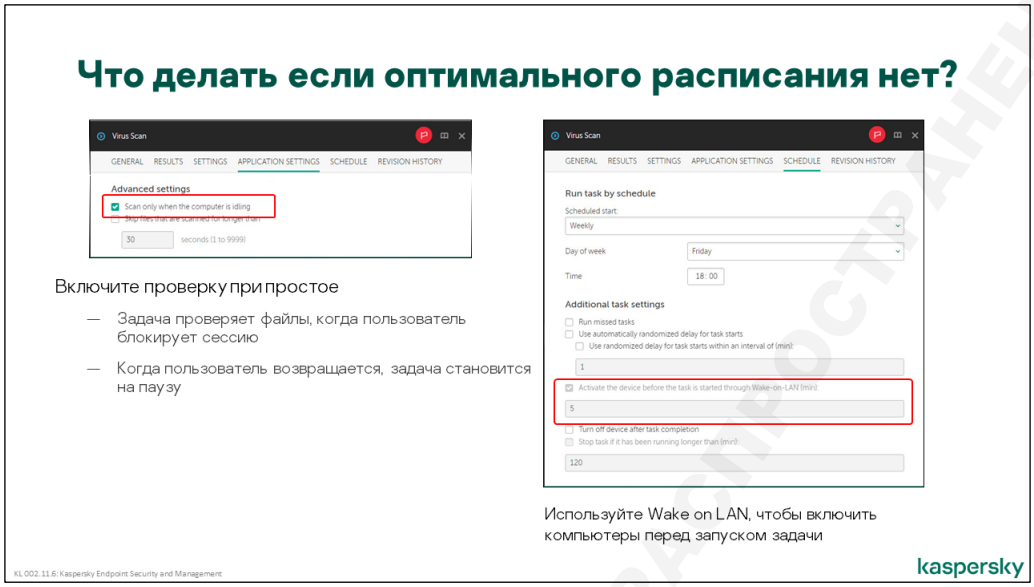
- **Активировать устройство перед запуском задачи функцией Wake On LAN за (мин.)** — позволяет планировать запуск проверки на ночное время или выходные дни, не беспокоясь о том, будет ли компьютер включен. Правда, для использования этой функции нужно, чтобы ее поддержка была включена в настройках BIOS компьютера
- **Выключать устройство после выполнения задачи** — может использоваться как продолжение предыдущей опции. Если проверка запланирована на ночное время или выходной, после ее завершения компьютер можно выключить
- **Остановить задачу, если она выполняется более чем** (**мин**.) — позволяет гарантированно завершить задачу до начала рабочего дня, чтобы выполняющаяся проверка не мешала работе пользователей

На серверах выполняйте поиск вирусов по выходным, когда они меньше загружены.

На рабочих станциях постарайтесь найти такое время запуска, когда компьютеры включены, но поиск вирусов не будет мешать пользователям:

- Быстрый поиск вирусов можно выполнять в обеденный перерыв
- Полную проверку выполняйте ночью. Объясните пользователям, в какой день недели нужно оставлять компьютеры включенными на ночь

## Что если оптимального расписания нет



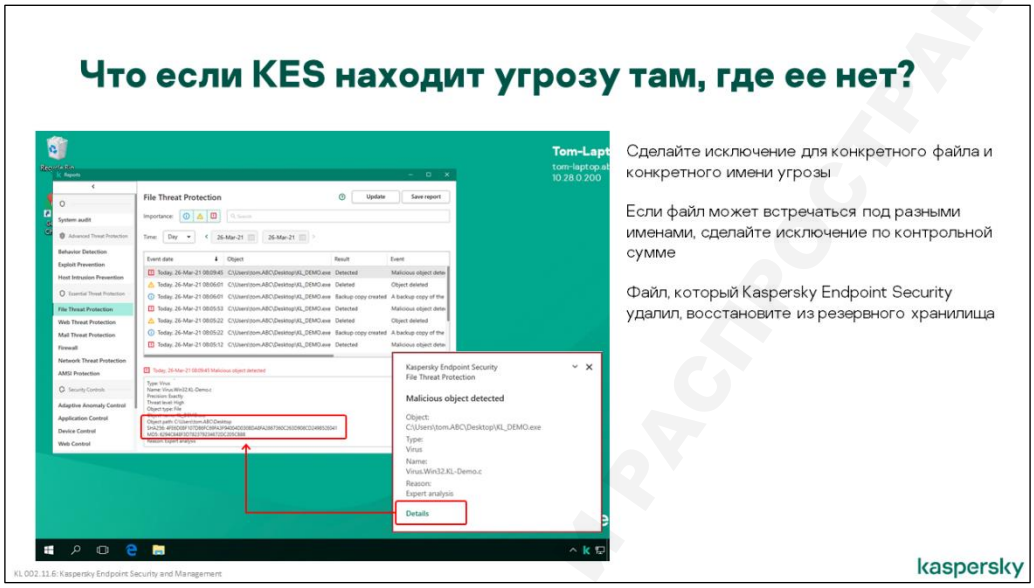

Если с пользователями договориться не получается, используйте Wake-On-LAN, чтобы включить компьютеры ночью и выполнить поиск вирусов. Если и этот вариант не работает, используйте так называемый *поиск при простое*.

Чтобы включить поиск при простое, откройте в задаче вкладку Параметры программы и включите опцию **Выполнять проверку во время простоя компьютера** (в области **Дополнительные параметры**). В таком режиме поиск вирусов будет выполняться, только если компьютер не используется (заблокирован или на нем работает экранная заставка), а в противном случае задача перейдет в состояние **Приостановлена**.

Полная проверка компьютера в режиме *при простое* может занять несколько дней или даже пару недель, но это лучше, чем не проверять компьютер вообще.

# 2.5 Что делать с ложными срабатываниями

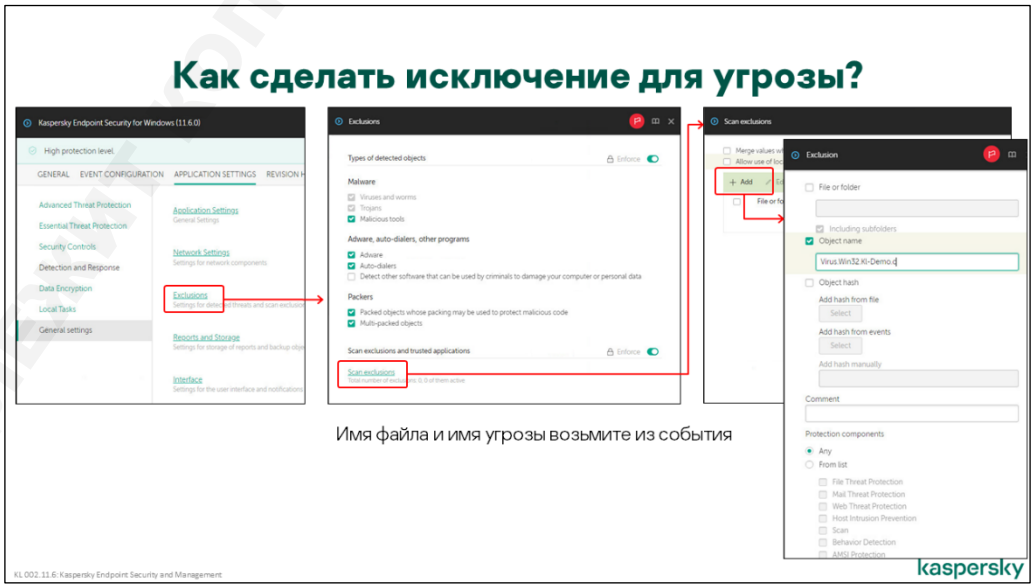
## Как настроить исключение для неправильного вердикта




Если Kaspersky Endpoint Security сообщает об угрозе в заведомо чистом файле, это ложное срабатывание.

Ложные срабатывания сильно мешают работе. Поэтому Лаборатория Касперского очень тщательно тестирует новые сигнатуры на огромной базе файлов операционных систем и популярных программ, чтобы не допустить ложных срабатываний. И уже во время проверки Kaspersky Endpoint Security сверяет файлы с Kaspersky Security Network и игнорирует угрозы в файлах, которые известны в KSN как доверенные.

Ложные срабатывания на файлах случаются крайне редко, и если случаются, как правило, это файлы мало распространенных программ: например, программ внутренней разработки.



Если Защита от файловых угроз или задачи поиска вирусов ошибочно находят угрозу в файле, создайте исключение для этого файла:

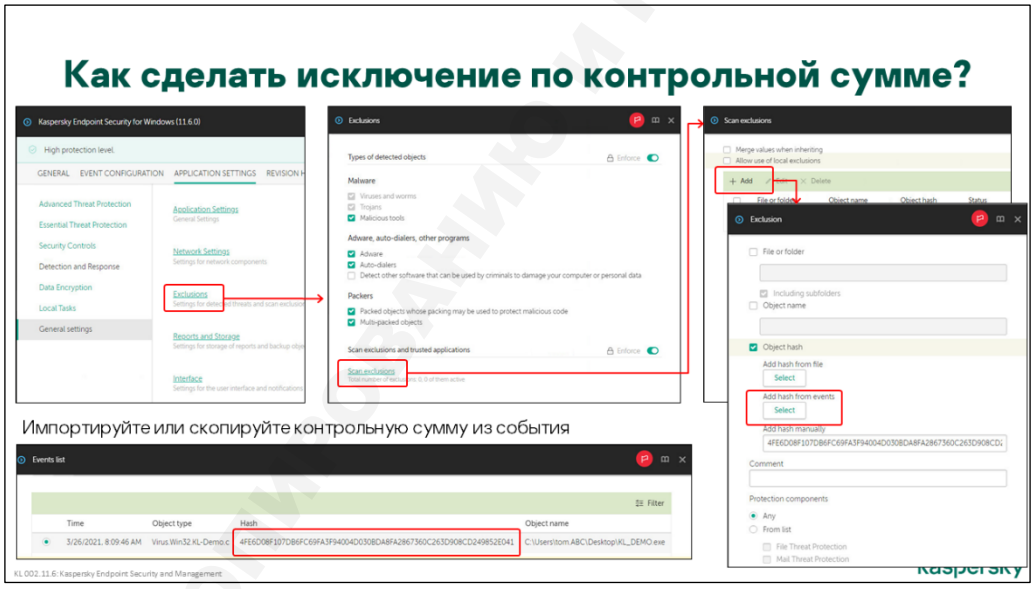
1. Откройте настройки доверенной зоны в политике Kaspersky Endpoint Security: **Параметры программы | Общие настройки | Исключения | Исключения из проверки**

2. Добавьте файл, на котором происходит ложное срабатывание в список **Исключения из проверки**. Отметьте флаг **Файл или папка**. Укажите полный путь к файлу в поле **Файл или папка** в нижней части окна. Используйте переменные среды, такие как *%ProgramFiles%*

> Безопаснее делать исключения не для файла вообще, а для конкретной угрозы, которую ошибочно находит Kaspersky Endpoint Security. Для этого:

3. Отметьте флаг **Название объекта** в окне исключения. Укажите имя угрозы в поле **Название объекта** в нижней части окна. Имя угрозы ищите в событии об угрозе от Kaspersky Endpoint Security в поле **Имя**

## Исключения по контрольной сумме




Что делать, если файл, для которого необходимо настроить исключения может находиться в разных местах на разных компьютерах?

Если версия файла одинакова на всех компьютерах, используйте контрольную сумму файла:

1. Откройте настройки доверенной зоны в политике Kaspersky Endpoint Security: **Общие настройки | Исключения | Исключения из проверки**

2. Добавьте файл, на котором происходит ложное срабатывание в список **Исключения из проверки**. Отметьте флаг **Хеш объекта**. Укажите контрольную сумму файла в поле **Хеш объекта** в нижней части окна. Контрольную сумму можно получить непосредственно из файла, добавить вручную или скопировать из события обнаружения.

> Kaspersky Endpoint Security определяет контрольные суммы проверяемых файлов и отображает эти данные в событиях обнаружения.

## Исключения по сертификатам

Что делать, если вы настроили исключение, но вышла новая версия программы с новым именем папки и исполняемого файла, и на нем тоже происходит ложное срабатывание?

Если имена файлов похожие, используйте маску пути. В маске символ «*» заменяет произвольное количество символов, а символ «?» заменяет один произвольный символ. Например, маска file*.exe соответствует всем файлам, которые начинаются на «file» и имеют расширение «.exe».

Если имена файлов совсем разные, но все файлы подписаны сертификатом, поместите сертификаты в хранилище сертификатов компьютеров, где используется программа и настройте Kaspersky Endpoint Security доверять этим сертификатам:

1. Откройте настройки доверенной зоны в политике Kaspersky Endpoint Security: **Параметры программы | Общие настройки | Исключения**

2. Включите параметр **Использовать доверенное системное хранилище сертификатов** и выберите одно из хранилищ. По умолчанию предлагается хранилище *Доверительные отношения в предприятии* (*Enterprise Trust*)

3. Поместите сертификат(ы), которыми подписаны файлы программы в выбранное хранилище на клиентских компьютерах. Для этого используйте, например, групповые политики Active Directory

На компьютере есть пользовательские хранилища сертификатов и хранилища сертификатов компьютера. Kaspersky Endpoint Security доверяет только сертификатам, которые находятся в хранилище компьютера

Для программ внутренней разработки можно использовать даже самоподписанные сертификаты.

# 2.6 Защита файлов: резюме


Защита от файловых угроз проверяет файлы на диске, к которым обращаются пользователи, программы и операционная система. Чтобы не замедлять компьютер, Защита от файловых угроз

проверяет только те файлы, которые представляют непосредственную угрозу. Но она не мешает пользователю копировать вредоносные файлы в архивах.

Задачи поиска вирусов проверяют все файлы и удаляют вредоносные файлы, которые пассивно лежат на компьютере. Например, вредоносные файлы в архивах.

Если удобного расписания для поиска вирусов нет, используйте поиск вирусов при простое компьютера.

Если Защита от файловых угроз замедляет компьютер или программы:

- Запланируйте поиск вирусов, поиск вирусов обновляет кэш проверки файлов и позволяет Защите от файловых угроз не проверять их еще раз, если они не менялись
- Настройте исключения для программ: для папок, исполняемых файлов или сертификатов
- Если медленно работает загрузка файлов по сети (например, профиля пользователя), и на сетевых серверах тоже есть средства защиты, не проверяйте сетевые диски
- В крайнем случае, приостанавливайте Защиту от файловых угроз на время работы ресурсоемких программ

Не выключайте Защиту от файловых угроз. Запланируйте поиск вирусов на компьютерах

# 3. Как настроить защиту от угроз по сети

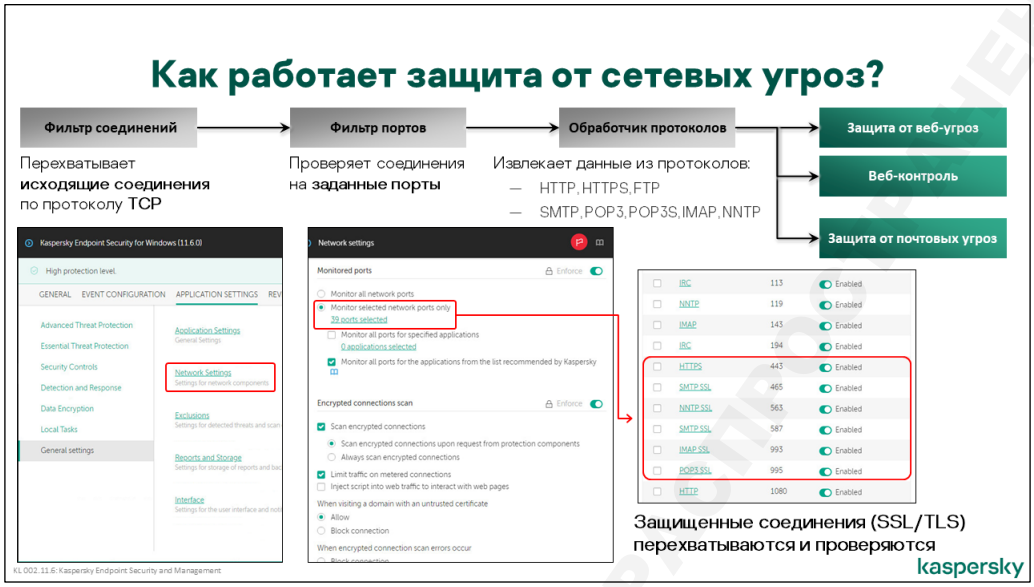
## 3.1 Как работает защита сети

### Что делают сетевые компоненты


Сеть — это один из основных путей распространения вредоносных программ. Поэтому защита сети и проверка сетевого трафика играет важную роль в обеспечении безопасности компьютера. В Kaspersky Endpoint Security за поиск вредоносных программ в сетевом трафике отвечают компоненты Защита от почтовых угроз и Защита от веб-угроз:

| | |
|---|---|
| **Защита от почтовых угроз** | Удаляет вредоносный код из почтовых сообщений и вложений<br>Переименовывает потенциально опасные вложения |
| **Защита от веб-угроз** | Не дает загружать вредоносные файлы<br>Не дает заходить на вредоносные и фишинговые сайты |

# Как Kaspersky Endpoint Security перехватывает трафик




Перехват сетевого трафика Kaspersky Endpoint Security осуществляет с помощью NDIS-фильтра. Драйвер перехватывает исходящие соединения от программ на компьютере и передает пакеты сетевым компонентам защиты. Kaspersky Endpoint Security определяет протокол соединения, и передает пакеты соответствующему компоненту:

| | |
|---|---|
| **HTTP, HTTPS, FTP** | Защита от веб-угроз, Веб-контроль |
| **SMTP, POP3, POP3S IMAP, NNTP** | Защита от почтовых угроз |

Остальные пакеты поступают сразу к программам и приложениям, для которых они предназначены.

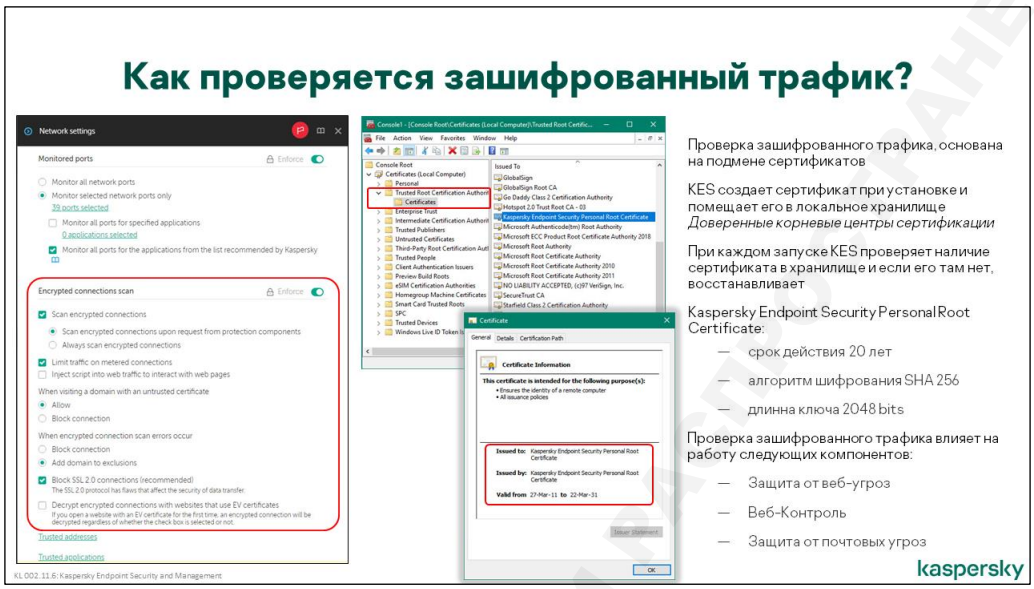
## Kaspersky Endpoint Security проверяет данные в защищенных соединениях (SSL/TLS)

Kaspersky Endpoint Security может перехватывать не все исходящие соединения, а только соединения на заданные порты. Для этого в политике Kaspersky Endpoint Security на вкладке **Параметры программы** выберите раздел **Общие настройки** | **Настройки сети** и в области **Контролируемые порты** выберите **Контролировать только выбранные сетевые порты**. Нажмите ссылку *Выбрано 39 портов* и укажите порты, которые нужно перехватывать.

Если вы не знаете, какие именно порты использует программа, включите опцию **Контролировать все порты для указанных программ**, и добавьте в список путь к исполняемому файлу программы.

Стандартные порты и программы уже указаны в списках контролируемых портов. Если используются нестандартные порты или программы, добавьте их в список.

# Как Kaspersky Endpoint Security проверяет зашифрованный трафик



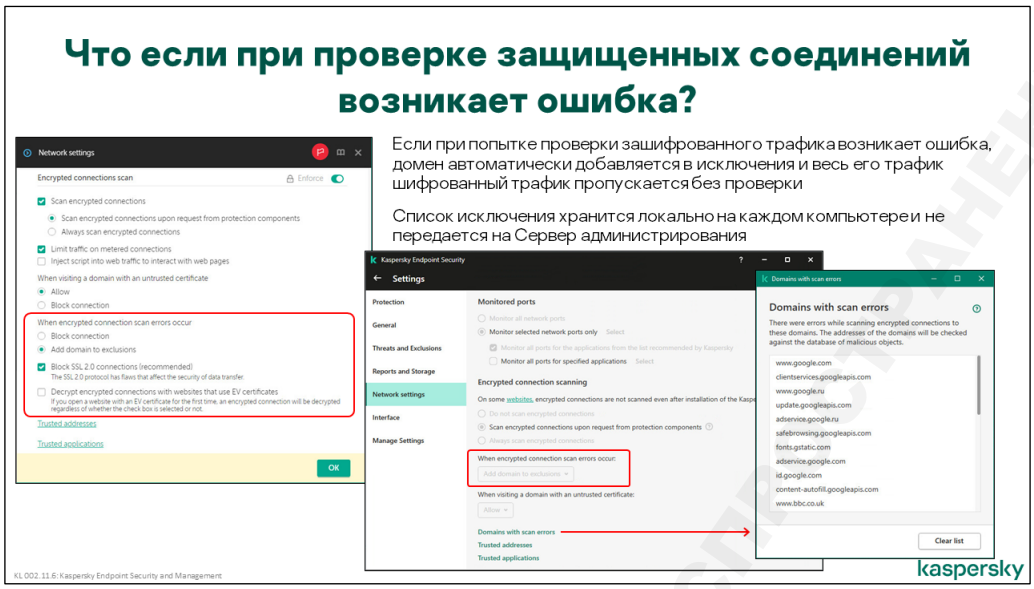

В процессе установки, Kaspersky Endpoint Security создает самоподписанный сертификат – Kaspersky Endpoint Security Personal Root Certificate и помещает его в локальное хранилище компьютера – Trusted Root Certification Authorities. При каждом запуске, KES проверяет наличие сертификата в хранилище, и если не его там нет, восстанавливает.

Проверка зашифрованного трафика (SSL/TLS) Kaspersky Endpoint Security осуществляется с помощью подмены сертификата. Kaspersky Endpoint Security перехватывает исходящее соединение от программы к серверу, получив сертификат сервера, KES генерирует аналогичный сеансовый сертификат, подписанный Kaspersky Endpoint Security Personal Root Certificate сертификатом, и отдает его клиентской программе. Это позволяет перехватить симметричный ключ шифрования и расшифровать весь сеанс связи.

Пользователь не получит никаких предупреждений от веб-браузера, поскольку Kaspersky Endpoint Security Personal Root Certificate находится в хранилище доверенных сертификатов.

Проверка зашифрованного трафика включена по умолчанию и влияет на работу следующих компонентов:

- Защита от веб-угроз
- Защита от почтовых угроз
- Веб-контроль



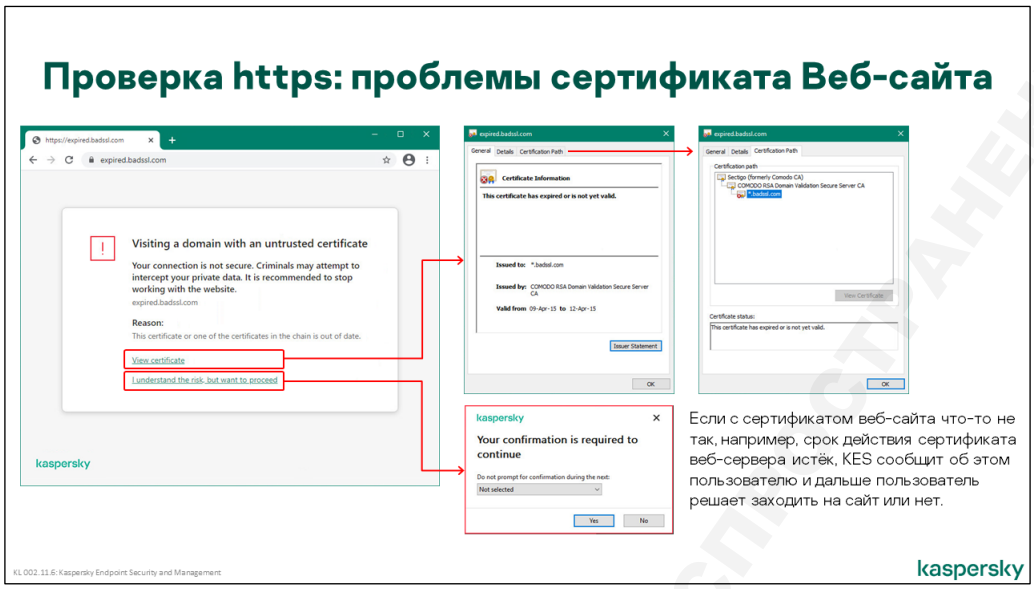

Протоколы SSL/TLS поддерживают три режима аутентификации: аутентификация двух сторон, аутентификация сервера перед анонимным клиентом и полная анонимность.

Например, когда пользователь подключается, по протоколу https к веб-серверу, в большинстве случаев используется второй с режим аутентификации – аутентификация сервера перед анонимным клиентом. В этом случае подмена сертификата не вызывает проблем.

Если используется первый режим аутентификации – двусторонняя аутентификация. Например, при работе клиент–банковских приложений, клиентов облачных хранилищ, перехваченный сертификат может быть не принят клиентской программой и у Kaspersky Endpoint Security возникнет ошибка проверки зашифрованного соединения.

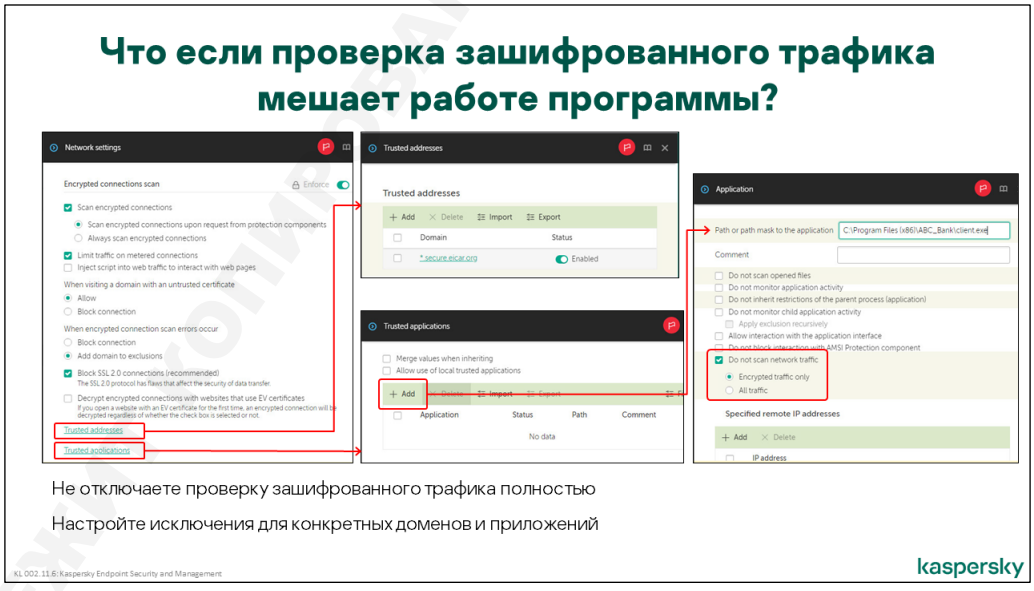
С настройками по умолчанию, если возникают ошибки при проверке защищенного соединения, домен автоматически добавляется в список *Домены с ошибками проверки* и весь его трафик пропускается без проверки. Список формируется для каждого компьютера отдельно, хранится локально и не передается на Kaspersky Security Center. Содержимое списка *Домены с ошибками проверки* можно посмотреть в локальном интерфейсе **Компоненты защиты | Настройки сети**, перейдя по одноименной ссылке.

При необходимости, можно сбросить локальные списки *Домены с ошибками проверки.* Для этого в политике Kaspersky Endpoint Security в разделе **Параметры программы | Общие настройки | Настройки сети** в области **В случае возникновения ошибки при проверке защищенных соединений** выбрать параметр **Блокировать соединение,** применить изменения, подождать пока политика распространится на компьютеры. Затем вернуть параметр **В случае возникновения ошибки при проверке защищенных соединений** в исходное значение – **Добавлять домен в исключения** и применить настройки политики. В результате, локальные списки *Домены с ошибками проверки* будут очищены.




Если у веб-сервера проблемы с сертификатом, например, время действия сертификата истекло, веб-браузер не сможет об этом сообщить пользователю, поскольку используется сеансовый сертификат KES, с которым все хорошо. О подключении к домену с недоверенным сертификатом сообщит KES и предоставит пользователю возможность самостоятельно решать подключаться к домену или нет.

При необходимости администратор может запретить подключение к доменам с недоверенным сертификатам. Для этого в области **При переходе на домен с недоверенным сертификатом** необходимо выбрать параметр **Блокировать.**




Большинство ресурсов в интернете используют защищенные соединения для передачи информации, поэтому не рекомендуется полностью отключать проверку защищенных соединений. Если проверка защищенных соединений мешает работе программ, настройте исключения.

Исключения настраиваются в политике Kaspersky Endpoint Security: откройте раздел **Параметры программы | Общие настройки | Настройки сети**. В области **Проверка защищенных соединений** доступны две ссылки для настройки исключений – **Доверенные адреса** и **Доверенные программы**.

Если проверка защищенных соединений мешает работе с веб-сайтом, добавьте адрес веб-сайта в список доверенных:

1. Перейдите по ссылке *Доверенные ареса*
2. Добавьте адрес веб-сайта в список. Чтобы задать маску, используйте спецсимволы «*» и «?»

Подмена сертификата для перечисленных в этом списке адресов сайтов осуществляться не будет.

Если все же у вас окажется программа, которая конфликтует с проверкой защищенных соединений, отключите для нее проверку зашифрованного трафика:

1. Перейдите по ссылке *Доверенные программы*

2. Добавьте исполняемый файл программы на вкладке **Программы**: укажите полный путь к файлу, используйте переменные среды, такие как %SystemRoot%

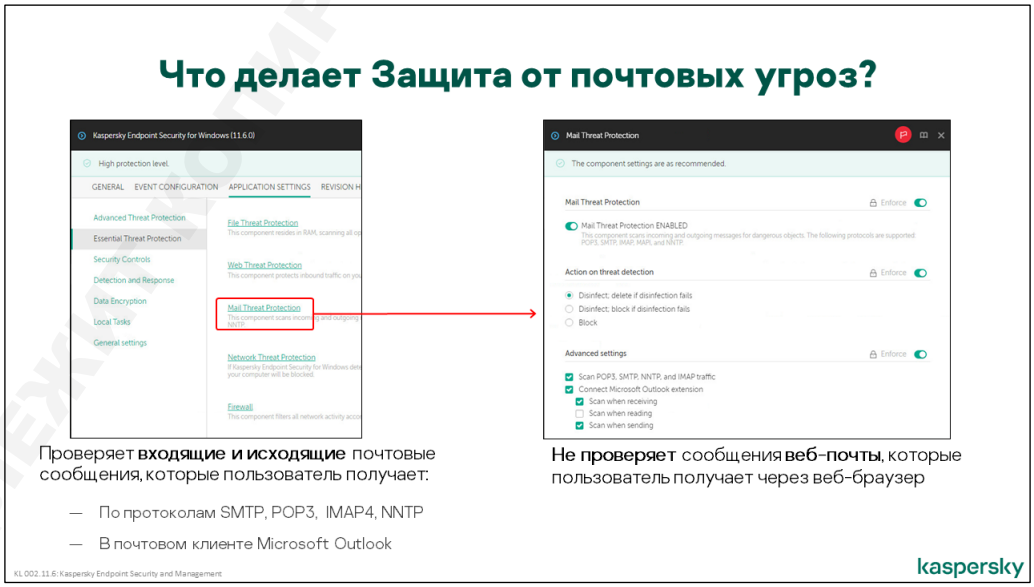
3. Отметьте флаг **Не проверять сетевой трафик**, выберите параметр **Только зашифрованный трафик** и снимите другие флаги

4. Если сервера, с которыми работает программа, имеют постоянные адреса (или фиксированный диапазон адресов) и порты, укажите их в нижней части окна: так безопаснее

Это исключение распространяется на компоненты Защита от почтовых угроз, Защита от веб-угроз и Веб-контроль

# 3.2 Защита от почтовых угроз

## Что делает Защита от почтовых угроз




Защита от почтовых угроз защищает от угроз, которые могут присутствовать в почтовых сообщениях. Перехват сообщений осуществляется на уровне протоколов (POP3, SMTP, IMAP и NNTP), а также путем встраивания в Microsoft Office Outlook (MAPI).

Защита от почтовых угроз обнаруживает и удаляет вредоносные программы, используя для этого сигнатуры вредоносных программ, эвристический анализ и Kaspersky Security Network. Кроме этого, в Защите от почтовых угроз есть возможность блокировать или переименовывать почтовые вложения, удовлетворяющие заданным маскам.

В зараженных сообщениях Защита от почтовых угроз меняет тему письма. В измененной теме указывается выполненное действие.

# Настройки Защиты от почтовых угроз

## Область защиты

Параметры безопасности определяют, кроме прочего, **Область защиты**. В терминах Защиты от почтовых угроз область защиты может принимать два значения:

— Входящие и исходящие сообщения
— Только входящие сообщения

Для защиты компьютера достаточно проверять только входящие сообщения. Проверка исходящих может предотвратить непреднамеренную отправку зараженного файла в архиве и избежать неприятной ситуации. Также проверку исходящих можно использовать для блокирования обмена вложениями определенных типов, например, музыки или видео.

По умолчанию, проверяются входящие и исходящие сообщения. Изменить область защиты можно только через MMC-консоль администрирования.

## Встраивание в систему

Группа параметров **Дополнительные настройки** уточняет область защиты:

— **Проверять трафик POP3/SMTP/NNTP/IMAP** — включает проверку сообщений электронной почты и электронных новостей, передаваемых по указанным протоколам
— **Подключить расширение для Microsoft Outlook** — включает проверку объектов[2] на уровне клиента Microsoft Office Outlook при получении, прочтении и отправке.
— Проверка на уровне протоколов работает независимо от используемых почтовых клиентов. Но сообщения, передаваемые по не перехватывающимся протоколам, как например, при работе с серверами Microsoft Exchange или Lotus Notes, проверяться не будут.
— Проверка на уровне почтового клиента, наоборот, работает независимо от того, каким образом получено сообщение. Правда, список поддерживаемых клиентов весьма ограничен.

## Способы проверки

Остальные настройки касаются проверки вложенных составных файлов.

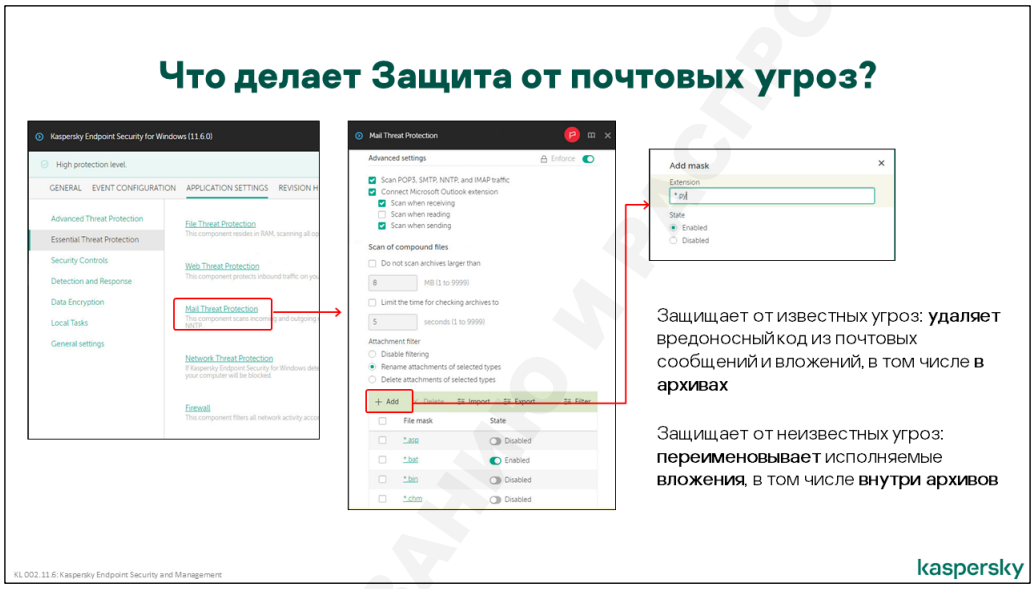
[2]Проверяются не только почтовые сообщения, но и объекты общих папок и календаря — любые объекты, получаемые через интерфейс MAPI из хранилищ Microsoft Exchange

Если вложенные файлы являются архивами, они могут быть распакованы и просканированы. Это поведение регулируется тремя настройками:

— **Проверять вложенные архивы** — позволяет полностью отключить проверку архивов. Как правило, лучше оставить этот параметр включенным, и проверять архивы на лету Защитой от почтовых угроз. Гораздо легче не допустить попадания инфицированного архива в почтовую базу, чем потом удалять его из базы задачей поиска вирусов.

— **Проверять вложенные файлы офисных форматов**

Отключить данные параметры можно только в MMC-консоли администрирования. Не выключайте эти параметры. Вредоносные файлы часто распространяются именно в виде вложенных архивов и офисных документов




— **Не проверять архивы размером более** *NN* **МБ** — ограничивает объем проверяемых архивов или файлов офисных форматов. Вредоносные программы исключительно редко распространяются в файлах большого размера. Включив это ограничение, можно избежать задержки при получении больших составных файлов.

— **Ограничить время проверки архива до** *NN* **с** — реализует защиту от «архивных бомб», проверка которых требует очень много времени и вычислительных ресурсов, затрудняя работу с компьютером

## Фильтр вложений

Остальные параметры касаются только вложенных файлов. Администратор может:

— **Не применять фильтр** — пропускает все невредоносные вложения

— **Переименовывать вложения указанных типов**[3] — используется по умолчанию и переименовывает вложения исполняемых типов (.exe, .bat, .cmd и т.п.). Это превентивная мера против неизвестных угроз. Пользователь не сможет запустить вложенный файл, не переименовав его сознательно.

Если включена проверка архивов, Защита от почтовых угроз будет переименовывать файлы с указанными расширениями внутри архивов.

[3]При переименовании последний символ расширения заменяется подчеркиванием

— Эту же опцию можно использовать в качестве меры противодействия эпидемии новой вредоносной программы. Если известны характерные имена вложений, используемые вредоносной программой, можно занести их в список и переименовывать так, чтобы пользователи не могли эти вложения открыть как обычные файлы. Переименование с большой вероятностью предотвращает заражение. В то же время при случайном совпадении полезного вложения с заданной маской, переименование не влечет серьезных последствий. Пользователь может обратиться к администратору и получить инструкцию, как переименовать файл обратно.

— **Удалять вложения указанных типов** — надежнее защищает от заражения, и кроме того может применяться для пресечения обмена файлами определенных типов: например, музыкальными или видеофайлами

Если включена проверка архивов, Защита от почтовых угроз будет удалять файлы указанных типов из вложенных архивов

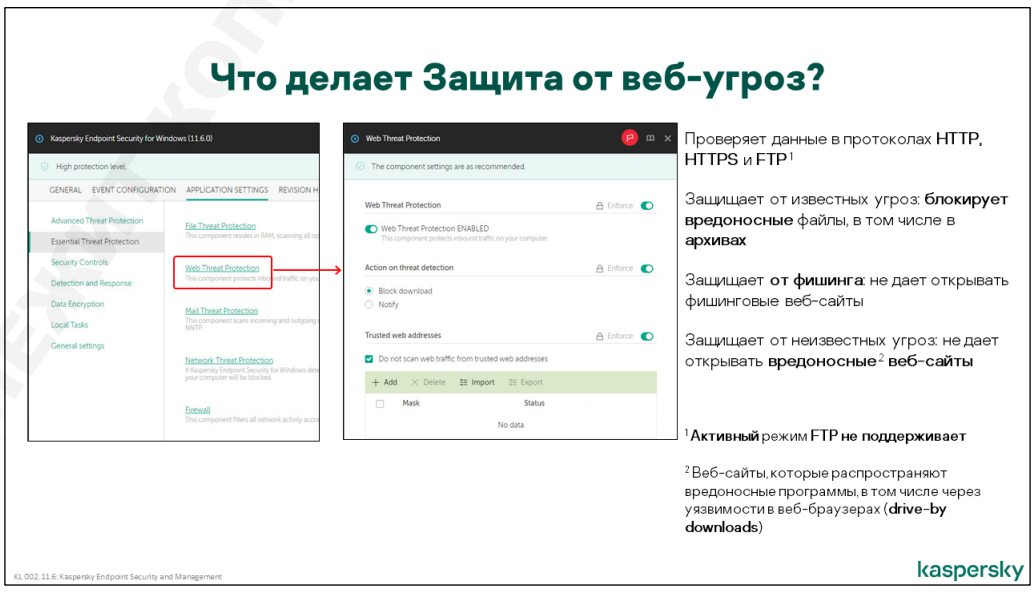
Исходно список фильтров содержит маски часто используемых расширений файлов. Пользовательские маски могут содержать не только расширение, но и часть имени. Для обобщения можно использовать спецсимволы «*» и «?». Добавляемые маски попадают в начало списка и сразу отмечаются как включенные.

## Исключения при ложных срабатываниях

Для Защиты от почтовых угроз правила исключений настраиваются так же, как и для Защиты от файловых угроз: в разделе настроек **Общие настройки** на вкладке **Параметры программы**, ссылка *Исключения* | *Исключения из проверки*. В качестве объекта **Файл или папка** можно указать имя или маску вложенного файла, на который должно распространяться исключение. Кроме того, аналогичное исключение нужно настроить для Защиты от файловых угроз, иначе сохранить или открыть полученный вложенный файл не получится.

# 3.3 Защита от веб-угроз

## Что делает Защита от веб-угроз



Защита от веб-угроз выполняет две важные функции:

- Блокирует доступ к фишинг-сайтам и потенциально опасным сайтам, анализируя адреса веб-страниц, которые открывает пользователь или программы
- Проверяет объекты, загружаемые по протоколам HTTP, HTTPS и FTP и блокирует вредоносные файлы

Для проверки ссылок используются четыре технологии:

- Проверка по базе вредоносных веб-адресов — простое сравнение адреса открываемого сайта с адресами веб-ресурсов, замеченных в размещении вредоносных программ, выполнении атак на компьютеры и прочей вредоносной деятельности
- Проверка по базе фишинговых веб-адресов — выполняется так же, как предыдущая проверка, только по базе сайтов замеченных в фишинге
- Эвристический анализ для обнаружения фишинговых ссылок — анализ содержимого сайтов на наличие HTML-кода характерного для фишинга
- Проверка в KSN — адреса открываемых сайтов проверяются в KSN. Опасные ссылки блокируются. Полученный ответ сохраняется в локальный кэш и используется при дальнейших проверках.

Для проверки файлов используются все доступные средства: сигнатурный анализ, эвристический анализ и KSN.

## Настройки Защиты от веб-угроз

### Действия

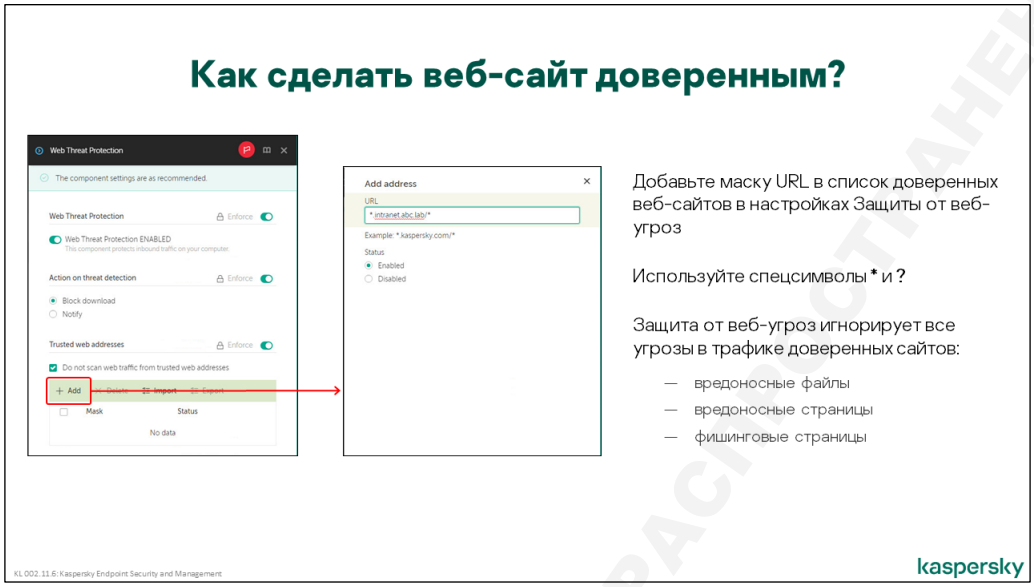
Ко всем обнаруженным опасным объектам применяется одинаковое действие, которое можно выбрать из двух доступных:

- Запрещать загрузку
- Информировать

В политике нужно устанавливать действие **Запрещать загрузку** и делать его обязательным, чтобы пользователи не имели возможности загружать опасные объекты или посещать опасные веб-сайты.

При попытке открыть запрещенный веб-ресурс или загрузить зараженный объект, в браузере будет показано уведомление о том, что загрузка заблокирована Kaspersky Endpoint Security.

# Как сделать веб-сайт доверенным



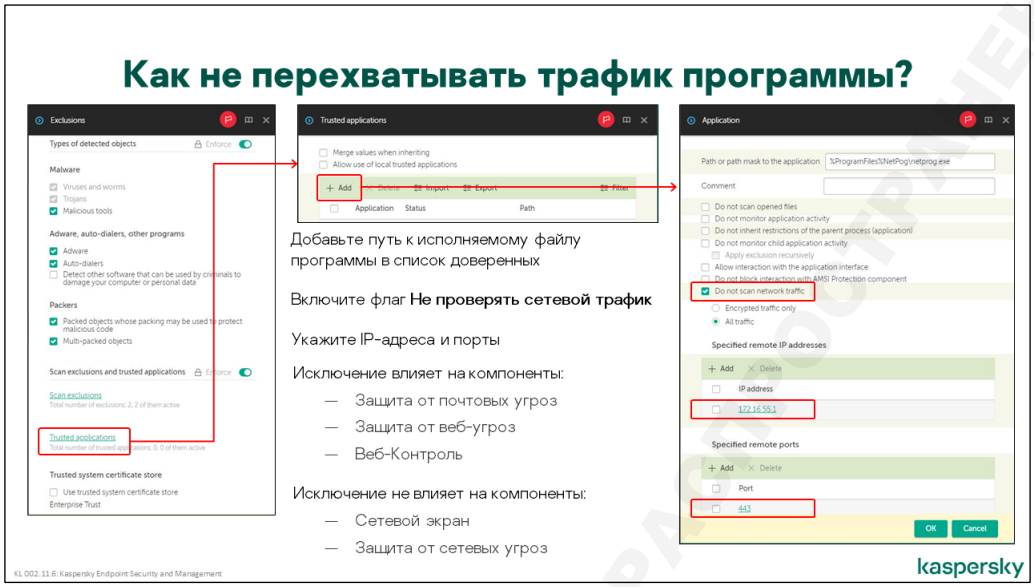

Если Защита от веб-угроз ошибочно считает веб-сайт вредоносным или фишинговым, добавьте адрес веб-сайта в список доверенных:

1. В разделе **Базовая защита** перейдите по ссылке *Защиты от веб-угроз*
2. Включите параметр **Не проверять веб-трафик с доверенных веб-адресов**
3. Добавьте адрес веб-сайта в список. Чтобы задать маску, используйте спецсимволы «*» и «?»

Адреса сайтов, перечисленные в этом списке, а также загружаемые с них объекты, не будут проверяться Защитой от веб-угроз.

Если Защита от веб-угроз ошибочно считает вредоносным файл, который пользователь загружает с веб-сайта, сделайте исключение для файлов в **Общих настройках** на вкладке **Параметры программы**. Примените исключение как минимум к Защите от веб-угроз, Защите от файловых угроз и к Поиску вирусов.

# 3.4 Как не перехватывать весь трафик программы




Начиная с версии 10SP2, Kaspersky Endpoint Security использует драйвер, который не разрывает соединение, а использует функции операционной системы, чтобы получить доступ ко всем пакетам.

Такой способ перехвата, как правило, не создает проблем в работе сетевых программ[4].

Если все же у вас окажется программа, которая конфликтует с новым методом перехвата, отключите для нее перехват трафика:

1. Откройте список доверенных процессов в политике Kaspersky Endpoint Security: откройте раздел **Общие настройки | Исключения** и перейдите по ссылке *Доверенные программы*

2. Добавьте исполняемый файл программы в список **Доверенные программы**: укажите полный путь к файлу, используйте переменные среды, такие как %SystemRoot%

3. Отметьте флаг **Не проверять сетевой трафик** и снимите другие флаги

4. Если сервера, с которыми работает программа, имеют постоянные адреса (или фиксированный диапазон адресов) и порты, укажите их в нижней части окна: так безопаснее

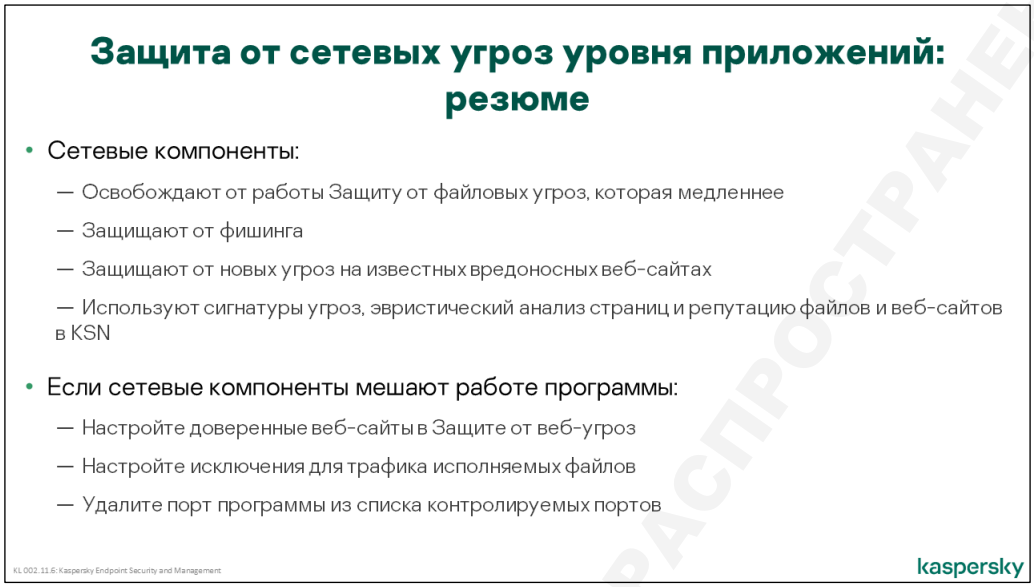
Это исключение распространяется на компоненты Защита от почтовых угроз, Защита от веб-угроз и Веб-контроль

[4] В старых версиях Kaspersky Endpoint Security (до 10 Service Pack 2) драйвер, который перехватывал соединения для компонентов защиты от сетевых угроз, работал как локальный прокси-сервер.

Когда программа устанавливала соединение с удаленным сервером, Kaspersky Endpoint Security подменял адрес сервера на свой адрес, чтобы получить пакеты программы, а потом уже устанавливал свое соединения с удаленным сервером, чтобы переслать проверенные пакеты. Ответные пакеты с сервера шли точно так же: сначала по соединению, которое установил Kaspersky Endpoint Security, затем от Kaspersky Endpoint Security к программе.

Некоторые сетевые программы были несовместимы с таким способом перехвата.

# 3.5 Защита сетевых соединений: резюме




Сетевые компоненты Защита от почтовых угроз и Защита от веб-угроз не потребляют много ресурсов. Наоборот, они позволяют Защите от файловых угроз проверять меньше файлов, и улучшают производительность компьютера.

Защита от веб-угроз — единственный компонент, который защищает от фишинга. Он же защищает от новых угроз, которые распространяются через известные вредоносные веб-сайты.

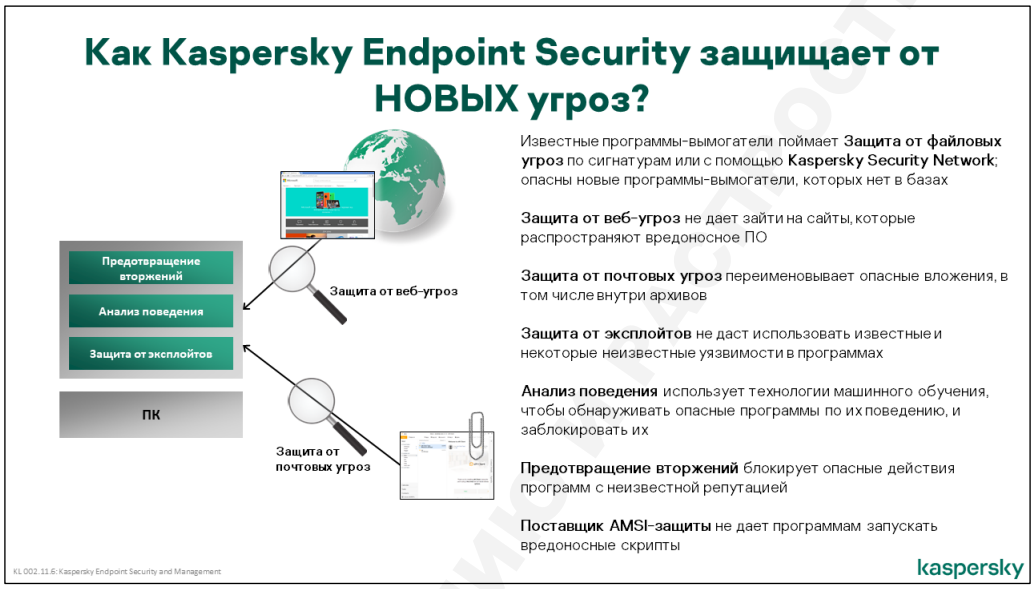
Не выключайте сетевые компоненты защиты, это не повлияет на производительность, но ухудшит защиту

Если Защита от веб-угроз или Защита от почтовых угроз ошибочно удаляют файлы, блокируют веб-сайты или мешают работе сетевых программ, настройте исключения:

— Исключения для веб-сайтов в настройках Защита от веб-угроз
— Исключения для программ в Общих параметрах | Исключениях
— Исключения для портов в Общих параметрах | Исключениях

# 4. Как настроить защиту от сложных угроз

## 4.1 Как Kaspersky Endpoint Security защищает от новых угроз




Злоумышленники постоянно создают новые вредоносные файлы. Лаборатория Касперского известна тем, что очень быстро обнаруживает новые угрозы и добавляет их сигнатуры в базу. Контрольные суммы вредоносных файлов попадают в Kaspersky Security Network еще быстрее. Но все равно злоумышленники на полшага впереди. Как Kaspersky Endpoint Security защищает от новых угроз и особенно от программ-вымогателей?

### Программы-вымогатели, которые шифруют документы и требуют деньги за пароль, наносят прямой и непосредственный ущерб

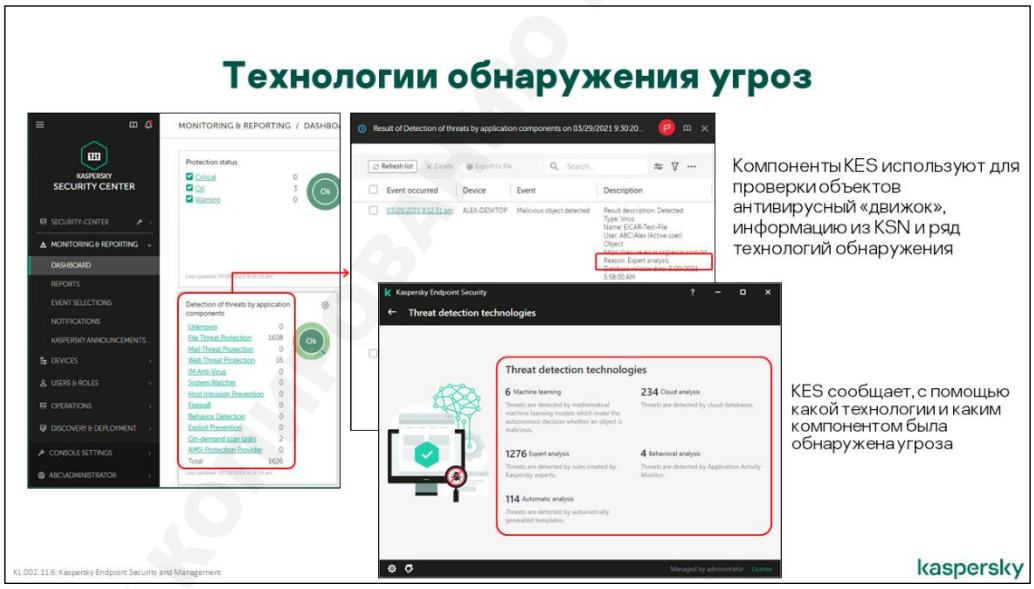
Kaspersky Endpoint Security пытается обнаруживать и блокировать вредоносные программы, в том числе и новые, на всех этапах атаки:

| | |
|---|---|
| **Злоумышленники публикуют вредоносные программы на зараженных и вредоносных веб-сайтах. Часто эти же веб-сайты они использовали и раньше** | *Защита от веб-угроз* использует базу известных вредоносных сайтов и репутацию веб-сайтов в KSN, и не дает пользователям на них заходить |
| **Злоумышленники рассылают новые вредоносные программы по почте** | *Защита от почтовых угроз* переименовывает исполняемые вложенные файлы, в том числе и в архивах |
| **Злоумышленники используют уязвимости в программах для запуска вредоносного кода** | *Защита от эксплойтов* не дает использовать известные и некоторые неизвестные уязвимости в программах |

| | |
|---|---|
| **Новые вредоносные программы отличаются кодом, чтобы обойти проверку по сигнатурам, но ведут себя похоже на другие вредоносные программы** | *Анализ поведения* следит за тем, что делают программы, и обнаруживает новые вредоносные программы по их поведению |
| **Зашифрованные данные статистически однородны, как будто их произвел генератор случайных чисел. Этим они отличаются от большинства файлов** | *Анализ поведения* использует эвристический и статистический анализ, технологии машинного обучения, чтобы обнаружить шифрование файлов |
| **Новые вредоносные программы не имеют никакой репутации в KSN** | *Предотвращение вторжений* не дает программам без репутации использовать многие функции операционной системы |

В основном новым угрозам противостоят Анализ поведения, Защита от эксплойтов и Предотвращение вторжений при поддержке Kaspersky Security Network.

## 4.2 Какие технологии обнаружения используются в Kaspersky Endpoint Security




Компоненты Kaspersky Endpoint Security можно разделить на три группы: компоненты, обеспечивающие статическую защиту, компоненты, обеспечивающие динамическую защиту и дополнительные компоненты.

Компоненты File / Web / Mail Threat Protection обеспечивают статическую защиту устройства – проверяют объекты перед их выполнением, блокируют запуск и загрузку опасных объектов.

Компоненты Behavior Detection, Exploit Prevention, Rollback обеспечивают динамическую защиту устройства – следят за действиями объектов в процессе их выполнения, анализируют, выявляют, блокируют опасное поведение.

К третьей группе относятся Host Intrusion Prevention, Firewall и Network Attack Blocker их задача уменьшить площадь атаки на защищаемом устройстве, ограничивая запуск и доступ к сети недоверенным программ. Облегчая, таким образом, задачу динамической и статической защите.

Компоненты Kaspersky Endpoint Security используют для проверки объектов антивирусный «движок», информацию из KSN и целый набор технологий. Ряд технологий обнаружения реализованы на стороне клиента, т.е. непосредственно в «движке» (сигнатурный анализ, эвристический анализ, поведенческий анализ). Ряд на стороне Лаборатории Касперского (экспертный анализ, машинное обучение, репутационный сервис). В KES они передают только результаты своей работы, в виде обновлений сигнатур, репутаций программ, шаблонов опасного поведения, моделей машинного обучения и т.д.

В событии обнаружения отображается название компонента и технология, с помощью которой была найдена угроза.

Технологии обнаружения в локальном интерфейсе Kaspersky Endpoint Security отображают источник получения информации об угрозе:

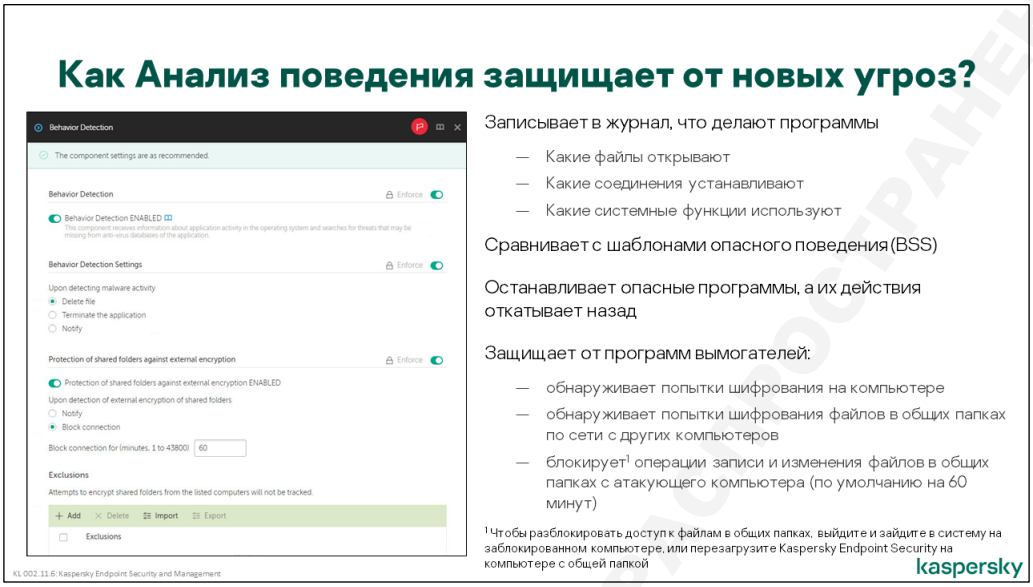
- **Автоматический анализ** – данные об угрозе были получены от системы автоматического анализа объектов. Процесс анализа объектов автоматизирован в «Лаборатории Касперского». Система автоматического анализа обрабатывает все объекты, поступающие в ЛК, выносит вердикты и формирует сигнатуры. Если система не может обработать объект, она передает его вирусным аналитикам
- **Экспертный анализ** – данные об угрозе были добавлены вирусными аналитиками «Лаборатория Касперского». Вирусные аналитики – эксперты, занимаются не только разработкой сигнатур угроз, они так же разрабатываю шаблоны опасного поведения, проектируют модели машинного обучения и т.д.
- **Поведенческий анализ** – данные об угрозе были получены на основе анализа поведения объекта
- **Облачный анализ** – данные об угрозе были получены от технологии Astraea, которая является частью KSN. Astraea – это система обработки больших данных, она получает данные от всех источников KSN-запросов, анализирует, ранжирует с точки зрения значимости и оценивает степень опасности
- **Машинное обучение** – данные об угрозе получены от модели машинного обучения. На стороне Лаборатории Касперского разрабатывается модель машинного обучения. Затем, модель обучается на большом массиве данных, используется данные полученные от KSN и системы Astraea. Обученная модель используется KES, параллельно с другими технологиями, для поиска угроз.
  Поскольку ландшафт угроз постоянно меняется, на стороне Лаборатории Касперского проходит регулярное улучшение и дообучение модели. Обновления к модели машинного обучения периодически поставляться в KES, таким же образом, как и сигнатуры угроз

## 4.3 Что делает Продвинутая защита

Компоненты и технологии, которые позволяют предотвращать или минимизировать последствия заражения новыми вредоносными программами, еще не внесенными в базы сигнатур, называют продвинутой защитой.

Из уже рассмотренных компонентов к продвинутой защите относится эвристический анализ файлов. Но главная роль в этом аспекте защиты принадлежит: Анализу поведения, Защите от эксплойтов, Откату вредоносных действий, Предотвращению вторжений и, в некоторой степени, компонентам контроля и сетевому экрану.

# Как Анализ поведения защищает от новых угрозы




Анализ поведения выполняет несколько функций:

— Ведет журнал активности программ для сравнения с базой поведенческих сигнатур
— Выявляет вредоносные программы и блокирует их действия
— Защищает папки общего доступа от внешнего шифрования

Главной задачей является именно выявление вредоносных программ. Для этого Анализ поведения ведет учет действий программ и сравнивает их с шаблонами опасного поведения. В журнал активности программ попадают обращения к файлам, установление сетевых соединений и вызов системных функций.

База шаблонов обновляема, но обновления для нее выходят сравнительно редко. Эффективность Анализа поведения практически не зависит от регулярности обновления баз.

## Настройки

Настройки Анализа поведения немногочисленны и, по сути, соответствуют включению или выключению самого компонента целиком или только Защиты папок общего доступа от внешнего шифрования.

## Действия

Если Анализ поведения обнаруживает вредоносное поведение, он прерывает программу, удаляет исполняемый файл и помещает его в Резервное хранилище.

Другие возможные действия:

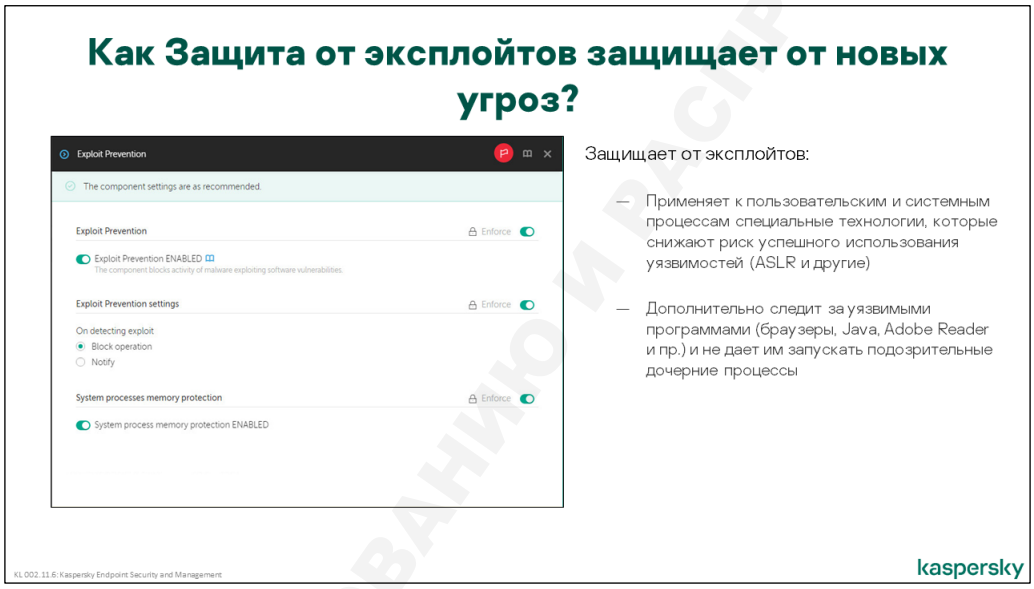
— **Информировать** — не выполнять никаких действий, только занести факт обнаружения вредоносной активности в отчет
— **Завершать работу программы** — завершить и выгрузить вредоносную программу из памяти
— **Удалять файл** — завершить программу, удалить вредоносный файл, а копию поместить в Резервное хранилище

Если Защита папок общего доступа от внешнего шифрования обнаруживает попытку шифрования файлов в общей папке по сети, она блокирует операции записи и удаления для этой сессии на 60 минут. Затем пытается восстановить незашифрованные версии файлов из копий с помощью компонента **Откат вредоносных действий**.

Не отключайте Анализ поведения. Он защищает от угроз, от которых другие компоненты не всегда защитят

Чтобы устранить ложные срабатывания или улучшить производительность, создавайте исключения.

## Как Защита от эксплойтов защищает от новых угроз

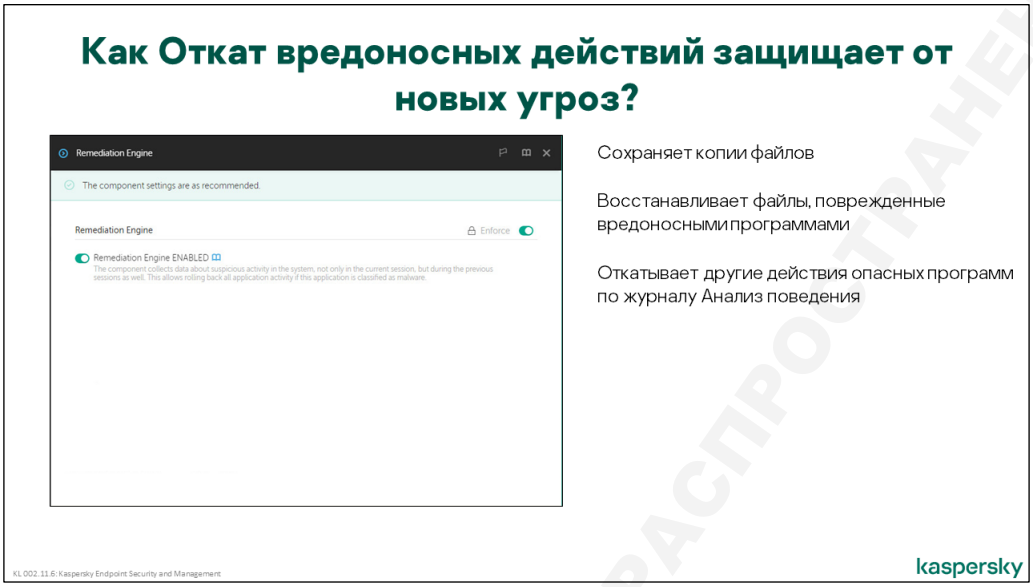



**Защита от эксплойтов** — защищает от широкого класса атак (эксплойтов), целью которых является получение прав администратора в системе или скрытое выполнение кода.

Эксплойты, как правило, используют атаку на переполнение буфера. В уязвимую программу или службу передаются некорректные параметры, обработка которых приводит к тому, что часть параметров уязвимая программа выполняет как код. В частности, с помощью таких атак на системные службы (которые выполняются с правами локальной системы) можно получить права администратора на компьютере.

Чаще всего с помощью такой атаки вредоносная программа пытается запустить саму себя с правами администратора. Включение данного параметра включает слежение за операциями запуска, и если уязвимая программа выполняет запуск другой программы не по инициативе пользователя, такой запуск блокируется.

# Как Откат вредоносных действий защищает от новых угроз



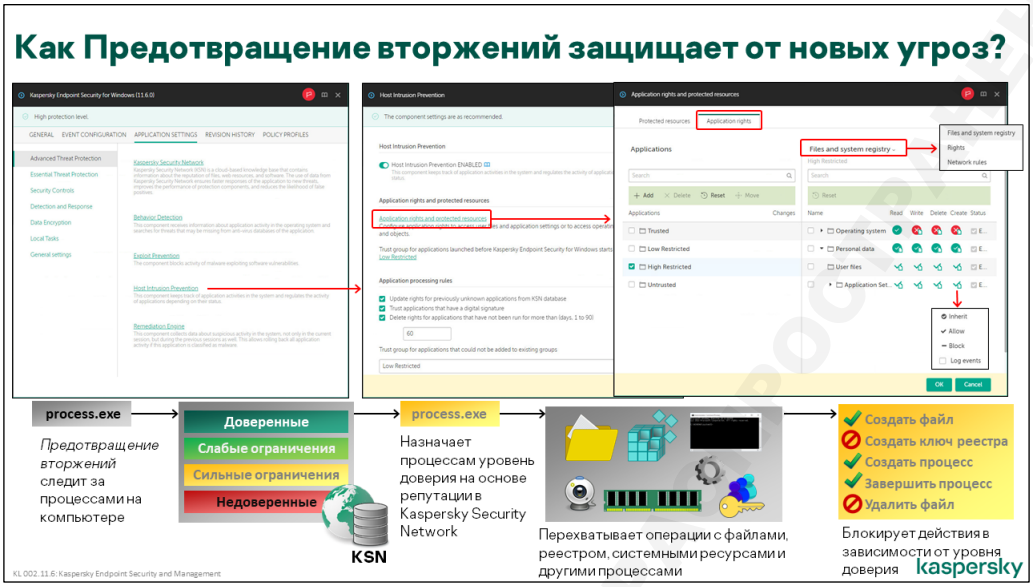

**Откат вредоносных действий** — выполняет откат действий приложений, которые удаляются Защитой от файловых угроз, задачами поиска и Анализом поведения.

Откатываются изменения файловой системы (создание, перемещение, переименование файлов) и ключей реестра (удаление созданных вредоносной программой записей). Кроме того, для небольшой группы файлов и ключей делается снимок состояния на момент старта системы, что позволяет откатываться к сохраненной версии, если вредоносная программа вносила изменения в эти файлы и ключи. К таким особым объектам относятся файлы hosts, boot.ini и ключи реестра, отвечающие за запуск программ и служб при старте системы.

Эта же опция восстанавливает файлы, зашифрованные программами-вымогателями, которые шифруют файлы на дисках и в общих папках, после чего требуют выкуп.

Для отката вредоносных действий используется журнал активности программ, который ведет компонент Анализ поведения.

# Как Предотвращение вторжений защищает от новых угроз




Основное назначение Предотвращения вторжений — регулировать действия уже запущенных программ, а именно, доступ к файловой системе, системному реестру и взаимодействие с другими программами.

## Как Предотвращение вторжений вычисляет репутацию программ

Предотвращение вторжений разделяет программы на категории (группы доверия), для которых и задаются ограничения. Все программы делятся по уровню доверия, на четыре заранее фиксированные группы:

- Доверенные
- Слабые ограничения
- Сильные ограничения
- Недоверенные

Kaspersky Endpoint Security определяет группу доверия во время первого старта программы. Основным инструментом для определения категории служит Kaspersky Security Network. Если доступа к сети нет или в KSN нет информации о программе, категория определяется в зависимости от настроек:

- **Группа доверия для программ, которые не удалось распределить по другим группам** — эта настройка позволяет администратору выбрать, какую категорию назначить программам, у которых еще нет репутации. Администратор может выбрать одну из трех групп: **Сильные ограничения**, **Слабые ограничения**, **Недоверенные**
- **Доверять программам, имеющим цифровую подпись** — если этот параметр включен, программы, подписанные доверенными сертификатами, будут автоматически помещаться в группу **Доверенные**

Доверенные сертификаты — это сертификаты, которым доверяет Kaspersky Security Network.

Определенная таким образом группа доверия сохраняется и используется при последующих запусках программы. Сохраненные сведения могут быть пересмотрены или удалены в результате действия следующих настроек:

— **Обновлять права для раннее неизвестных программ из базы KSN** — позволяет автоматически изменять группу доверия программы, если ранее ее не удалось определить с помощью KSN

— **Удалять права для программ, не запускавшихся более чем 60 дней** — позволяет не хранить информацию о группах доверия для программ, которые давно не запускались. Время, в течение которого хранится группа доверия, можно изменить

## Как Предотвращение вторжений ограничивает программы

Предотвращение вторжений ограничивает взаимодействие с другими программами и службами операционной системы, в зависимости от группы доверия. Обобщенно, ограничения по умолчанию для категорий доверия выглядят следующим образом:

| | |
|---|---|
| **Доверенные** | Нет ограничений |
| **Слабые ограничения** | Разрешено почти все, кроме внедрения в модули операционной системы и доступа к устройствам записи: веб-камерам и микрофонам |
| **Сильные ограничения** | Запрещены взаимодействия с модулями операционной системы и другими программами. Разрешена работа только с собственным сегментом оперативной памяти |
| **Недоверенные** | Запрещено все, в том числе запуск программы |

Предотвращение вторжений позволяет ограничивать доступ к файлам и папкам на диске, а также к ключам системного реестра. У Предотвращения вторжений есть список защищаемых ресурсов. Они сгруппированы в две категории:

— Операционная система
— Персональные данные

В каждой категории есть свои подкатегории и описания ресурсов: пути к папкам, маски файлов, маски ключей реестра. Изначально в списке защищаемых ресурсов уже присутствуют группы наиболее важных файлов и ключей реестра. Например, в категории *Операционная система* есть подкатегория *Параметры автозапуска*, где перечислены все ключи реестра, относящиеся к автозапуску программ.

Права доступа к группам ресурсов определяются для операций: *Чтение*, *Запись*, *Удаление* и *Создание*.

По умолчанию Предотвращение вторжений защищает ресурсы так:

| | Операционная система | Персональные данные |
|---|---|---|
| Доверенные | Полный доступ | Полный доступ |
| Слабые ограничения | *Полный доступ* ко всему, кроме критических файлов операционной системы<br>Для критических файлов операционной системы *только чтение* | Полный доступ |
| Сильные ограничения | Только чтение | Полный доступ |
| Недоверенные | Нет доступа | Нет доступа |

Ограничения для программы автоматически распространяются и на ее дочерние процессы. Если программа с ограничениями запускает доверенную программу, доверенная программа тоже будет ограничена. Если доверенную программу запускает пользователь или другая доверенная программа, ограничений не будет

## Как настраивать Предотвращение вторжений

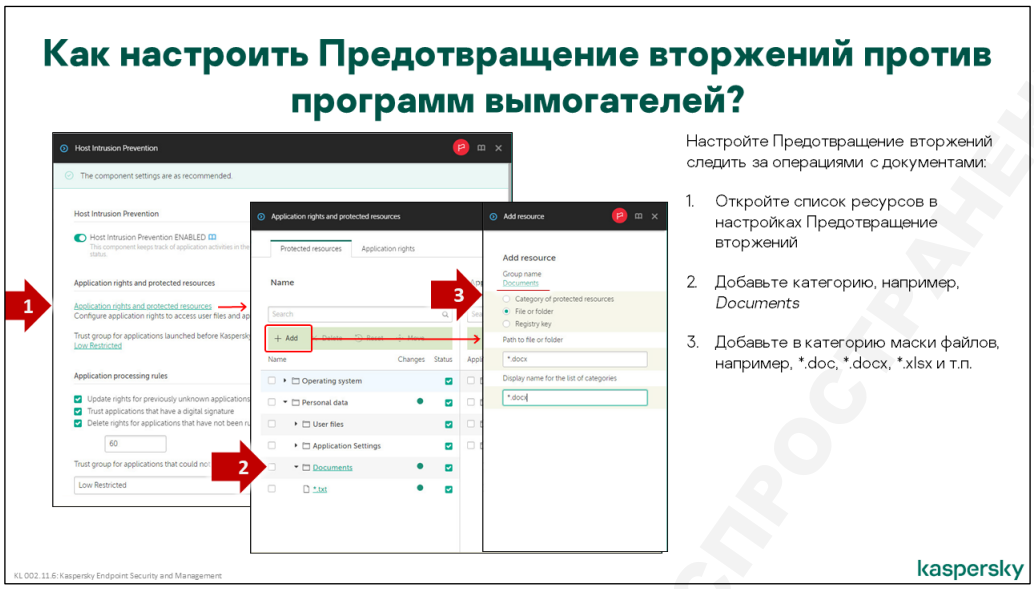
Администратор может изменить ограничения для любой группы доверия и даже для любой отдельной программы.

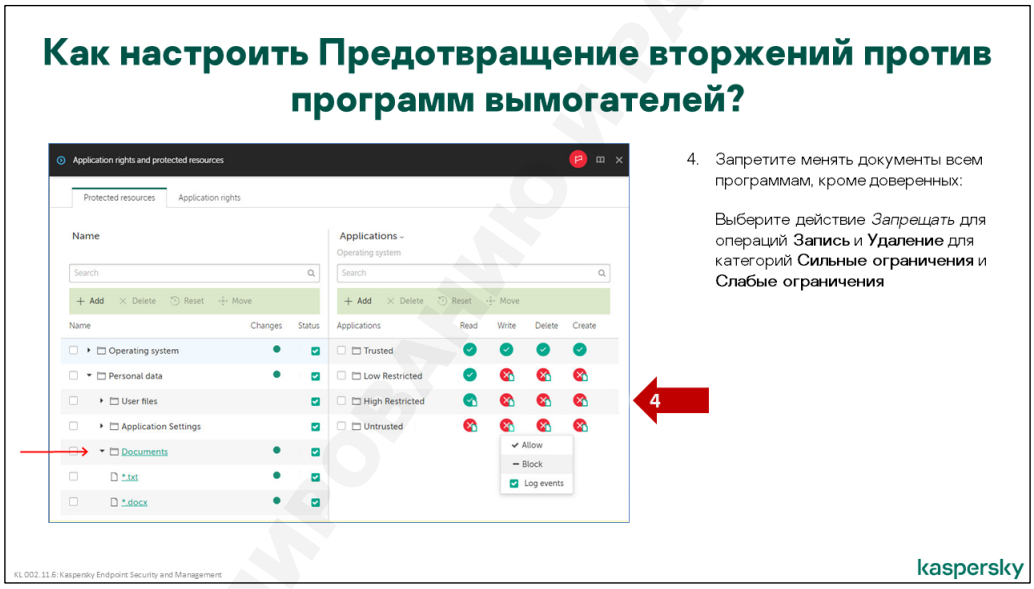
Не меняйте настройки Предотвращения вторжений, если не уверены точно, что делаете

Чтобы найти группы доверия и их ограничения:

1. Откройте раздел **Продвинутая защита** | **Предотвращение вторжений** в политике Kaspersky Endpoint Security
2. Перейдите по ссылке **Права программ и защищаемые ресурсы**
3. Перейдите на вкладку **Права программ**
4. Выберите группу доверия в левой панели
5. Вверху в правой панели, в выпадающем списке, выберите права

Здесь администратор может ограничить или расширить права для программ с выбранной репутацией. Например, он может разрешить доступ к веб-камере программам со слабыми ограничениями.




Чтобы увидеть защищаемые ресурсы:

1. Откройте раздел **Продвинутая защита** | **Предотвращение вторжений** в политике Kaspersky Endpoint Security
2. Перейдите по ссылке *Права программ и защищаемые ресурсы*

Чтобы защитить другие файлы или ключи реестра, добавьте их как свои ресурсы. Держите свои ресурсы в отдельной категории.

Чтобы добавить свои защищаемые ресурсы:

1. С помощью кнопки **Добавить** создайте свои категории и описания ресурсов
2. Настройте права доступа к ресурсу в таблице справа

Чтобы знать, когда предотвращение вторжений блокирует операцию, включите запись в журнал. Для этого кликните по действию в таблице и выберите **Записывать в отчет**. Вы можете

записывать в отчет, и когда Предотвращение вторжений разрешает действие[5], просто чтобы понять, какие программы работают с выбранным ресурсом.

Ограничения, установленные для программы, наследуются всеми ее дочерними процессами, даже если их исполняемые файлы относятся к группе **Доверенные**. Таким образом, программы с более низким уровнем доверия не могут воспользоваться привилегиями программ более высокого уровня доверия, чтобы обойти запреты

## Как настроить предотвращение вторжений против программ-вымогателей

С настройками по умолчанию Предотвращение вторжений защищает от программ с плохой репутацией операционную систему и другие программы на компьютере.

Администратор может легко защитить и файлы пользователей от программ неизвестного происхождения. Этим он защитит их и от программ-вымогателей, которые шифруют документы.

Идея простая. Программы-вымогатели:

- либо уже известны в KSN как вредоносные, и Kaspersky Endpoint Security не даст их запустить
- либо не имеют никакой репутации в KSN и получают от Предотвращения вторжений репутацию *Слабые ограничения* (по умолчанию) или *Сильные ограничения*, в зависимости от выбора администратора

Программы для работы с документами, такие как Microsoft Office, наоборот, хорошо известны и имеют репутацию *Доверенные*.

Поэтому, чтобы защитить документы, нужно не дать их менять программам с ограничениями. Для этого:

1. Откройте раздел **Продвинутая защита** | **Предотвращение вторжений** в политике Kaspersky Endpoint Security и перейдите по ссылке *Права программ и защищаемые ресурсы*

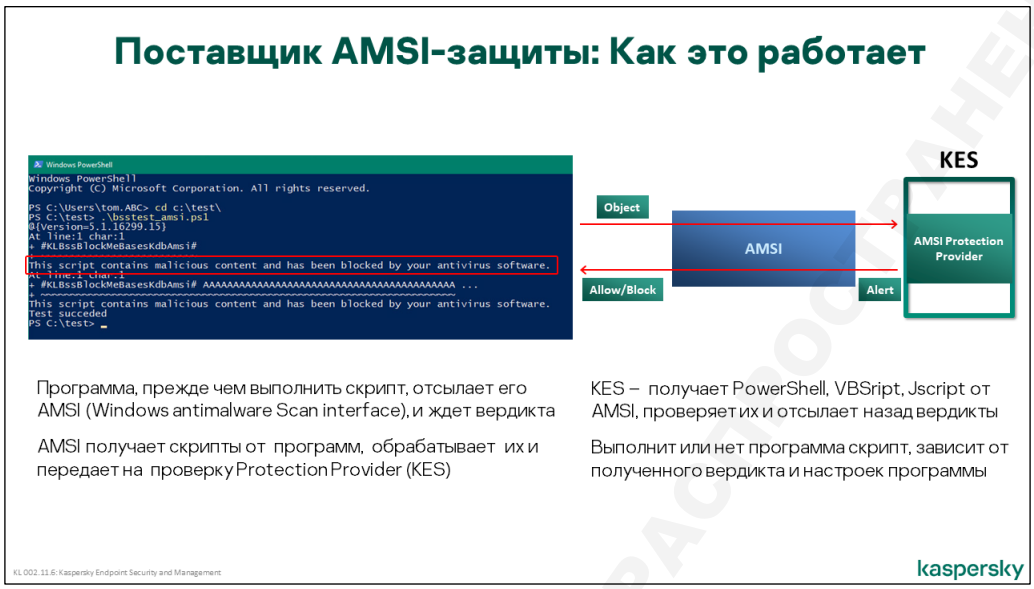
2. Добавьте документы в список защищенных ресурсов Предотвращения вторжений: выберите в списке слева категорию **Персональные данные** | **Файлы пользователя** и добавьте в нее новую категорию *Документы*

3. Добавьте в категорию расширения документов, такие, как **.doc*, **.docx*, **.pdf* и т.п. Для этого добавьте в категорию **Файл или папку** и укажите расширение в поле **Путь**. Повторите для всех расширений

4. Запретите менять документы программам с ограничениями. Для этого выберите категорию в списке слева и измените права в таблице справа: запретите **Запись** и **Удаление** программам с *сильными ограничениями* и *слабыми ограничениями*

[5] Будьте осторожны, чтобы не создать слишком большой поток событий с компьютеров на Сервер администрирования. Если нужно анализировать события о разрешении доступа, сохраняйте их только в локальном журнале Kaspersky Endpoint Security и не пересылайте на Сервер администрирования

# Как поставщик AMSI-защиты защищает от новых угроз?



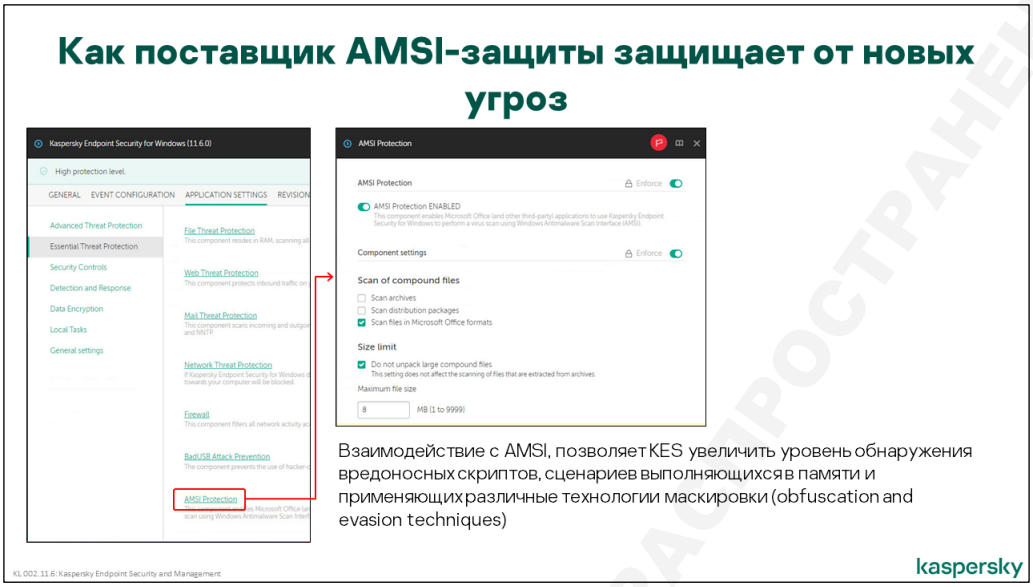

Antimalware Scan Interface (AMSI) – открытый API, разработанный компанией Microsoft, который позволяет антивирусным и другим решениям безопасности выполнять синхронное сканирование макросов и других скриптов во время выполнения и блокировать выполнение вредоносного кода приложениями.

Компонент **Поставщик AMSI** позволяет Kaspersky Endpoint Security лучше взаимодействовать с AMSI и за счет этого повысить уровень обнаружения целого ряда атак, например, бесфайловых атак.

В основе бесфайловых атак лежит следующая идея: зачем разрабатывать инструмент – вредоносную программу, если для достижения своих целей можно воспользоваться уже существующим, легитимными средствами. (например, PowerShell, JavaScript, VBScript и т.д.). Задача злоумышленника при организации бесфайловой атаки – перехватить управление процессом, запустить в памяти процесса свой код и воспользоваться этим кодом для вызова средств, имеющихся на устройстве.

Обнаружить такую атаку сложно, потому что у злоумышленника пропадает необходимость размещать на устройстве программы, которые могут быть распознаны, как вредоносные. Кроме того, часто применяются разнообразные методы маскировки. Например, метод запутывания (obfuscate) кода, усложняющий анализ кода, и техники обхода (evasion techniques), позволяющие незаметно передавать на компьютер требуемую информацию.

## Как происходит взаимодействие



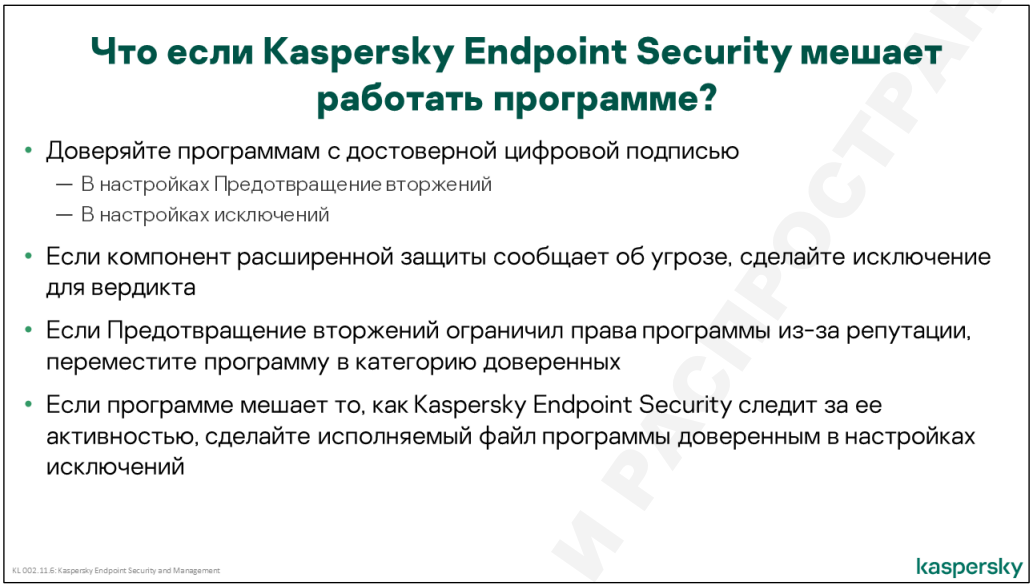

Опишем работу поставщика **Поставщик AMSI** на примере распространенного сегодня варианта атаки – запуск интерпретатора PowerShell из макроса в документе и выполнение вредоносного скрипта в PowerShell.

В процессе открытия документа, прежде чем выполнить скрипт, программа предает его на проверку в ASMI и ожидает от него вердикта. AMSI протоколирует действия скрипта и передает его команды, через поставщика AMSI, антивирусному провайдеру – Kaspersky Endpoint Security. Это и позволяет предоставить доступ антивирусному провайдеру к тем командам, которые скрипт соорудил на лету полностью в памяти. Kaspersky Endpoint Security проверяет команды, генерируемые скриптом и возвращает вердикт. AMSI в зависимости от полученного вердикта, сообщает приложению выполнять данный скрипт или нет. Такая схема работы реализована для приложений Microsoft, но может быть реализована для любого приложения, которое поддерживает работу с AMSI.

Кроме скриптов, приложения могут передавать на проверку Kaspersky Endpoint Security архивы и дистрибутивы плагинов перед их установкой.

# 4.4 Как исключить программу из мониторинга

## Что делать, если KES мешает работать программе




Практически любой эвристический анализ дает ложные срабатывания. Чтобы их уменьшить, исключите из анализа заведомо чистые программы:

— Программы, доверенные в Kaspersky Security Network
— Программы, подписанные доверенными сертификатами

Чтобы не блокировать программы, доверенные в KSN, просто используйте KSN. Чтобы доверять подписанным программам, используйте настройку Предотвращения вторжений — **Правила обработки программ | Доверять программам, имеющим цифровую подпись**.

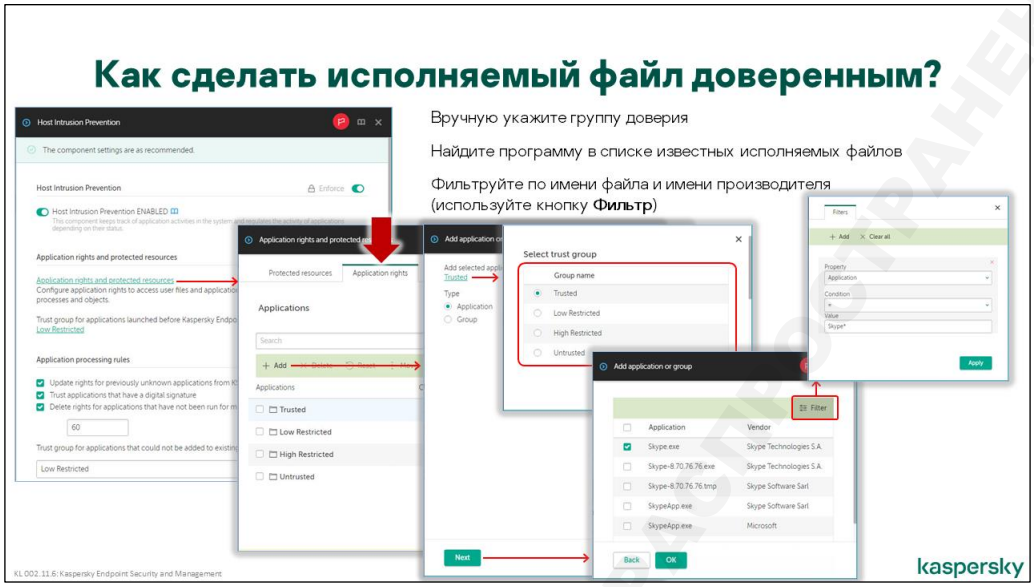
Kaspersky Endpoint Security доверяет не всем цифровым подписям, а только тем, которые основаны на доверенных сертификатах. Доверенные сертификаты, это те, которые происходят от доверенных центров сертификации.

Kaspersky Endpoint Security использует свою базу сертификатов, и не обязательно доверяет сертификатам в локальном хранилище *Доверенные корневые центры сертификации*. Если сертификат скомпрометирован, Kaspersky Endpoint Security узнает об этом из Kaspersky Security Network, и не будет доверять файлам, подписанным этим сертификатом.

Цифровым подписям с самоподписанным сертификатом Kaspersky Endpoint Security тоже не доверяет. Чтобы доверять программам собственной разработки, которые подписаны самоподписанным сертификатом, добавьте сертификат в доверенную зону Kaspersky Endpoint Security, как описано в подразделе Исключения по сертификатам, раздела 2.5

Если у программы нет цифровой подписи, вы можете вручную поместить ее в группу *Доверенные* в политике Предотвращения вторжений. Или же можно полностью исключить программы из проверки Анализом поведения и Предотвращением вторжений. Как это сделать, читайте ниже.

# Как изменить категорию доверия для программы




Большинство распространенных коммерческих программ имеют репутацию Доверенные. Но некоторые программы с открытым кодом имеют репутацию Слабые ограничения. А программы собственной разработки компании могут не иметь репутации в KSN, а от Предотвращения вторжений могут получить репутацию Слабые ограничения (или Сильные ограничения, в зависимости от настроек в политике).

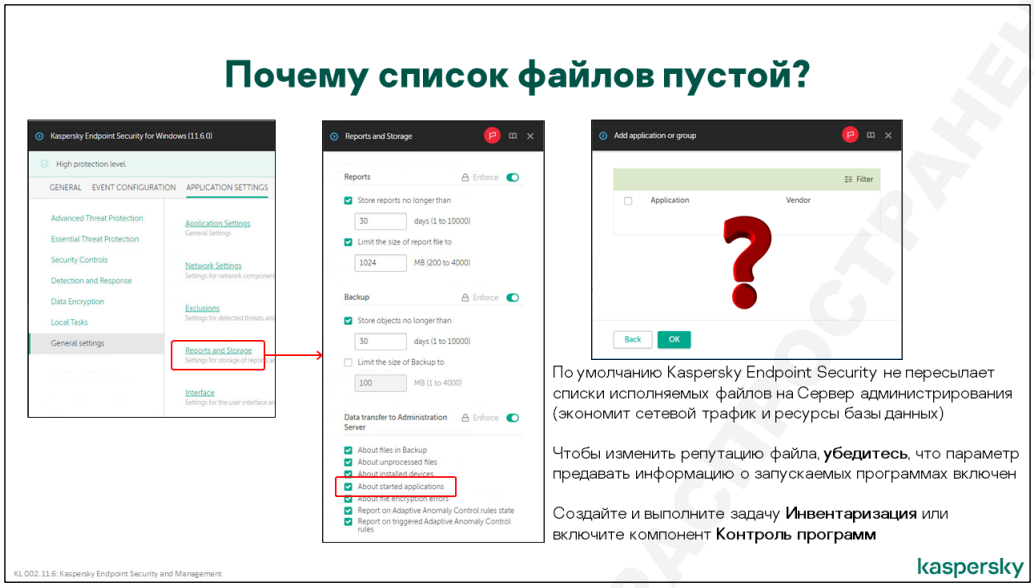
Если ограничения репутации мешают работать программе, измените ее репутацию в политике Kaspersky Endpoint Security:

1. Откройте раздел **Продвинутая защита** | **Предотвращение вторжений** в политике Kaspersky Endpoint Security
2. Перейдите по ссылке Права программ и защищаемые ресурсы
3. Перейдите на вкладку **Права программ**
4. Нажмите **Добавить** над списком категорий приложений
5. Выберите группу, в которую необходимо переместить файл: **Доверенные, Слабые ограничения** и т.д. и нажмите **Далее**
6. Нажмите **Фильтрация** и отфильтруйте список приложений по имени исполняемого файла.
7. Отметьте исполняемый файл в результатах работы фильтра и нажмите **ОК**

Если администратор выбрал репутацию файла в политике, Предотвращение вторжений на компьютерах будет использовать эту репутацию, а не репутацию из KSN. Репутация из KSN используется только для файлов, не заданных явно в политике. Т.е. для большинства файлов, потому что по умолчанию в политике есть только репутационные группы, а файлов нет.

Если администратор добавил файл в репутационную группу в политике, он может изменить ограничения для этого файла как угодно. Например, администратор может добавить программу в группу *Доверенные*, но потом открыть права программы и запретить ей доступ к веб-камере.

## Что делать, если в политике список известных программ пустой



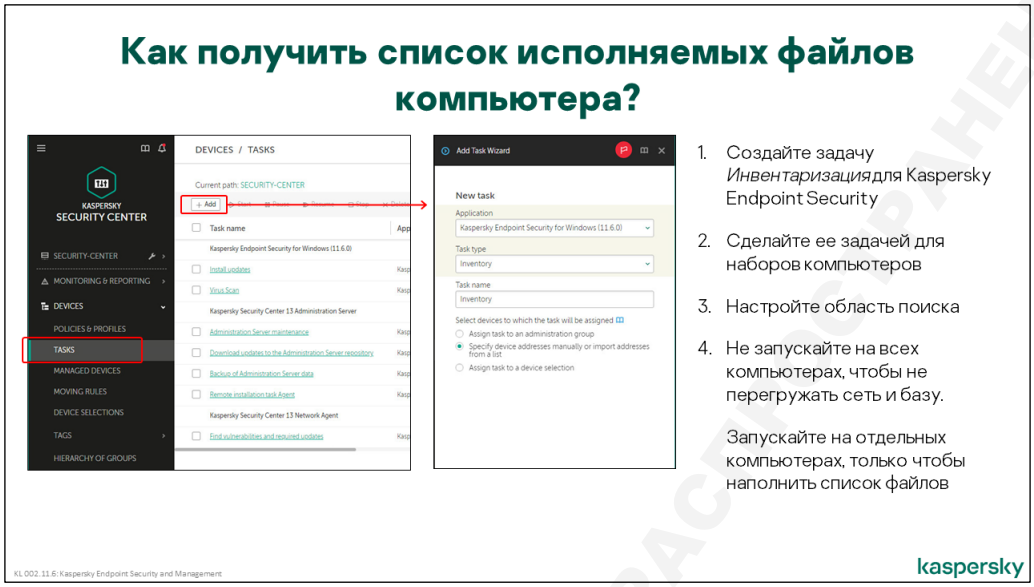

Если вы используете политики с настройками по умолчанию, скорее всего список исполняемых файлов в политике окажется пустым.

Kaspersky Endpoint Security на компьютерах перехватывает все исполняемые файлы, и Предотвращение вторжений присваивает всем им репутацию. Но на Сервер администрирования эти данные по умолчанию не поступают. А политика показывает только те исполняемые файлы, о которых Kaspersky Endpoint Security сообщил на Сервер администрирования.

Чтобы Kaspersky Endpoint Security переслал на сервер списки исполняемых файлов компьютеров, создайте и выполните задачу **Инвентаризация** или включите компонент **Контроль программ** и запустите требуемую программу.

Списки исполняемых файлов компьютера относительно большие. Если их пошлют на Сервер все управляемые компьютеры, это заметно увеличит загрузку сети. И, как правило, это не нужно. Не запускайте задачу **Инвентаризация** для всех компьютеров. Не включайте **Контроль программ** для компьютеров, на которых не планируется его использовать для контроля запуска программ. Чтобы получить только нужные файлы, создавайте задачу **Инвентаризация** для набора компьютеров.

## Как получить список программ с компьютера

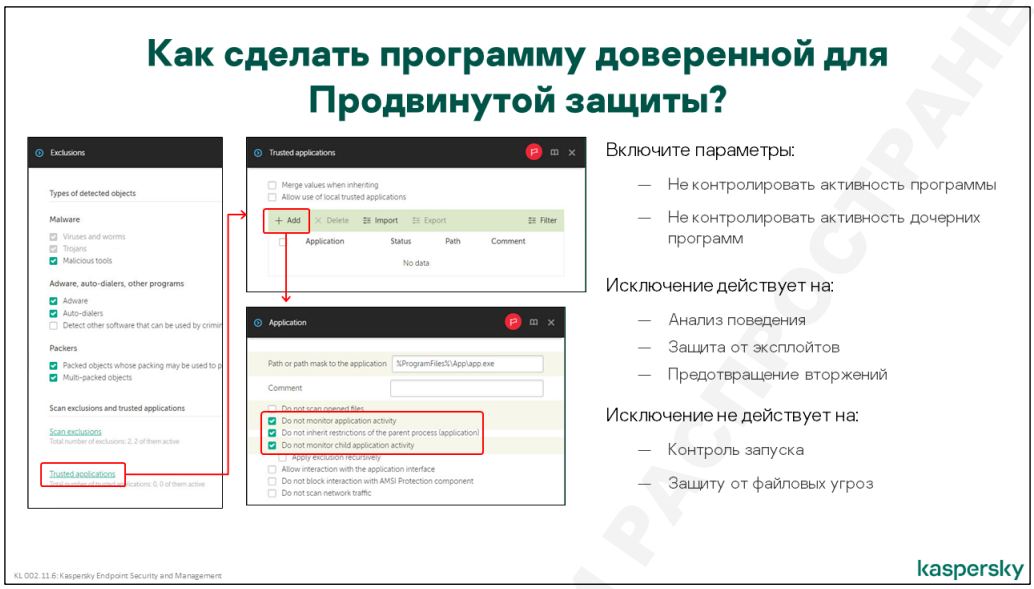



Собирать списки файлов со всех компьютеров не рекомендуется. Часто у администраторов есть тестовые компьютеры, на которых установлены все типичные программы. Если такие компьютеры есть, собирайте списки исполняемых файлов с них. А чтобы наполнить локальный список известных программ на тестовом компьютере, и не запускать все программы вручную, используйте задачу *Инвентаризации*.

Задача *Инвентаризации* сканирует файлы в указанных папках, находит исполняемые файлы, добавляет их в локальный список известных исполняемых файлов и активирует передачу данных на Сервер администрирования. Чтобы результаты сканирования попали на сервер, параметр информировать Сервер о запускаемых программах должен быть включен в политике Kaspersky Endpoint Security.

Чтобы создать задачу инвентаризации, запустите мастер создания задачи на странице **Устройства | Задачи**. Выберите тип задачи **Инвентаризация** из задач *Kaspersky Endpoint Security для Windows*. Если это задача для тестового компьютера, после создания задачи, откройте ее свойства и включите область поиска *Все жесткие диски*. Назначьте задачу отдельным тестовым компьютерам.

# Как сделать программу доверенной для Анализа поведения и Предотвращения вторжений




Если установленные Предотвращением вторжений ограничения все-таки мешают нормальной работе какой-нибудь программы, можно исправить положение, настроив соответствующее исключение. Исключения для Предотвращения вторжений бывают двух типов:

- **Исключение для ресурсов** — разрешает любым программам выполнять любые операции с указанной группой ресурсов (недоступно через веб-консоль)
- **Исключения для программ** — позволяют снять любые ограничения для отдельной программы

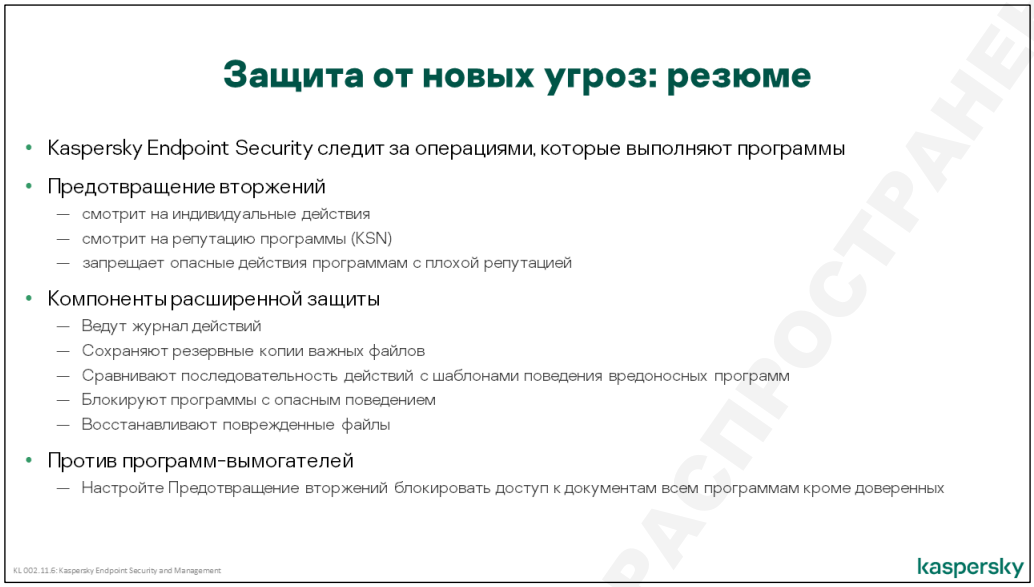
Исключения для ресурсов задаются в свойствах Предотвращения вторжений, на вкладке **Защищаемые ресурсы**. В качестве ресурсов, для которых настраиваются исключения, можно указывать папки, файлы и ключи системного реестра.

Исключения для программ настраиваются в доверенных программах, и предоставляют несколько возможностей:

- **Не контролировать активность программы** — отключить ограничения, касающиеся непосредственно указанной программы
- **Не наследовать ограничения родительского процесса** — отключает ограничения, наследованные от процесса, который запустил программу и родительских процессов боле высокого уровня
- **Не контролировать активность дочерних программ** — отключает ограничения для процессов, запущенных программой, для которой задано исключение

Эти исключения распространяются и на Анализ поведения, и на Предотвращение вторжений.

# 4.5 Защита от новых и сложных угроз: резюме




Почти все компоненты Kaspersky Endpoint Security помогают защищать от новых угроз, но в первую очередь за это отвечают Анализ поведения и Предотвращение вторжений. Оба компонента следят за операциями, которые выполняют программы.

Предотвращение вторжений вычисляет репутацию исполняемых файлов и ограничивает действия программ с плохой или неизвестной репутацией. Репутацию программ поставляет Kaspersky Security Network или администратор, через настройки политики.

Анализ поведения следит не за отдельными действиями программ, а за тем, что они делают вообще. Для этого он записывает все, что делают программы в журнал и потом ищет в последовательности действий признаки вредоносной активности. С помощью журнала действий Откат вредоносных действий откатывает действия вредоносных программ.

У Анализа поведения есть специальные эвристики, чтобы обнаруживать действия программ-вымогателей, которые шифруют документы и требуют выкуп. Во многих случаях Анализ поведения с помощью Отката вредоносных действий может восстановить зашифрованные документы.

Чтобы лучше защититься от программ-вымогателей, настройте Предотвращение вторжений блокировать доступ к документам программам с плохой репутацией.

Не выключайте Анализ поведения и Предотвращение вторжений. Это компоненты, в которых реализованы передовые технологии для защиты от самых сложных угроз

# 5. Как контролировать сетевые соединения

## 5.1 Как Сетевой экран защищает от угроз


С точки зрения безопасности Сетевой экран выполняет две функции:

- Блокирует несанкционированные сетевые подключения к компьютеру, тем самым снижая вероятность его заражения
- Блокирует несанкционированную сетевую активность программ на клиентском компьютере. Это снижает риск возникновения эпидемий, а также ограничивает действия пользователей сознательно или неосознанно нарушающих политику безопасности

Сетевой экран тесно связан с Предотвращением вторжений. Предотвращение вторжений ограничивает доступ программ к настройкам операционной системы, другим программам и файлам пользователей. Сетевой экран смотрит на ту же репутацию программ и ограничивает их доступ к сети. Этим сетевой экран не дает уже запущенным вредоносным программам нанести ущерб: например, отправить пароли пользователя злоумышленнику.

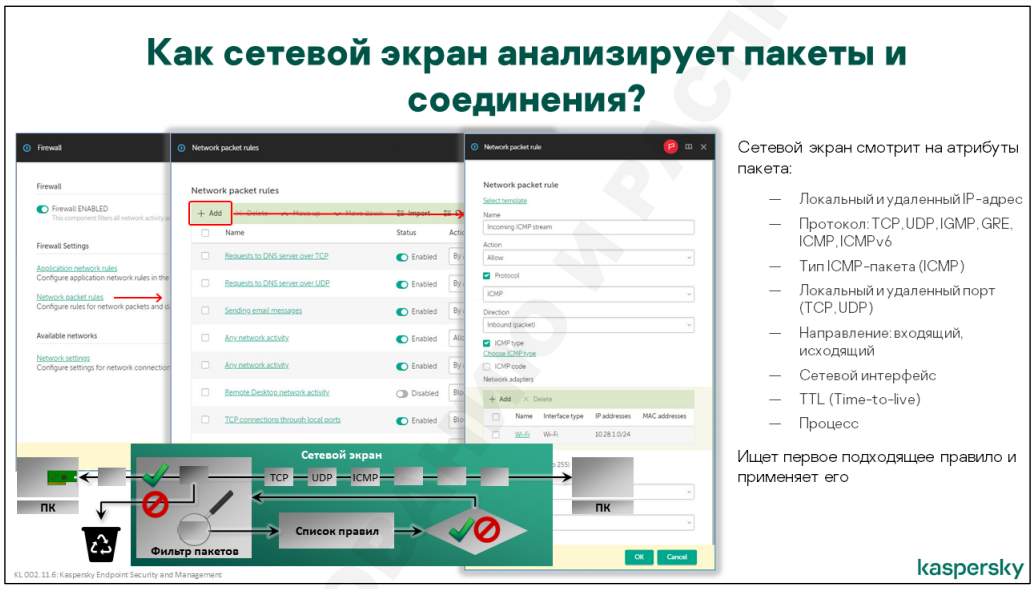
Параллельно с Сетевым экраном пакеты анализирует защита от сетевых угроз. Если Сетевой экран использует относительно простые правила, чтобы блокировать пакеты и соединения, защита от сетевых угроз смотрит на последовательности пакетов и ищет в них следы сетевых атак, например, атак на переполнение буфера через известные уязвимости. Соединения, по которым идет атака, блокируются.

# 5.2 Как работает сетевой экран в Kaspersky Endpoint Security

Сетевой экран контролирует соединения на сетевом и транспортном уровнях с помощью пакетных правил. Он анализирует водящие и исходящие пакеты, сравнивает их с имеющимися правилами и выполняет одно из двух действий:

— Разрешить
— Блокировать

## Как сетевой экран анализирует пакеты и соединения




Самая простая часть Сетевого экрана Kaspersky Endpoint Security это список пакетных сетевых правил. Чтобы его увидеть, откройте раздел Сетевой экран в политике Kaspersky Endpoint Security и перейдите по ссылке **Сетевые пакетные правила**.

Пакетное правило содержит следующие атрибуты:

| | |
|---|---|
| **Действие** | **Разрешать**, **Запрещать** или **По правилам программы**<br>*По правилам программы* означает, что Сетевой экран пойдет искать подходящее правило в настройках программы, к которой относится пакет. А если у этой программы нет настроек, то в настройках репутационной группы, в которую входит программа |
| **Протокол** | TCP, UDP, ICMP, ICMPv6, IGMP, GRE |
| **Направление** | **Входящее (пакет)** — применяется к входящим пакетам<br>**Входящее** — применяется к пакетам во входящих соединениях<br>**Входящее/исходящее** — применяется ко всем пакетам<br>**Исходящее (пакет)** — применяется к исходящим пакетам<br>**Исходящее** — применяется во всех пакетах в исходящих соединениях<br>Протокол *TCP* устанавливает соединения, поэтому вместе с протоколом TCP используйте направления *Входящее*, *Исходящее* и *Входящее/Исходящее*<br>Остальные протоколы не устанавливают соединения, а посылают пакеты. Вместе с ними используйте *Входящее (пакет)*, *Исходящее (пакет)* и *Входящее/Исходящее* |
| **Удаленные порты** | Порты на удаленном компьютере<br>Можно задать для протоколов TCP и UDP<br>Чтобы задать несколько портов, перечислите их через запятую: например, *25, 110*<br>Чтобы указать диапазон, используйте дефис: *0-1024* |
| **Локальные порты** | Порты на локальном компьютере<br>Можно задать для протоколов TCP и UDP |
| **ICMP-тип** | *Эхо-запрос*, *ответ на эхо-запрос*, *истекло время жизни пакета*, *цель недоступна* и т.д.<br>Можно выбрать для протоколов ICMP и ICMPv6 |
| **ICMP-код** | Уточняющий код для некоторых ICMP-типов. Можно выбрать код 0, 1 или 2<br>Например для ICMP-пакета *Цель недоступна*, код 0 означает *Сеть недоступна*, код 1 — *Хост недоступен*, код 2 — *Протокол недоступен*[6] |
| **Сетевые адаптеры** | Позволяет указать сетевой адаптер по **типу интерфейса**, **IP-адресу** и **MAC-адресу**<br>Типы интерфейсов: *Loopback*, *Проводная сеть (Ethernet)*, *Беспроводная сеть (Wi-Fi)*, *Туннель*, *PPP-соединение*, *PPPoE-соединение*, *VPN-соединение*, *Модемное соединение* |
| **TTL** | Время жизни пакета |
| **Удаленные адреса** | Адреса удаленных компьютеров, которые можно задать прямо или косвенно<br>Чтобы задать адреса прямо, выберите **Адреса из списка** и наполните список IP-адресов<br>Чтобы задать адреса косвенно, выберите **Любой адрес** или **Адрес подсети**. Адрес подсети может быть: *Доверенные сети*, *Локальные сети* и *Публичные сети* |
| **Локальные адреса** | Адреса локального компьютера (у компьютера может быть много адресов)<br>Можно выбрать или Любой адрес, или Адреса из списка и наполнить список |

IP-адреса можно указывать и IPv4 и IPv6

Сетевой экран сравнивает атрибуты пакета с атрибутами правила, и если все они совпадают — протокол, порты, направление, сетевой адаптер, локальный адрес, удаленный адрес — то применяет действие, указанное в правиле.

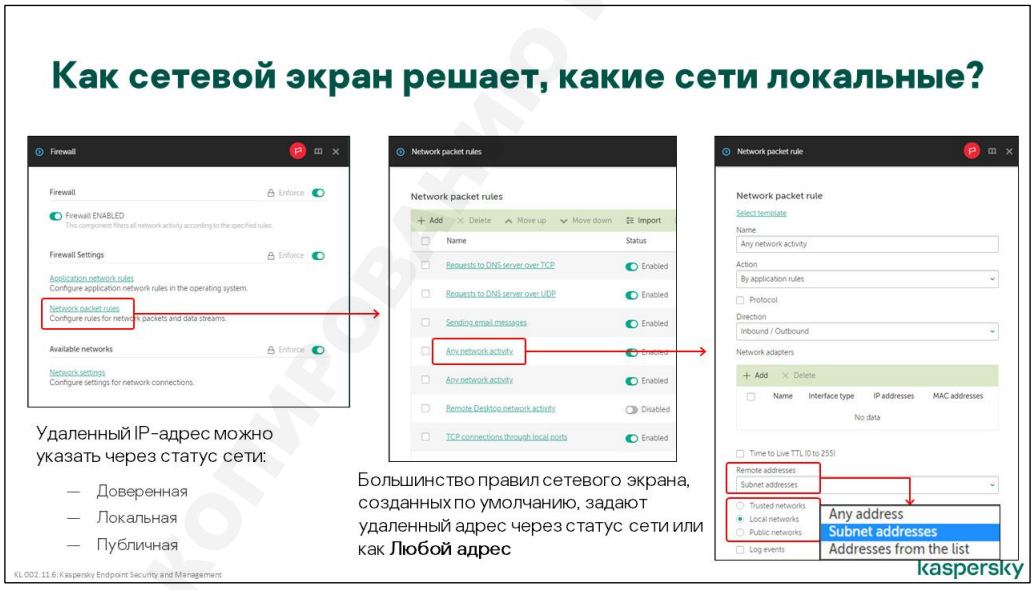
Применение правила может сопровождаться записью в журнале работы сетевого экрана. За это отвечает параметр **Записать в отчет**.

Сетевой экран смотрит на правила по порядку сверху вниз и применяет первое подходящее. Чтобы изменить порядок правил, выберите правило и переместите его кнопками **Вверх** и **Вниз**.

Политика изначально содержит список пакетных правил, обеспечивающих разумный уровень безопасности для компьютеров как внутри корпоративной сети, так и за ее пределами. Подробнее о том, какой эффект производят стандартные настройки рассказывается в конце этой главы, после изучения всех параметров.

Стандартные пакетные правила не являются незыблемыми. Администратор может изменять и удалять их, а также создавать свои. Для удобства настройки правил, протокол, порты и направление можно задавать с помощью шаблонов (например, *Любая сетевая активность*, *Просмотр веб-страниц*, *Сетевая активность для работы удаленного рабочего стола* и т. п.) Чтобы выбрать шаблон, используйте кнопку справа от поля **Название** в настройках правила.

## Как сетевой экран решает, какие сети локальные?




Адреса удаленных компьютеров в правилах могут быть заданы косвенно, как **Адреса подсети**: *Доверенные сети*, *Локальные сети* или *Публичные сети*. Как Сетевой экран решает, какие адреса относятся к каким сетям?

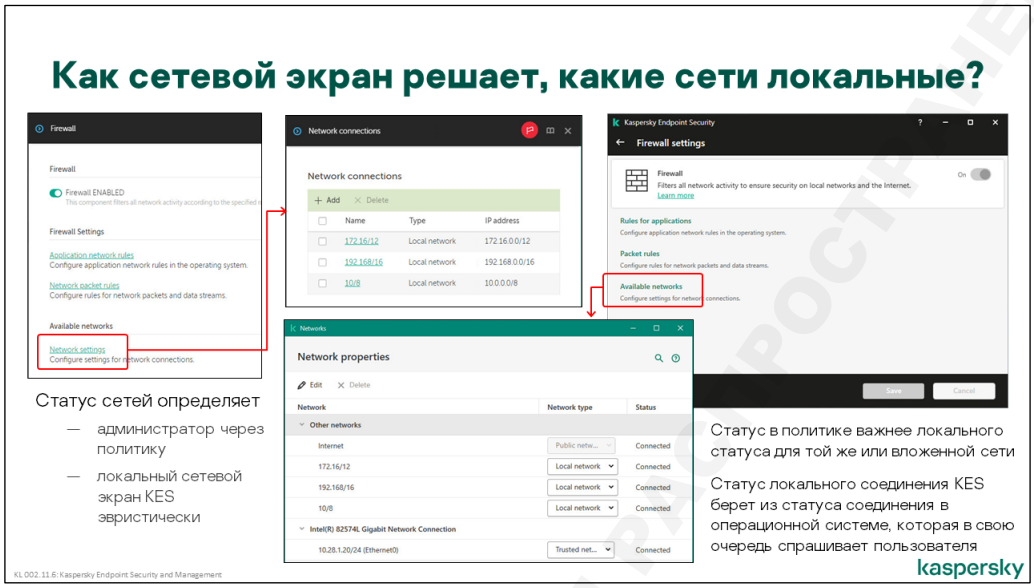
Статусы сетей указывает администратор в политике Kaspersky Endpoint Security. А если политика ничего не говорит о статусе сети, Сетевой экран определяет статус сетей самостоятельно на клиентском компьютере.

Чтобы добавить в политику сеть и выбрать ее статус:

1. Нажмите ссылку **Настройка сети** в разделе Базовая защита | Сетевой экран
2. Нажмите кнопку **Добавить** над списком

[6] Типы сообщений ICMP и значения кодов смотрите в документации к протоколу

3. Введите удобное имя подсети и выберите ее тип
4. Укажите адрес подсети в формате <*IP-адрес*>/<*длина маски в битах*>, например *192.168.0.0/24* или *1234::cdef/96* для IPv6-сетей




На компьютере к сетям из политики Сетевой экран добавляет сети, настроенные для сетевых адаптеров компьютера. Если сеть адаптера совпадает или входит в сеть из политики, она получает статус сети из политики.

Если сеть адаптера не входит ни в одну из сетей из политики, Сетевой экран выбирает ей статус исходя из статуса сети в операционной системе. Если сеть доменная, рабочая или домашняя, Сетевой экран дает ей статус *Локальной сети*. Если сеть публичная в операционной системе, она будет *публичной* и для Сетевого экрана Kaspersky Endpoint Security.

Все остальные адреса считаются адресами публичных сетей.

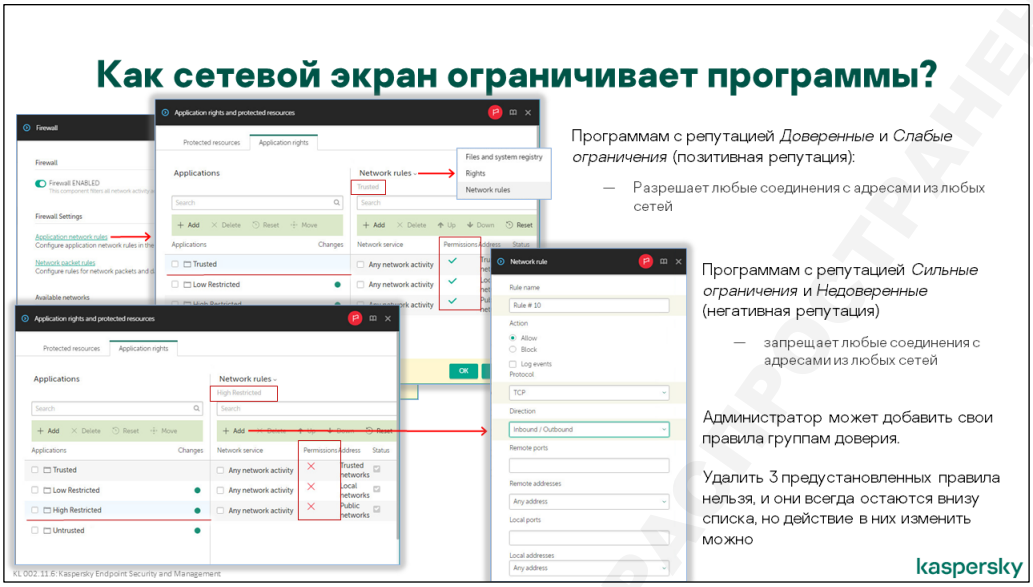
Например, в политике может быть указана сеть 172.16.0.0/16 со статусом **Локальная сеть**. Управляемый компьютер при этом может иметь два сетевых интерфейса, настроенных для работы в сетях 172.16.55.0/24 and 192.168.5.0/24 соответственно. Предположим, что Kaspersky Endpoint Security присвоил обоим сетям статус **Публичная сеть**. При наложении настроек политики на локальные, итоговым статусом сети 172.16.55.0/24 будет **Локальная сеть**, потому что в политике указана сеть 172.16.0.0/16, которая содержит в себе 172.16.55.0/24. У второй сети 192.168.5.0/24 статус останется **Публичная сеть**, поскольку в политике подходящей сети не указано.

По умолчанию в политике указаны три стандартных диапазона сетей, каждому из которых присвоен статус **Локальная сеть**:

— 10.0.0.0/8
— 172.16.0.0/12
— 192.168.0.0/16

Такие настройки разумны внутри периметра корпоративной сети. Но для работы за пределами сети, например, при подключении через VPN или с ноутбука во время командировки, настройки должны быть пересмотрены.

# Как сетевой экран ограничивает программы?




Если Сетевой экран не нашел подходящего правила для пакета, или нашел, но действие в правиле *По правилам программы*, он идет искать пакетное правило для этой программы в настройках программы. А если у программы в политике нет настроек, он смотрит на репутацию программы и ищет подходящее пакетное правило в настройках для репутации.

Сетевой экран использует те же репутации, что и Предотвращение вторжений. Настройки, по которым Предотвращение вторжений выбирает репутацию, распространяются и на Сетевой экран. Если компонент Предотвращение вторжений не установлен, Сетевой экран сам определяет репутацию, используя настройки Предотвращения вторжений. Программа не может быть *доверенной* для Предотвращения вторжений, и быть в *сильных ограничениях* для Сетевого экрана. Репутация у программы всегда одна.

Чтобы увидеть пакетные правила для программ и репутаций:

1. Нажмите ссылку *Права программ и защищаемые ресурсы* в области **Предотвращение вторжений | Права программ и защищаемые ресурсы**
2. В левом окне **Программы** выберите программу или репутацию
3. В верху правого окна, в выпадающем списке выберите **Сетевые правила**

По умолчанию в политике нет программ, а есть только репутации и настройки для репутаций. Администратор может добавить программы к той или иной репутации и после этого может добавить в свойствах программы какие угодно пакетные правила. Добавляйте программы точно так же, как и в Предотвращении вторжений.

У каждой программы и репутации в списке правил всегда есть три правила и они всегда находятся внизу списка:

— Любая сетевая активность в Доверенных сетях
— Любая сетевая активность в Локальных сетях
— Любая сетевая активность в Публичных сетях

Для репутаций **Доверенные** и **Слабые ограничения** действие всех трех правил по умолчанию **Разрешать**, а для репутаций **Сильные ограничения** и **Недоверенные** — **Запрещать**. Стандартные правила нельзя удалить или изменить, за исключением атрибута **Действие**, который администратор может менять по своему усмотрению.

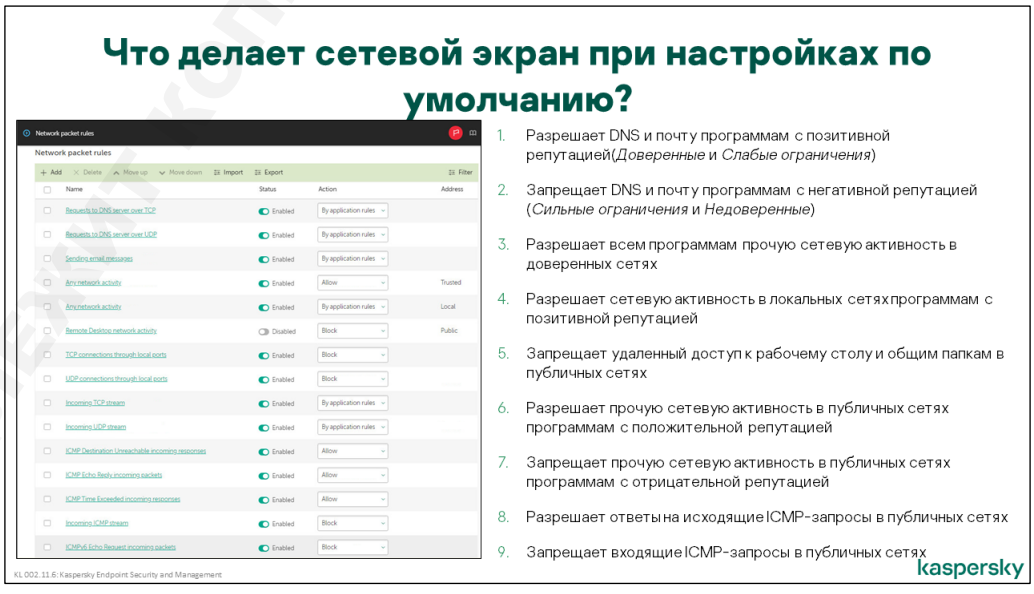
По умолчанию, когда в политике заданы только репутации, у репутаций есть только эти три правила и больше никаких других правил нет. Вместе эти правила перехватывают всю сетевую активность, потому что любой адрес относится или к доверенной, или к локальной, или к публичной сети. Поэтому для любого пакета всегда найдется правило: пакет обязательно относится к процессу, у процесса обязательно есть репутация, а у репутации обязательно есть как минимум одно правило для любого удаленного адреса по типу сети.

Администратор может добавить свои правила в список правил репутации или программы. У этих правил есть не все атрибуты, а только:

| | |
|---|---|
| **Действие** | Разрешать или Запрещать |
| **Протокол** | TCP, UDP, ICMP и ICMPv6 |
| **Направление** | *Входящее*, *Исходящее* или *Входящее/Исходящее* |
| **Удаленные порты** | для TCP и UDP |
| **Локальные порты** | для TCP и UDP |
| **ICMP-тип** | для ICMP и ICMPv6 |
| **ICMP-код** | для ICMP и ICMPv6 |
| **Удаленные адреса** | |
| **Локальные адреса** | для TCP и UDP |
| **Действие** | Разрешать или Запрещать |

# 5.3 Что делает сетевой экран с настройками по умолчанию

## Что делает Сетевой экран при настройках по умолчанию



Стандартная политика не содержит правил для программ (кроме, стандартных, заданных для репутаций). Поэтому окончательный статус сетей и репутации программ определяются сетевым экраном локально.

Пакетные правила наследуются из политики, и согласно им, пакеты фильтруются следующим образом:

1. Первые три правила регулируют возможность отсылать DNS-запросы (протоколы TCP и UDP, внешний порт 53) и почту (протокол TCP, внешние порты 25, 465, 143, 993). В этих правилах выбрано действие **По правилам программы**, т.е. программы из групп **Доверенные** и **Слабые ограничения** будут иметь возможность отправлять DNS-запросы и почту, а все остальные нет

2. Четвертое правило разрешает любую сетевую активность в *доверенных* сетях всем программам. Таким образом, в доверенных сетях изначально разрешена любая активность, кроме ограничений на работу с DNS и почтой для недоверенных программ и программ с сильными ограничениями

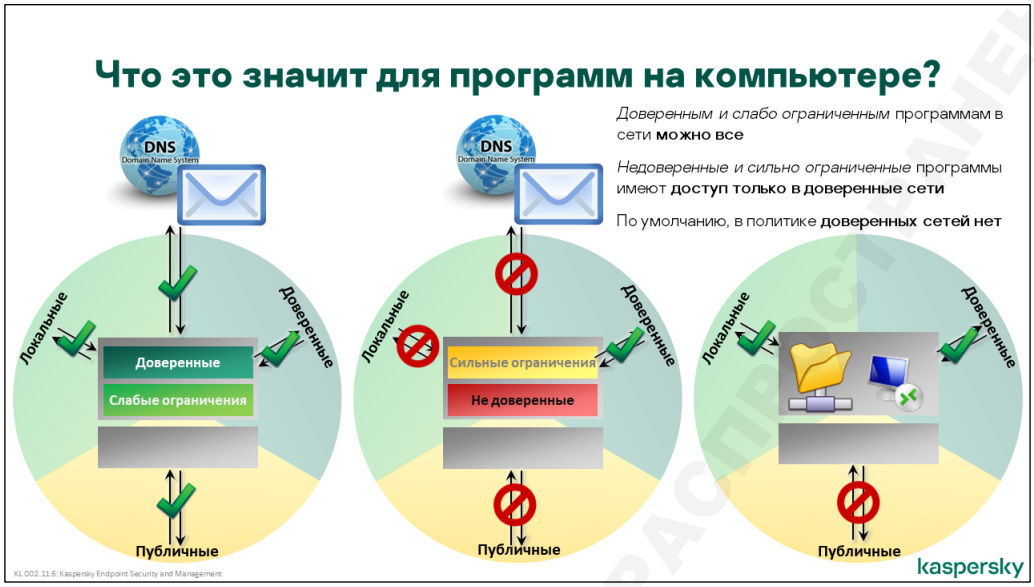
3. Пятое правило определяет порядок обработки пакетов в *локальных* сетях. Такие пакеты обрабатываются по правилам программ. С учетом предыдущих правил, получается, что для программы из групп **Доверенные** и **Слабые ограничения** ограничений на работу в локальных сетях нет, а остальные программы доступа к сетям с таким статусом не имеют

4. Оставшаяся часть списка регулирует работу в сетях со статусом **Публичные**. Правила 6–8 запрещают подключение к компьютеру из публичных сетей с помощью удаленного рабочего стола, а также блокируют подключение к локальной службе DCOM, NetBIOS-пакеты, доступ к общим папкам Windows, и доступ к Universal Plug & Play устройствам

5. Правила 9 и 10 разрешают входящие потоки (сеансы TCP и UDP) только к программам из групп **Доверенные** и **Слабые ограничения**. При этом, поскольку исходящие потоки правилами фильтрации по умолчанию не регулируются, они тоже фильтруются согласно правилам для программ. Т.е. программы из групп **Сильные ограничения** и **Недоверенные** доступа к публичным сетям изначально не имеют

6. Правила с 11-го по 15-е блокируют входящие диагностические запросы ICMP, оставляя при этом возможность отправлять ICMP пакеты для проверки связи с удаленными компьютерами.

# Что это значит для программ на компьютере



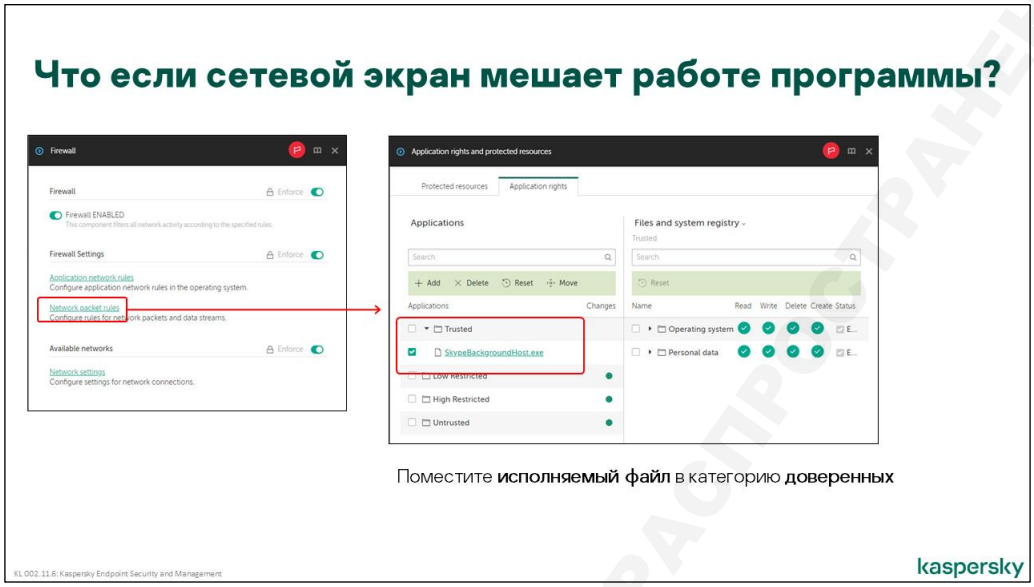

Доверенные программы и программы со слабыми ограничениями имеют полный доступ ко всем сетям. Поэтому по умолчанию Сетевой экран не мешает известным программам.

Недоверенные программы и программы с сильными ограничениями имеют доступ только к доверенным сетям, и даже там не могут работать с почтой и DNS. Но по умолчанию в политике доверенных сетей нет, поэтому эффективно недоверенные программы и программы с сильными ограничениями доступа к сети не имеют.

Этим Сетевой экран не дает неизвестным вредоносным программам воровать пароли, загружать дополнительные модули, получать команды из центра управления и участвовать в спам-рассылках

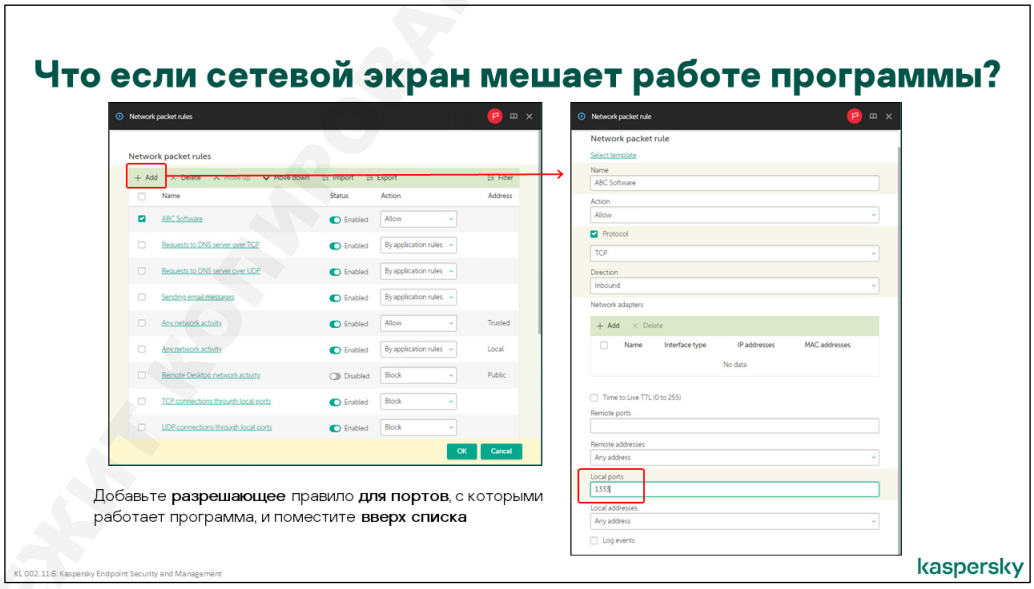
Дополнительно Сетевой экран запрещает доступ к службам операционной системы (общим папкам, удаленному рабочему столу, DCOM и др.) и блокирует ICMP-запросы из публичных сетей.

# Что если сетевой экран мешает работать программе




Подавляющее большинство программ, использующих сеть, автоматически относятся к группам **Доверенные** и **Слабые ограничения**, и поэтому могут беспрепятственно обмениваться данными по сети.

Но малоизвестные программы с открытым кодом или программы собственной разработки могут получить репутацию **Сильные ограничения** и не смогут работать с сетью.




Чтобы дать доступ к сети программам с репутацией Сильные ограничения, используйте один из следующих подходов:

— Измените репутацию программы, добавьте ее исполняемый файл в репутацию Слабые ограничения или доверенные, как описано в разделе 4.3

— Если файлы программы подписаны сертификатом, используйте настройки Предотвращения вторжений, чтобы доверять файлам этой программы

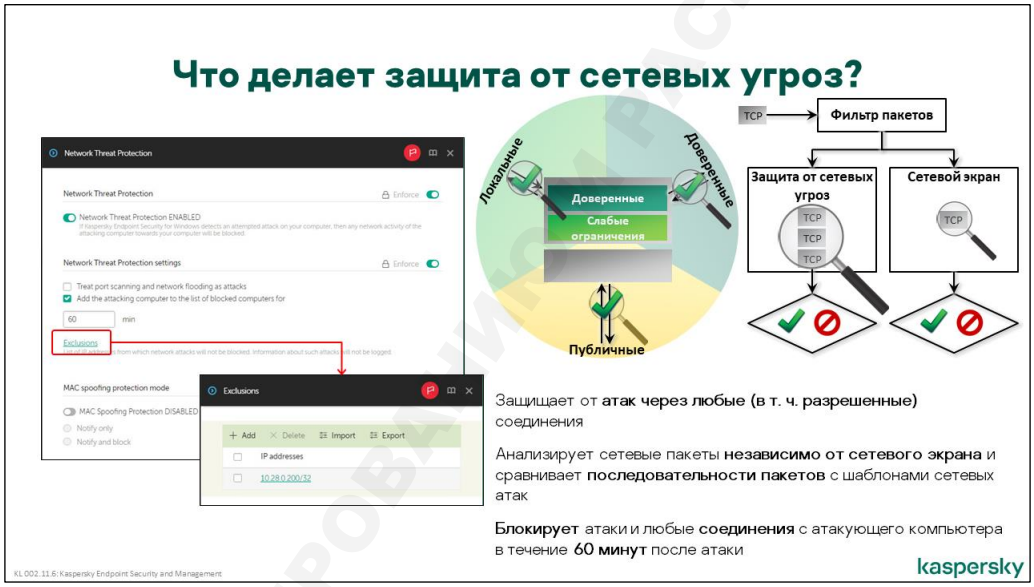
— Если файлы не подписаны сертификатом, подумайте над тем, чтобы подписать их самоподписанным сертификатом и использовать настройки исключений, чтобы доверять этому сертификату

— Или разрешите адреса и порты, которые использует программа, простыми пакетными правилами. Пакетные правила обрабатываются раньше, чем правила для программ и репутаций.

Поместите свои правила в начало списка пакетных правил

# 5.4 Зачем нужна защита от сетевых угроз

## Что делает защита от сетевых угроз




Назначение компонента Защита от сетевых угроз соответствует названию. Под сетевыми угрозами понимаются сканирование портов, атаки на отказ в обслуживании, атаки на переполнение буфера и другие способы удаленного вредоносного воздействия на программы и службы, запущенные на компьютере.

Защита от сетевых угроз работает на основании сигнатур и блокирует все соединения, которые соответствуют описаниям известных сетевых атак.

Как уже упоминалось раньше, не всегда для заражения компьютера вредоносная программа сохраняет исполняемый код в файловой системе. Например, с помощью атаки на переполнение буфера вредоносная программа может модифицировать уже загруженный в память процесс, и таким образом передать свой код на выполнение. Защита от сетевых угроз — это единственный компонент, способный предотвратить заражение по такому сценарию. Поэтому защита должна быть включена, а ее настройки должны быть обязательны.

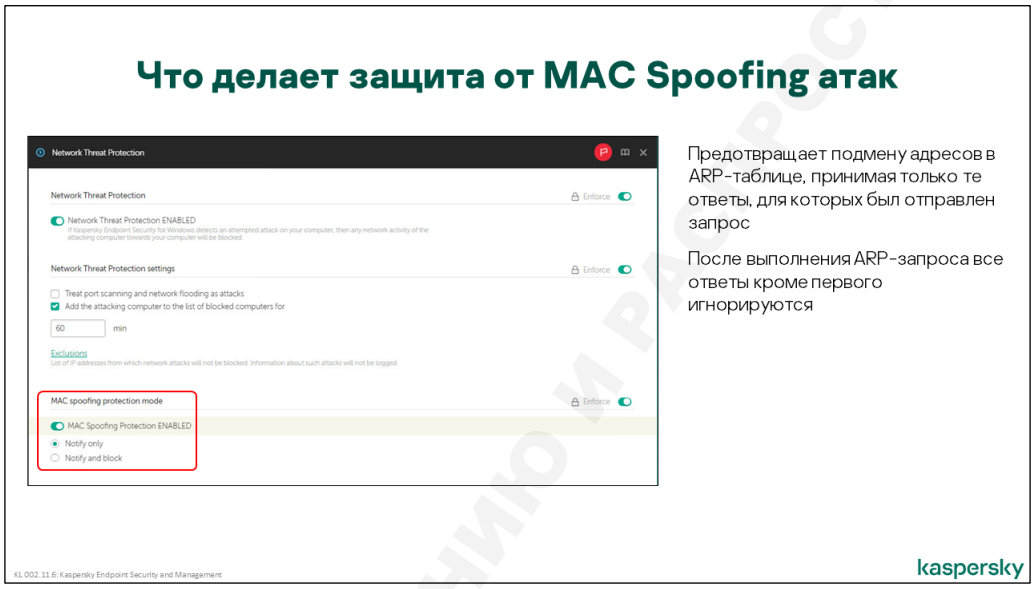
Защита от сетевых угроз практически не имеет настраиваемых параметров. Если компонент включен, то атаки блокируются автоматически.

В качестве дополнительной реакции Kaspersky Endpoint Security может блокировать все пакеты с атакующего компьютера в течение некоторого заданного времени. За это отвечает опция **Добавить атакующий компьютер в список блокирования на NN мин.**, которая по умолчанию

включена и блокирует компьютеры на 60 минут. При необходимости заблокированный компьютер можно разблокировать вручную, но только в локальном интерфейсе Kaspersky Endpoint Security.

Иногда Защита от сетевых угроз считает большое количество пакетов от камер наблюдения и других подобных устройств атакой, и блокирует пакеты. Чтобы этого избежать, добавьте адреса устройств в список исключений. Защита от сетевых угроз не будет анализировать пакеты с доверенных адресов.

## Что делает защита от MAC-спуфинга



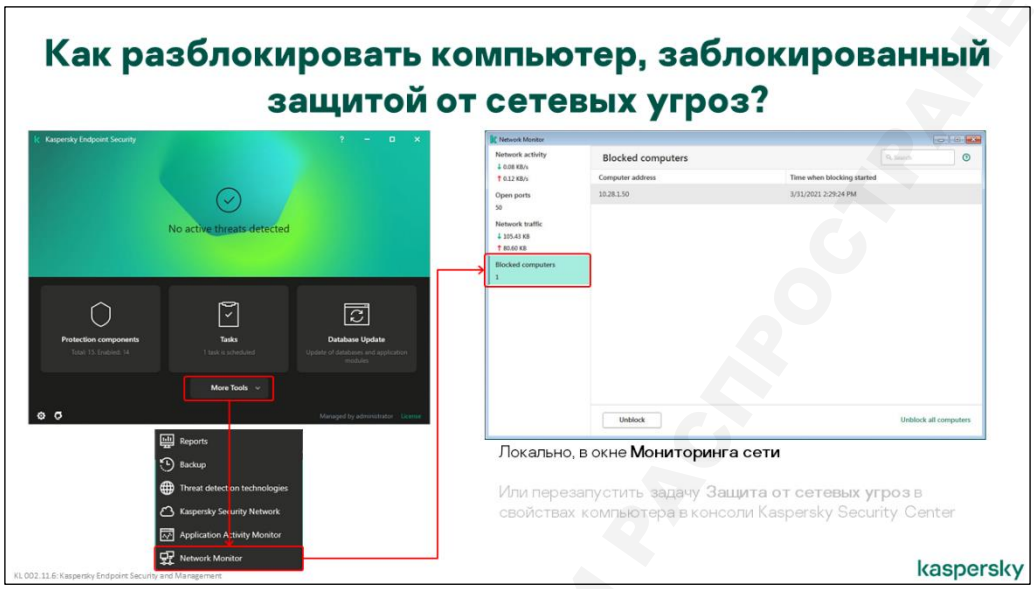

Защита от MAC-спуфинга предотвращает несанкционированную модификацию ARP-таблиц на устройствах защищенных Kaspersky Endpoint Security.

Для защиты от несанкционированной модификации ARP-таблиц используется следующие методы:

- Игнорирует входящие ARP-ответы без предварительно отправленного ARP-запроса
- В ответ на отправленный ARP-запрос, принимает только первый ARP-ответ, все остальные ARP-ответы игнорируются, данные о них записываются в журнал
- Ожидание ARP-ответа в течение определенного времени. Ответы, поступившие позже игнорируются
- Ответ на входящий ARP-запрос осуществляется без добавления записи в системную ARP-таблицу

Работа защиты от MAC-спуфинга регулируется двумя опциями в разделе **Базовая защита** | **Защита от сетевых угроз**. Защиту можно включить или выключить (по умолчанию защита выключена) и настроить реакцию на потенциально опасные атаки.

# Как разблокировать компьютер, заблокированный защитой от сетевых угроз



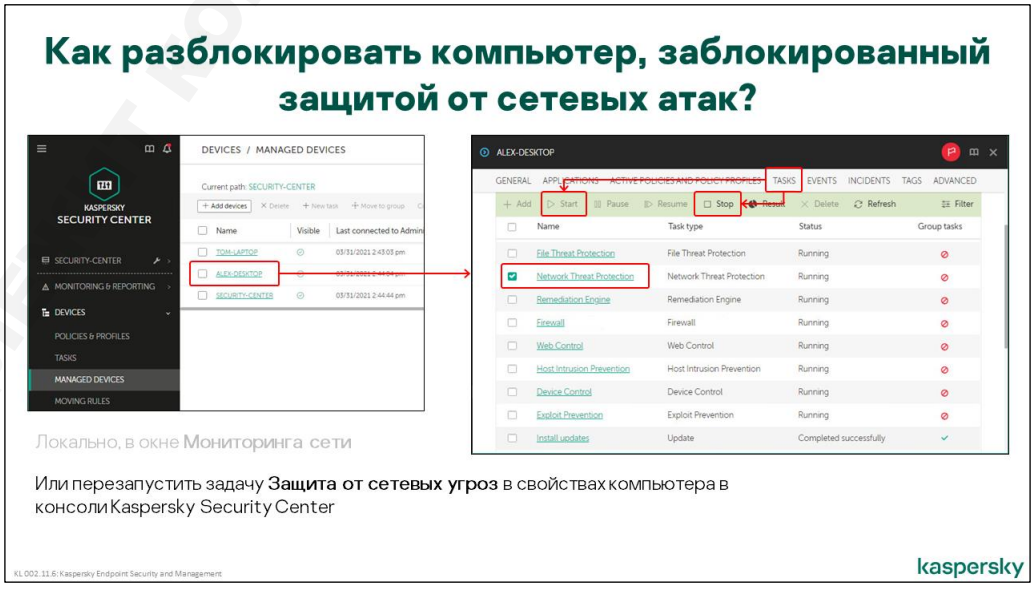

Когда один клиентский компьютер блокирует другой клиентский компьютер из-за сетевой атаки, администратор в консоли видит только событие о сетевой атаке. Ни списка заблокированных компьютеров, ни событий о том, что компьютер был заблокирован, а впоследствии разблокирован, он не видит.

Найти список заблокированных компьютеров можно в локальном интерфейсе Kaspersky Endpoint Security:

1. В окне Kaspersky Endpoint Security откройте список **Больше функций** и выберите **Мониторинг сети**

2. В окне **Мониторинга сети** выберите раздел **Заблокированные компьютеры**

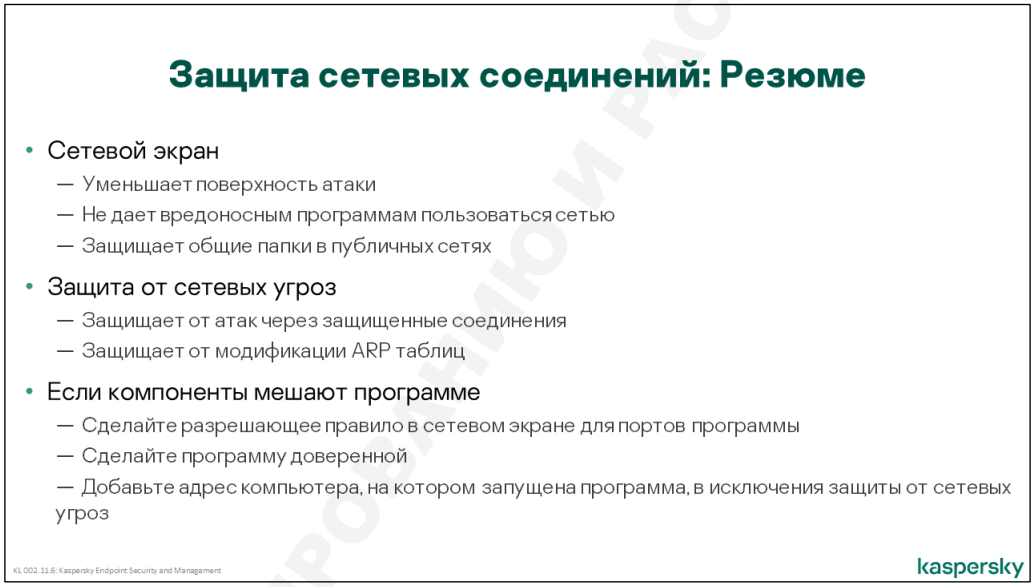
3. Чтобы разблокировать компьютер, выберите его и нажмите **Разблокировать**



Чтобы разблокировать компьютер из консоли администрирования, перезапустите компонент Защита от сетевых угроз на компьютере, который заблокировал атаку:

1. Найдите событие об атаке и посмотрите, какой компьютер сообщил о событии (а не какой компьютер атаковал)
2. Найдите этот компьютер в консоли и откройте его свойства
3. Перейдите на вкладку **Задачи** и найдите компонент **Защита от сетевых угроз**
4. Остановите компонент и запустите его (используйте контекстное меню или кнопки справа от списка)

# 5.5 Защита сети: резюме




На сетевом уровне пакеты сканируют компоненты Сетевой экран и Защита от сетевых угроз. Прочие компоненты базовой защиты (Защита от веб-угроз и Защита от почтовых угроз) проверяют данные на уровне приложений.

Сетевой экран защищает службы компьютера в публичных сетях, а также не дает пользоваться сетью недоверенным программам и программам с сильными ограничениями. Этим он не дает неизвестным вредоносным программам связываться с центром управления.

Защита от сетевых угроз анализирует последовательности пакетов в разрешенных соединениях и блокирует известные типы атак.

Если эти компоненты мешают работать программам:

- Сделайте программу доверенной для Предотвращения вторжений. Сетевой экран использует репутации программ из Предотвращения вторжений
- Разрешите порты и адреса, с которыми работает программа, простыми пакетными правилами
- Добавьте адрес программы в исключения Защиты от сетевых угроз

# 6. Как защитить компьютер за пределами сети

## 6.1 Каким локальным сетям доверять

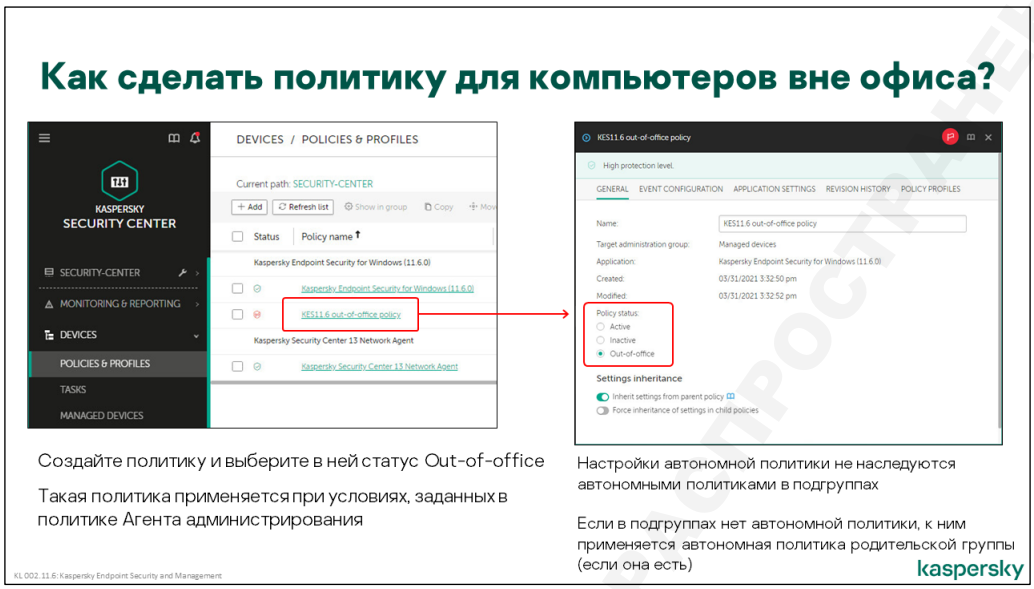

Внутри корпоративной сети компьютеры подвергаются меньшей опасности заражения, чем за ее пределами. Вполне разумно было бы менять настройки компьютеров, когда они перемещаются за пределы офиса.

В частности, политика по умолчанию считает все сети с адресами 10.0.0.0/8, 172.16.0.0/12 и 192.168.0.0/16 локальными и разрешает в них доступ к общим папкам компьютера, службам Windows и доступ к рабочему столу компьютера по протоколу RDP.

Но за пределами сети компании адреса 10.0.0.0/8, 172.16.0.0/12 и 192.168.0.0/16 могут быть у сетей отелей, кафе, аэропортов и других публичных точек доступа. Доверять им как локальным сетям опасно.

Используйте специальные политики для автономных пользователей, чтобы изменить настройки Kaspersky Endpoint Security за пределами сети компании.

# 6.2 Как создать политику для компьютеров вне офиса




Политика **Для автономных пользователей** — это третий возможный статус политики, кроме **Активная** и **Неактивная**.

Политика для автономных пользователей может быть в любой группе. Причем в группе может быть только одна политика для автономных пользователей для конкретной версии Kaspersky Endpoint Security. Распространяется такая политика точно так же, как и активная политика, но если активная политика применяется немедленно, то политика для автономных пользователей — только после выполнения специальных условий (см. ниже).

Если в дочерней группе нет своей политики для автономных компьютеров, в ней будет применяться политика для автономных пользователей ближайшей родительской группы. В то же время, если политика для автономных пользователей есть и в родительской, и в дочерней группе, между собой они никак не связаны. Какие бы параметры ни были обязательными в политике родительской группы, политику для автономных пользователей дочерней группы это никак не ограничивает.

Иными словами, отдельные настройки автономных политик не наследуются — в отличие от активных политик, где отдельные настройки, закрытые замком, наследуются политиками дочерних групп. Автономные политики наследуются только целиком — теми подгруппами, где нет своей автономной политики.

## Как сделать политику для компьютеров вне офиса

Чтобы создать политику для автономных пользователей:

1. Запустите мастер создания политики: выберите вкладку **Устройства | Политики и профили политик** и нажмите **Добавить**

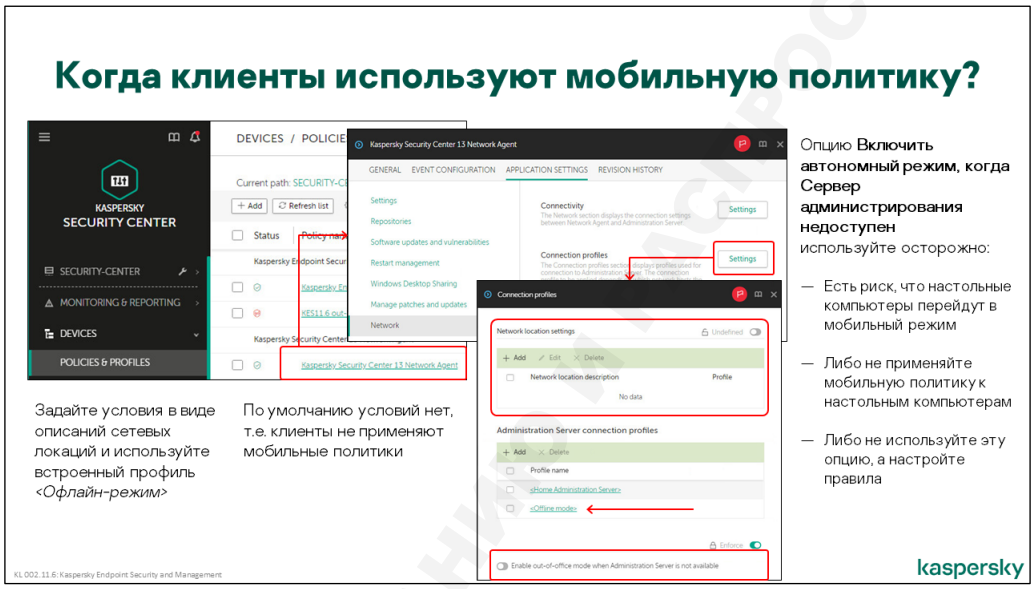
2. Выберите программу Kaspersky Endpoint Security для Windows

**Примечание**: состояние **Для автономных пользователей** есть только в политиках Kaspersky Endpoint Security для Windows. В политиках Агента администрирования или, например, Kaspersky Security для Windows Servers Enterprise Edition такой возможности нет.

3. Примите соглашение KSN
4. Дайте политике понятное имя
5. Выберите состояние политики: **Для автономных пользователей**
6. Создайте политику с настройками по умолчанию

Чтобы изменить состояние уже готовой политики, откройте раздел **Общие** в свойствах политики.

## Когда компьютеры переходят на политику для автономных пользователей




По умолчанию, компьютеры никогда не переходят на политику для автономных пользователей. Чтобы они переходили на такую политику, задайте условия в политике Агента администрирования одним из двух способов:

1. Включите параметр **Включить автономный режим, когда Сервер администрирования недоступен**

   Компьютеры будут переходить на автономную политику, если компьютер не подключен ни к какой сети, или если Агент администрирования три раза подряд не смог синхронизироваться с Сервером администрирования.

   На практике обычно это означает, что компьютер был отключен от корпоративной сети. По умолчанию период синхронизации равен 15 минутам. Следовательно, в автономный режим клиент переключится мгновенно после отключения сети или через 30–45 минут, если сеть не отключалась.

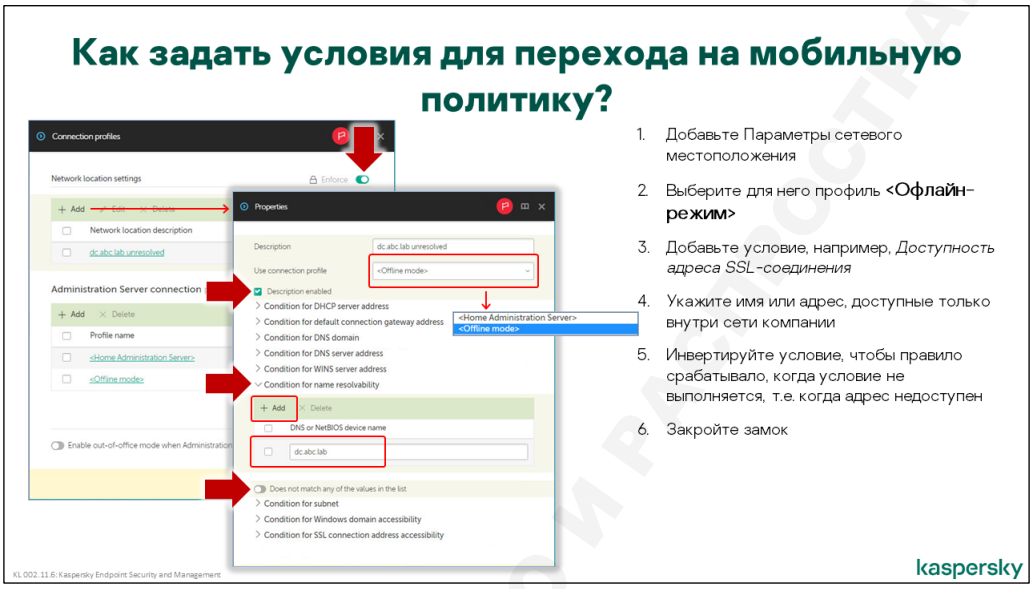
2. Настройте сетевые местонахождения для профиля *<Офлайн-режим>*

Лучше настройте сетевые местонахождения. С их помощью можно точнее описать, когда компьютер находится в сети компании, а когда нет.

Если в сети много компьютеров и Сервер администрирования перегружен, не все компьютеры смогут соединиться с Сервером при штатной синхронизации. Может оказаться так, что компьютер не синхронизируется три раза подряд и перейдет на автономную политику внутри сети компании. В зависимости от настроек автономной политики, компьютер может заблокировать доступ к своим сетевым папкам. Этим компьютером может оказаться и файловый сервер, и контроллер домена.

Конечно, если компьютеры не могут синхронизироваться с Сервером администрирования, это отдельная проблема, которую нужно решать[7]. Но неудачные условия перехода в автономный режим могут усугубить проблему.

## Как задать условия перехода на автономную политику




Вместо параметра **Включить автономный режим, когда Сервер администрирования недоступен**, настройте сетевые местонахождения, которые лучше описывают, когда компьютер находится внутри сети компании, а когда снаружи.

Агенты администрирования могут использовать разные профили соединения в разных сетевых местонахождениях. Подробнее профили описывает курс KL 302. Чтобы компьютеры перешли в автономный режим, настройте сетевые местонахождения для профиля *<Офлайн-режим>*.

В политике Агента администрирования есть разные условия для описания сетевых местонахождений. Многие из них простые и понятные, например, адрес подсети компьютера или адрес основного шлюза. Но они не могут точно определить сеть компании. Допустим, во внутренней сети используется подсеть 192.168.0.0/24. Такая же сеть может быть в отеле, в кафе или в бесплатной точке доступа на улице. Поэтому условия по адресу подсети, шлюза или DNS-сервера недостаточно надежные.

Лучше используйте **Условие для разрешимости имен** и укажите имя, которое есть только на внутреннем DNS-сервере компании. Настройте компьютеры переходить в автономный режим, когда они не могут разрешить это имя:

1. В политике Агента администрирования откройте **Параметры программы | Сеть** и в области **Профили соединений** нажмите кнопку **Параметры**

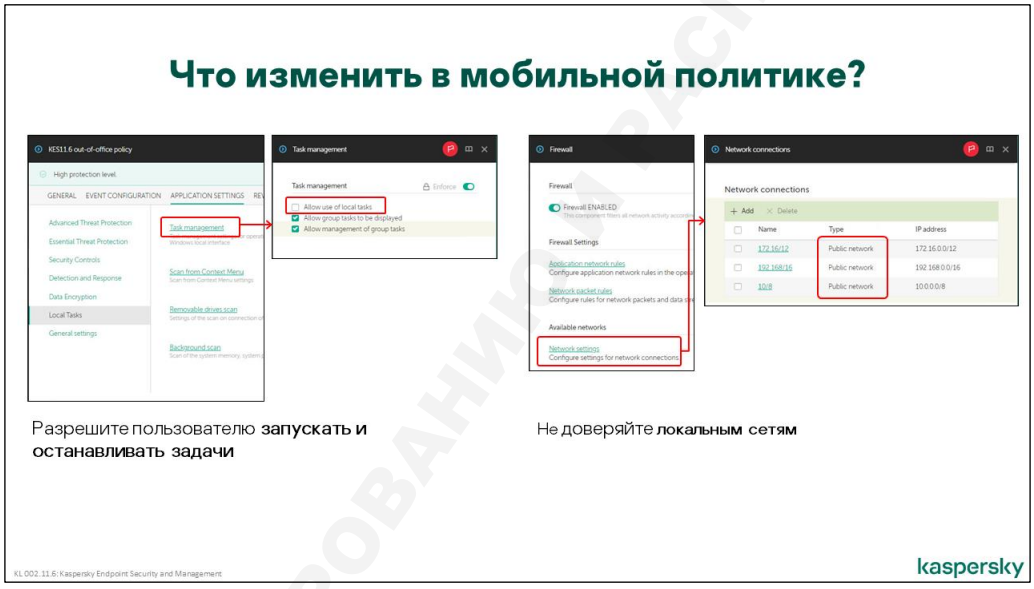
2. Добавьте параметры сетевого местоположения: нажмите кнопку **Добавить** над верхним списком

3. Дайте сетевому местонахождению понятное название, например, «*Недоступно имя <внутреннее DNS-имя>*» и включите параметр **Описание активно**

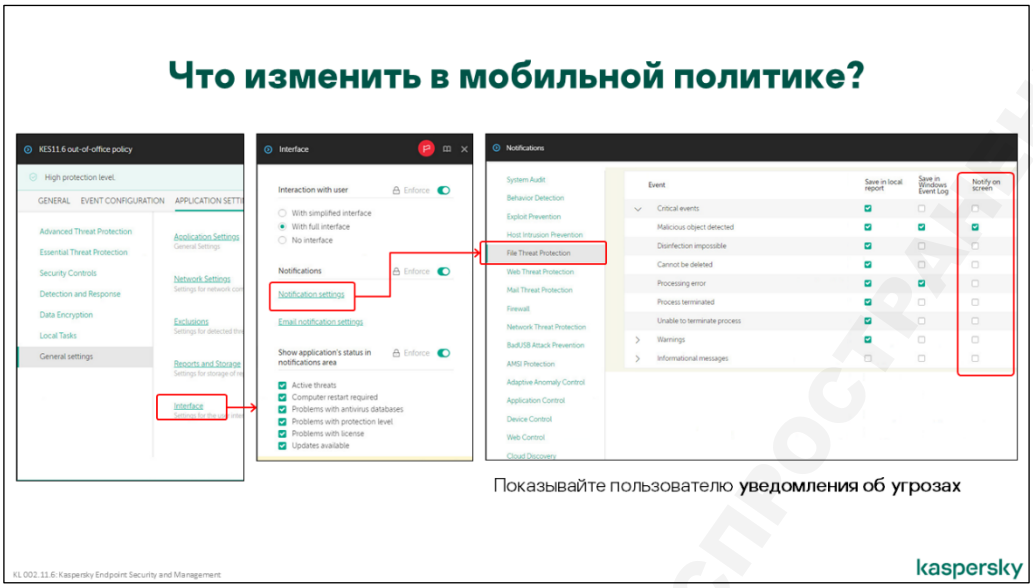
[7] Как правильно масштабировать Kaspersky Security Center в больших сетях рассказывает курс KL 302.

4. В поле **Использовать профиль подключения** выберите профиль <*Офлайн-режим*>
5. Добавьте условие типа **Условие для разрешимости имен**
6. Добавьте в список значений имя, которое разрешимо только во внутренней сети
7. Под списком **DNS- или NetBIOS-имя устройства** переключите параметр в состояние **Не соответствует ни одному из значений списка**. Это будет означать, что условие срабатывает, если указанное имя разрешить не удается
8. Сохраните условие

## 6.3 Какие настройки задать компьютерам вне офиса




Политика по умолчанию предполагает, что сети 10.0.0.0/8, 172.16.0.0/12 и 192.168.0.0/16 являются локальными, и требуют меньше ограничений. Это не обязательно будет безопасным предположением вне сети офиса. Такие адреса могут быть у сетей отелей, кафе или других публичных точек доступа и доверять им нельзя. Сделайте эти сети публичными в автономной политике. Или, если вы доверяете пользователям, удалите все сети из политики: Сетевой экран будет смотреть на статусы сетей в операционной системе, а их может выбирать пользователь компьютера.




Политика для автономных компьютеров должна учитывать тот факт, что компьютер находится не в корпоративной сети, и что обслуживанием Kaspersky Endpoint Security вынужденно занимается пользователь. Соответственно, такая политика должна давать пользователю необходимый доступ к информации о состоянии защиты и к инструментам управления Kaspersky Endpoint Security. Как минимум стоит дать пользователю возможность выполнять проверку подозрительных файлов и носителей, а также запускать обновление. Для этого нужно разрешить пользователю управлять групповыми или локальными задачами, или и теми, и другими. Соответствующие настройки ищите в политике в разделе **Локальные задачи**.

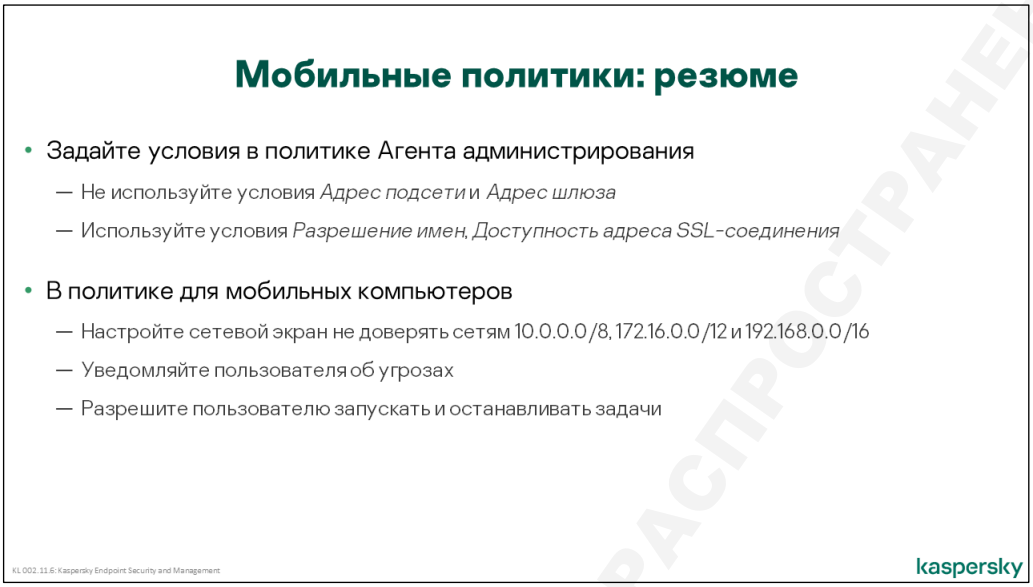
Чтобы помочь пользователю принимать рациональные решения, касающиеся защиты, нужно дать ему возможность получать больше информации об инцидентах. Пользователя стоит уведомлять об угрозах, необходимости лечения активного заражения и об устаревших базах

— Откройте список локальных событий Kaspersky Endpoint Security в разделе **Параметры программы | Общие настройки | Интерфейс** политики (ссылка *Настройка уведомлений* в области **Уведомления**)

— Выберите компонент и установите флаг напротив важных для пользователя событий в колонке **Уведомлять на экране**

Предупреждайте пользователя о проблемах Kaspersky Endpoint Security красным треугольником на значке в панели уведомлений. Выберите, о каких проблемах сообщать пользователю, в разделе **Предупреждения** политики.

# 6.4 Автономные политики: резюме




Если пользователи работают за пределами сети компании, им нужны другие настройки Kaspersky Endpoint Security. Специально для этого в Kaspersky Security Center есть политики для автономных пользователей.

По умолчанию, политики для автономных пользователей не используются. Чтобы они использовались, настройте условия в политике Агента администрирования. Настройте сетевые местонахождения для профиля <*Офлайн-режим*>. В описаниях сетевых местонахождений укажите условия, которые надежно описывают, когда компьютер в сети компании, а когда нет. Используйте условия типа *Изменить условие для разрешимости имен* и *Изменить условия для доступности адреса SSL-соединения*.

В политике для автономных пользователей усильте настройки защиты:

— Настройте сетевой экран не доверять сетям 10.0.0.0/8, 172.16.0.0/12 и 192.168.0.0/12

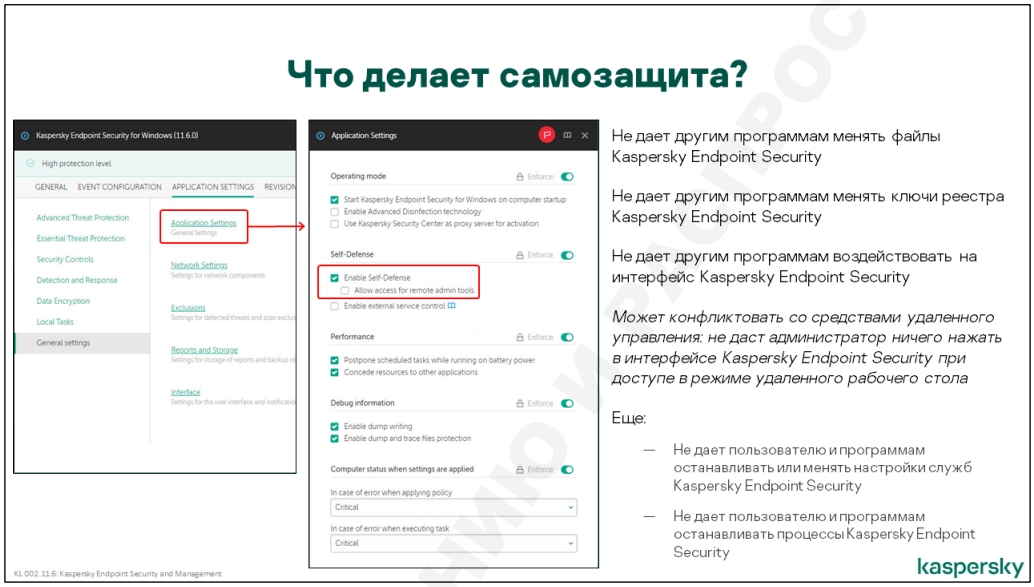
Дайте пользователям больше информации и контроля над Kaspersky Endpoint Security:

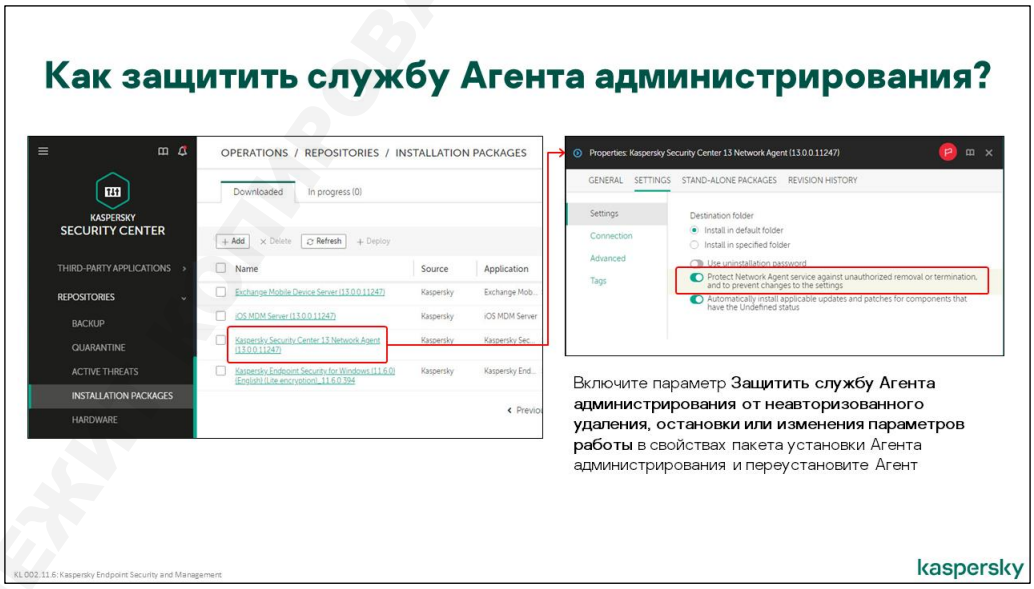
— Сообщайте об угрозах на экране компьютера
— Сигнализируйте о проблемах на иконке в области
— Разрешите пользователю запускать и останавливать задачи

# 7. Что еще есть в защите и зачем

## 7.1 Что делает и зачем нужна самозащита

### Что делает самозащита




В Kaspersky Endpoint Security реализована технология самозащиты, предотвращающая несанкционированное отключение продукта и другие попытки нарушить его нормальное

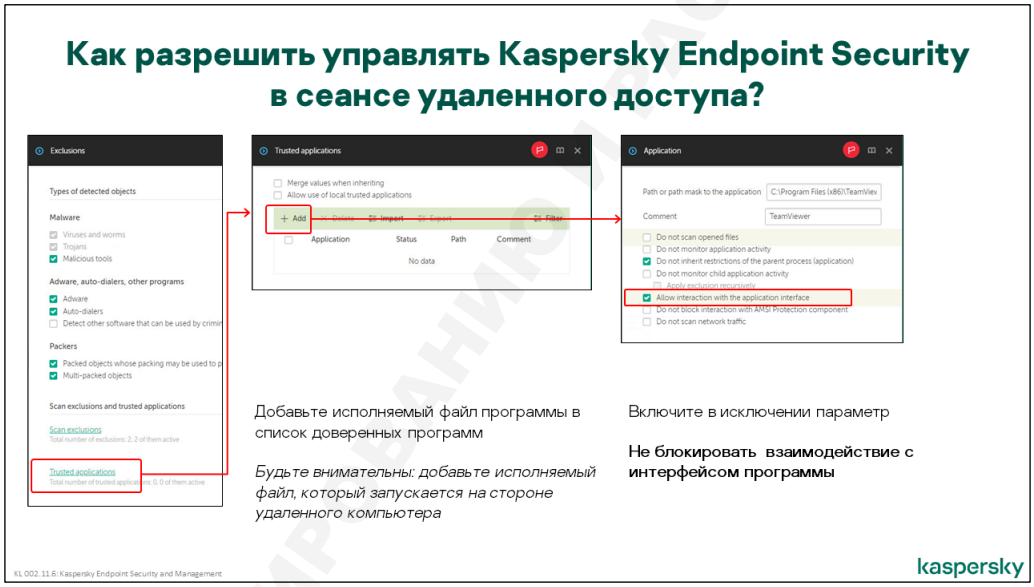
функционирование. Работа самозащиты регулируется двумя опциями в разделе **Общие настройки | Параметры программы | Настройки программы**:

— Параметр **Включить самозащиту** отвечает за защиту процессов Kaspersky Endpoint Security в оперативной памяти компьютера, его исполняемых и вспомогательных файлов на жестком диске и ключей в реестре системы

— Опция **Выключить возможность внешнего управления системными службами** не дает остановить службы[8] Kaspersky Endpoint Security, кроме как через интерфейс продукта

Отключение самозащиты понижает уровень защиты компьютера, поэтому по умолчанию оба параметра включены и являются обязательными. Отключать самозащиту следует только при наличии проблемы совместимости с другими приложениями (например, утилитами удаленного управления, хотя для устранения этой проблемы есть лучшие решения) или при поиске неисправностей на управляемом компьютере.

## Как управлять KES в сеансе удаленного доступа




Чтобы вредоносные программы не выключали защиту, имитируя команды пользователя в окне продукта, самозащита по умолчанию принимает события мыши и клавиатуры только непосредственно от устройств, а не от других процессов. Поэтому, когда администратор пытается управлять Kaspersky Endpoint Security через программу удаленного доступа, такую как UltraVNC или TeamViewer, самозащита не дает ничего нажать в окне Kaspersky Endpoint Security.

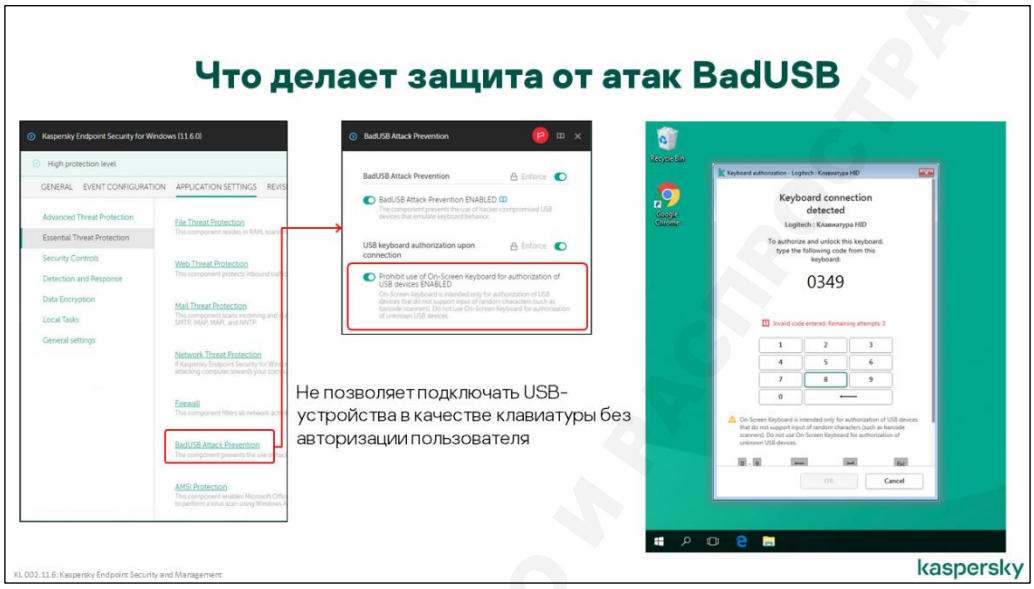
Если вам нужно управлять Kaspersky Endpoint Security, через программу удаленно доступа, а самозащита не дает этого делать, настройте исключение. Добавьте исполняемый файл средства удаленного доступа, который работает на управляемых компьютерах, в список доверенных программ.

Процесс, который запускает администратор у себя на компьютере, не обязательно совпадает с процессом на удаленном компьютере, который принимает соединение и дает доступ к рабочему столу. Добавляйте именно процесс, который работает на удаленном компьютере

[8] У Kaspersky Endpoint Security есть две службы: собственно Kaspersky Endpoint Security (avp.exe) и Kaspersky Seamless Update Service (avpsus.exe)

В свойствах доверенной программы включите флаг **Не блокировать взаимодействие с интерфейсом программы**. Остальные флаги отключите. Не разрешайте программам больше, чем им нужно для работы.

## Что делает защита от атак BadUSB




Прошивка любой флэшки может быть модифицирована. При подключении к компьютеру, такая флэшка, может опознаваться операционной системой как другое устройство и скрытно выполнять ряд функций, предусмотренных злоумышленником. Например, флэшка может опознаваться как клавиатура и отправлять команды от имени вошедшего в систему пользователя. На практике, это могут быть совершенно любые действия: скрытая загрузка вредоносной программы или перехват и отправка конфиденциальных данных. И даже если пользователь не обладает правами Администратора в системе, это не решит проблему, так как существуют различные способы повышения привилегий, а прав обычного пользователя обычно хватает, чтобы организовать утечку данных.

Компонент Защита от атак BadUSB не позволяет подключаться USB-устройствам в качестве клавиатуры без авторизации пользователем. Происходит это следующим образом, при подключении USB-устройства, если оно опознается операционной системой как клавиатура, Защита от атак BadUSB вводит пользователю уведомление и просит пользователя авторизовать устройство.

По умолчанию компонент **Защита от атак BadUSB** не устанавливается на компьютеры. При необходимости, его можно до установить с помощью задачи Kaspersky Endpoint Security **Смена состава компонентов**. Компонент **Защита от атак BadUSB** рекомендуется устанавливать на ноутбуки.

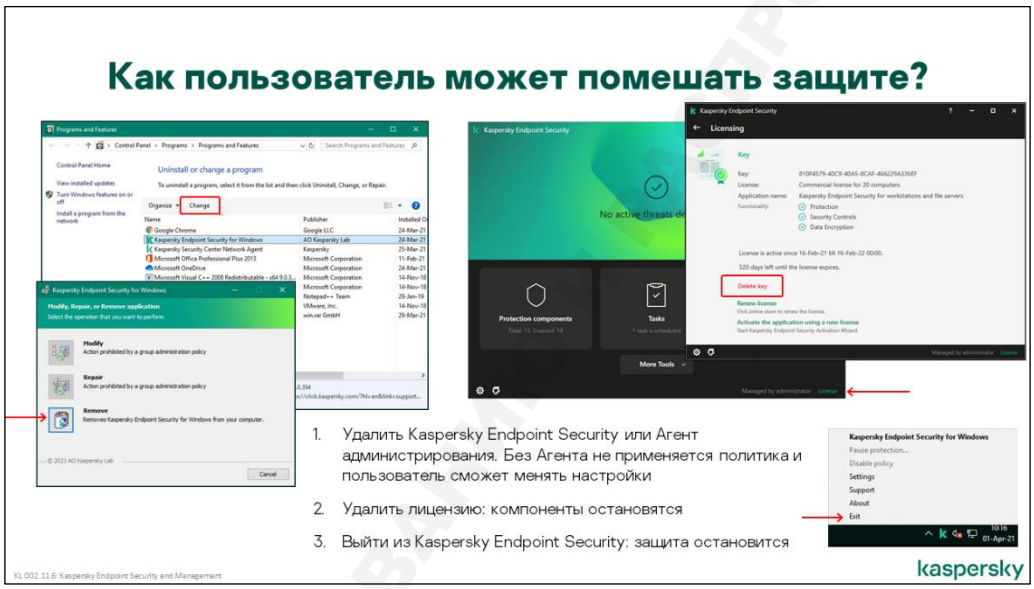
Работа защиты от атак BadUSB регулируется двумя параметрами в разделе **Параметры программы | Базовая защита | Защита от атак BadUSB**:

- Параметр **Защита от атак BadUSB** может иметь два состояния **Включена** или **Выключена**, по умолчанию защита включена
- Параметр **Заперт на использование экранной клавиатуры для USB-устройств** позволяет пользователю воспользоваться экранной клавиатурой для авторизации устройства. По умолчанию, запрещено использование экранной клавиатуры

Если планируется использование защиты от атак BadUSB на ноутбуках. Рекомендуется, в политике для автономных пользователей разрешить использование экранной клавиатуры, чтобы избежать проблем с авторизацией беспроводных пультов и презентеров.

# 7.2 Как защитить Kaspersky Endpoint Security от пользователя

## Как пользователь может остановить защиту



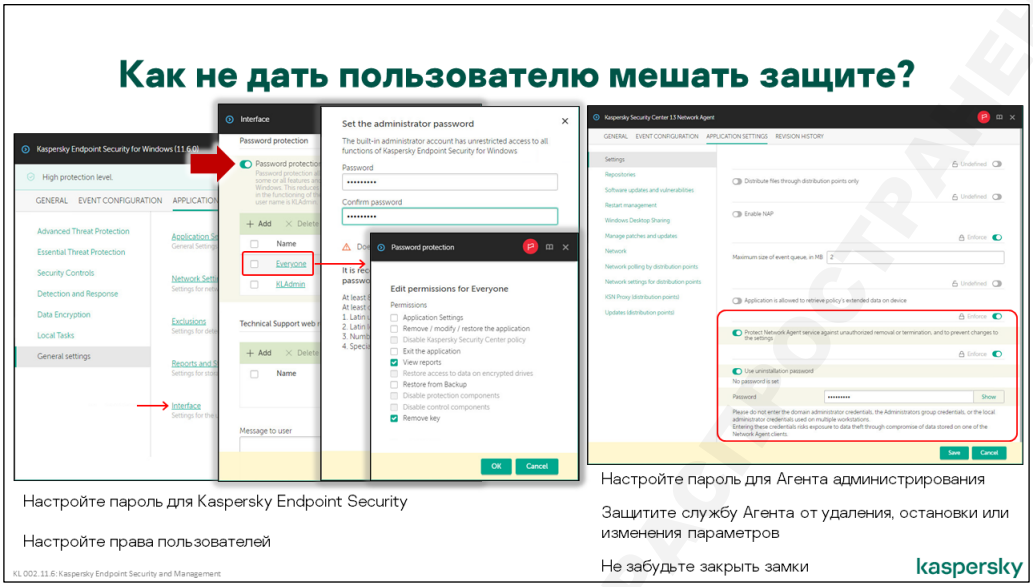

Настройки по умолчанию оставляют пользователю как минимум две возможности отключить защиту:

- Закрыть Kaspersky Endpoint Security командой **Выход** в контекстном меню иконки в области уведомлений. Этот способ не требует даже повышения привилегий, он доступен любому пользователю.
- Деинсталлировать Kaspersky Endpoint Security, что требует наличия у пользователя прав администратора. Но у некоторых пользователей, особенно пользователей ноутбуков, эти права могут быть.

Чтобы не дать пользователям ослаблять или совсем останавливать Kaspersky Endpoint Security, настройте защиту паролем для упомянутых действий в политике, и сделайте нужные настройки обязательными (то есть закройте замок). Дополнительно самозащита Kaspersky Endpoint Security будет блокировать попытки выгрузить из памяти процессы приложения или удалить его файлы с диска.

Еще один, менее очевидный способ отключить защиту — деинсталлировать Агент администрирования. Спустя 10–20 минут после удаления Агента администрирования, Kaspersky Endpoint Security выходит из-под действия политики и пользователю становятся доступны все его настройки. Агент администрирования тоже можно защитить паролем, и эта возможность по умолчанию тоже не включена.

# Как включить защиту паролем




Защита паролем может распространяться на большинство действий пользователя в отношении Kaspersky Endpoint Security: изменение настроек, отключение, деинсталляция.

Чтобы включить защиту паролем Kaspersky Endpoint Security:

1. Откройте политику на вкладке **Параметры программы**, в разделе **Общие настройки | Интерфейс,** переключите параметр **Защита паролем** в состояние **Включена**

2. Задайте пароль

3. Настройте разрешения для группы **Everyone.** Выберите, какие операции не потребуют от пользователя ввести пароль:

   — **Настройка программы** — защищает все параметры Kaspersky Endpoint Security, в том числе и опции включения компонентов, но не ограничивает возможность остановки компонентов через их контекстное меню

   — **Удаление / изменение / восстановление программы** — добавляет в мастер деинсталляции Kaspersky Endpoint Security запрос пароля

   — **Выключение политики Kaspersky Security Center** — добавляет в контекстное меню иконки Kaspersky Endpoint Security команду временного отключения политики по паролю

   — **Завершение работы программы** — запрашивает пароль при использовании команды **Выход**. От попыток завершить работу Kaspersky Endpoint Security нештатным способом защищает самозащита

   — **Просмотр отчетов** — требует пароль, перед тем как показать события в локальном интерфейсе Kaspersky Endpoint Security

> Пароль защищает и графический интерфейс Kaspersky Endpoint Security и интерфейс командной строки.

— **Восстановление доступа к данным на зашифрованных устройствах** — использовать средства восстановления зашифрованной информации должен администратор, а не пользователь

— **Восстановление из резервного хранилища** — требует пароль, при восстановлении файлов из резервного хранилища

— **Выключение компонентов защиты** — не запрещает запускать компоненты защиты и локальные задачи, если они отображаются, и запрашивает пароль только при попытке остановить. Для задачи обновления аналогичной опции нет

— **Выключение компонентов контроля** — ставить пароль на отключение контроля устройств, контроля программ, веб-контроля

Эта возможность удобна для администраторов при локальной диагностике проблем. Политика не дает менять локальные параметры, что мешает диагностике. Но перемещать проблемный компьютер в отдельную группу на время диагностики и затем возвращать его назад — неудобно. Особенно если за централизованное управление защитой отвечает одно подразделение ИТ, а за локальную диагностику — другое. Возможность временно отключать политику по паролю на отдельном компьютере позволяет выполнять диагностику, не меняя общих настроек на Сервере администрирования.

— **Удаление ключа** — пользователь, не зная пароля, не сможет остановить защиту, удалив лицензию вручную

Защита паролем хороша тем, что действует, даже когда политика отключена. После того как настройки защиты паролем применились к Kaspersky Endpoint Security, даже если администратор отключит политику, пользователь не сможет управлять защитой, не зная пароля. Защита паролем позволяет настроить отдельные права каждому пользователю или группе пользователей.

## Настройка защиты паролем для Агента администрирования

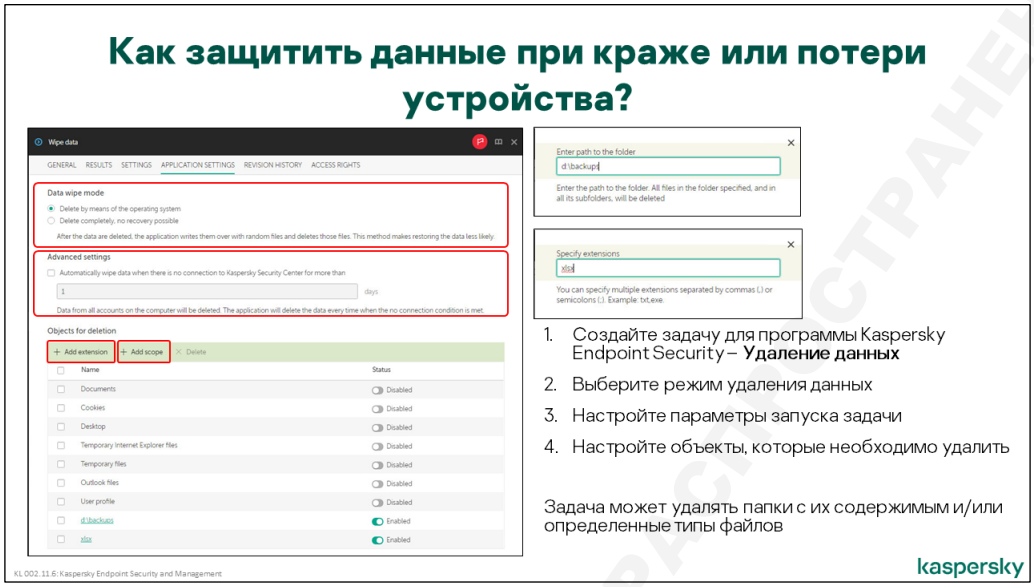
Агент администрирования не так заметен в системе, как Kaspersky Endpoint Security. Одно из немногих мест, где его можно увидеть — список установленных программ. Слово «*Kaspersky*» в названии продукта может спровоцировать некоторых пользователей на попытку удалить Агент администрирования. Если пользователь обладает правами администратора, он сможет это сделать.

Чтобы защитить Агент администрирования, задайте пароль на деинсталляцию в его политике. Политику Агента администрирования создает мастер первоначальной настройки.

Пароль для деинсталляции Агента администрирования относится к разделу **Параметры**. В стандартной конфигурации пароль не задан и не является обязательным. Включите опцию **Использовать пароль деинсталляции**, задайте пароль и закройте замок этой группы настроек.

После применения политики, в мастер деинсталляции Агента администрирования добавляется окно с запросом пароля. Попытка удалить Агент через командную строку, не указав пароль, также завершится неудачно.

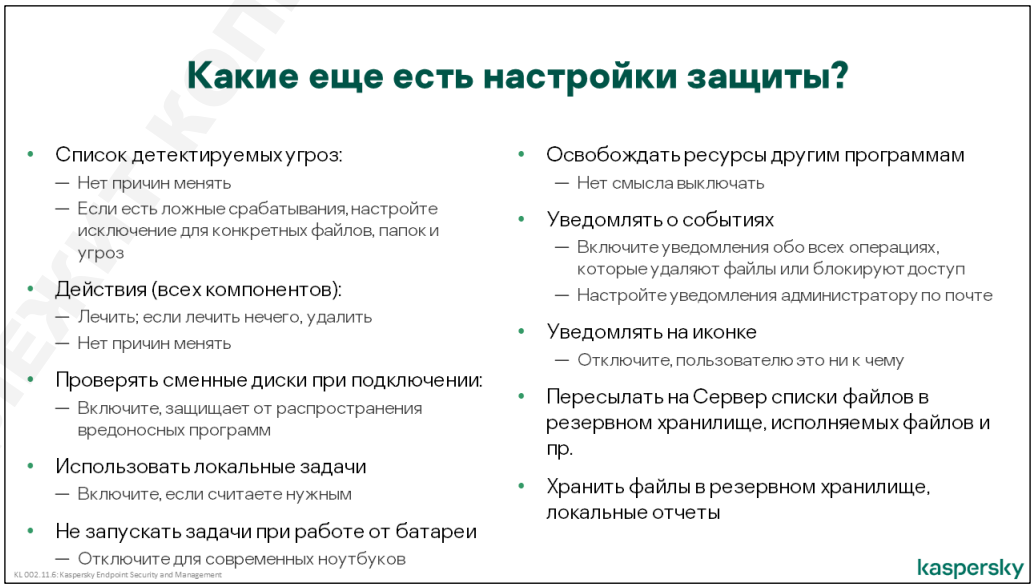
## Как защитить данные при краже или потери устройства




Kaspersky Endpoint Security имеет ряд инструментов, позволяющих защитить данные пользователей при краже и потере устройства. Одним из таких инструментов является задача **Удаление данных**.

Данная задача позволяет Администратору удалять данные пользователя – папки и/или файлы заданных расширений – либо средствами операционной системы, либо перезаписывая данные случайными без возможности восстановления. Задача может быть запущена вручную по желанию Администратора или автоматически при отсутствии связи с Kaspersky Security Center более **X** дней.

# 7.3 Какие еще есть настройки защиты



В политике Kaspersky Endpoint Security больше настроек, чем мы рассмотрели в этой части.

## Действия

У большинства компонентов защиты можно выбрать, как поступать с вредоносными файлами и другими угрозами.

По умолчанию все компоненты пытаются лечить вредоносные файлы, а если лечение не удается или не предусмотрено, удаляют их. Администратор может выбрать сразу удалять все вредоносные файлы, или не удалять вредоносные файлы, а только блокировать. Блокировать, но не удалять стоит, только если вы что-то тестируете. На защищенных компьютерах используйте действие, которое удаляет вредоносные файлы. Лучше просто оставьте действие по умолчанию.

Перед тем как лечить или удалять, Kaspersky Endpoint Security копирует файл в **Резервное хранилище**. Это специальная папка на компьютере, где Kaspersky Endpoint Security хранит зашифрованные копии вредоносных программ. Если Kaspersky Endpoint Security удалил файл по ошибке, администратор сможет восстановить его из **Резервного хранилища**, после того как настроит исключение.

## Остальные настройки

Нерассмотренные настройки, как правило, нет причин менять. Что они делают, написано в справке к Kaspersky Endpoint Security. Краткое описание некоторых настроек дает таблица:

| Общие настройки \| Исключения \| Объекты для обнаружения | |
|---|---|
| **Вирусы, черви (нельзя выключить)** | Не меняйте эти настройки |
| **Троянские программы (нельзя выключить)** | Все эти объекты как минимум мешают пользователю, а как максимум наносят серьезный ущерб |
| **Вредоносные утилиты (включено)** | Если администраторы используют для тестов утилиты, которые считаются вредоносными, настройте для них исключения, но не выключайте всю категорию объектов |
| **Рекламные программы (включено)** | |
| **Программы автодозвона (включено)** | |
| **Другие (выключено)** | К категории **Другие** относятся утилиты удаленного управления, такие как RAdmin, UltraVNC, DameWare и другие. Злоумышленники могут использовать эти легитимные средства для несанкционированного доступа к компьютерам. Но ими же могут санкционированно пользоваться администраторы и пользователи компании. Включайте на свое усмотрение. |
| **Упакованные файлы, которые могут нанести вред (включено)** | |
| **Многократно упакованные файлы (включено)** | |
| **< Имя компонента> \| Действие при обнаружении угрозы** | |
| **Лечить** | Не меняйте настройки действий. Пусть компоненты удаляют все вредоносные объекты |
| **Удалять, если лечение невозможно** | При ложных срабатываниях настраивайте исключения. Ошибочно удаленные файлы восстанавливайте из Резервного хранилища после того, как настроили исключение |
| **Локальные задачи \| Проверка съемных дисков** | |
| **Действие при подключении съемного диска: (по умолчанию) не проверять** | Измените действие на **Быстрая проверка** или **Подробная проверка** |
| **Максимальный размер съемного диска: (по умолчанию) 4096 МБ** | Хотя Защита от файловых угроз проверит все, что пользователь запустит или скопирует со съемного диска, лучше не оставлять на съемных дисках вредоносные файлы в пассивном состоянии. Пользователь может прийти с этим диском к клиенту и случайно заразить компьютер |

| | |
|---|---|
| | Чтобы пользователи не ждали слишком долго, пока Kaspersky Endpoint Security проверит большой диск, установите максимальный размер на свое усмотрение, например в 32 МБ |
| **Локальные задачи \| Управление задачами** | |
| **(По умолчанию) Выключено** | Не включайте. Локальными задачами сложно управлять с Сервера администрирования, и они запутывают администратора<br>Если вам нужно, чтобы пользователи могли сами запускать обновление или останавливать поиск вирусов, лучше включите параметр **Разрешить управление групповыми задачами** в этом же списке |
| **Общие настройки \| Параметры программы \| Производительность \| Откладывать задачи по расписанию при работе от аккумулятора** | |
| **(По умолчанию) Включено** | Многие современные ноутбуки могут работать от аккумулятора около 10 часов и даже дольше. Откладывать поиск вирусов и тем более обновление до тех пор, пока пользователь не подключит ноутбук к электросети, может быть опасно. Для таких компьютеров опцию отключите.<br>В то же время старые ноутбуки могут быть не предназначены для длительной автономной работы и именно для них был введен этот параметр. Разделите старые и новые ноутбуки в разные группы и задайте им подходящие настройки через отдельные политики. |
| **Общие настройки \| Параметры программы \| Производительность \| Уступать ресурсы другим программам** | |
| **(По умолчанию) Включено** | Не выключайте |
| **Общие настройки \| Отчеты и хранение \| Отчеты** | |
| **Хранить отчеты не более: (по умолчанию) 30 дней**<br>**Максимальный размер файла: (по умолчанию) 1024 МБ** | Большинству компаний достаточно истории событий в 30 дней<br>Если вам нужно хранить события дольше, увеличьте время хранения и максимальный размер файлы<br>Подумайте о том, чтобы пересылать события в SIEM-систему (см. курс KL 009) |
| **Общие настройки \| Отчеты и хранение \| Резервное хранилище** | |
| **Хранить объекты не более: (по умолчанию) 30 дней**<br>**Максимальный размер хранилища: (по умолчанию) не задан** | Если вы подозреваете, что файл вредоносный, но Kaspersky Endpoint Security на него не реагирует, получите его репутацию из KSN в реальном времени или отправьте файл в техническую поддержку через портал *companyaccount.kaspersky.com* |
| **Общие настройки \| Отчеты и хранение \| Передача данных на Сервер администрирования** | |
| **О файлах резервного хранилища**<br>**О необработанных файлах**<br>**Об установленных устройствах**<br>**О запускаемых программах**<br>**Об ошибках шифрования** | Первые два списка включите: они сообщают об угрозах и ложных срабатывания<br>Списки устройств и ошибок шифрования пересылайте, если используете контроль устройств и шифрование.<br>Список запускаемых файлов пересылайте только с отдельных компьютеров, не включайте его для всей сети |
| **Общие настройки \| Интерфейс \| Правила уведомлений \| Компонент \| <Событие>** | |
| **Сохранять в локальном журнале**<br>**Сохранять в журнале событий Windows**<br>**Уведомлять на экране**<br>**Уведомлять по почте** | Храните в локальном журнале все события<br>В журнале Windows храните как минимум сообщения о сбоях, чтобы увидеть их, если Kaspersky Endpoint Security не работает<br>Уведомлять на экране оставьте только для событий контроля. Чем меньше пользователь видит сообщений от Kaspersky Endpoint Security, тем лучше |

| | |
|---|---|
| | Не настраивайте уведомления по почте здесь |
| **Общие настройки \| Интерфейс \| Взаимодействие с пользователем** | |
| **Отображать полный интерфейс программы: по умолчанию включено**<br>**Упрощенный интерфейс программы: по умолчанию выключено** | Выберите *Без интерфейса*, если пользователи жалуются на то, что Kaspersky Endpoint Security мешает работать<br>Если политика компании не разрешает полностью скрывать интерфейс программы защиты от пользователей, включите С *упрощенным интерфейсом*: пользователи будут видеть иконку Kaspersky Endpoint Security в области уведомлений, но не смогут открыть главное окно программы и понять, какие компоненты и задачи запущены |
| **Общие настройки \| Интерфейс \| Предупреждения** | |
| **Наличие активных угроз**<br>**Необходимость перезагрузки компьютера**<br>**Проблемы с базами сигнатур**<br>**Проблемы с уровнем защиты**<br>**Проблемы с лицензией**<br>**Наличие обновлений** | Выключите на компьютерах внутри сети. Проблемы нужно видеть администратору, а не пользователю, и в консоли администрирования, а не в локальном интерфейсе<br>Включите в политике для автономных пользователей, чтобы пользователи ноутбуков сами обслуживали защиту |

## Защита компьютера: резюме


Все компоненты защиты в Kaspersky Endpoint Security или обнаруживают и блокируют угрозы, или уменьшают поверхность атаки, т.е. не дают пользователю и программам делать потенциально опасные вещи на компьютере.

Поэтому, не выключайте компоненты защиты. Вместо этого создавайте исключения для тех программ, которые работают медленно.

Настройте регулярный поиск вирусов. Во-первых, он обнаруживает пассивные угрозы. Во-вторых, он обновляет кэш проверенных файлов, и после него *Защита от файловых угроз* и другие компоненты работают быстрее.

Все компоненты приносят пользу с настройками по умолчанию. Как правило, эти настройки тяжело улучшить, и поэтому не стоит менять. Но чтобы лучше защитить компьютеры от программ вымогателей, настройте *Предотвращение вторжений* защищать документы.

Настройки по умолчанию можно улучшить для ноутбуков, которые работают не в сети компании. Создайте для них политику для автономных пользователей.

Наконец, защищайте не только компьютеры от вредоносных программ, но и Kaspersky Endpoint Security от пользователей. Задайте пароль для Kaspersky Endpoint Security и Агента администрирования.