002.11.6

Kaspersky Endpoint Security and Management

Часть III. Контроль

kaspersky

Учебный курс

Содержание

1. Общие сведения

1.1 Назначение компонентов контроля

Кроме защиты от вредоносных программ, в Kaspersky Endpoint Security входят инструменты для контроля действий, которые могут нанести ущерб пользовательским компьютерам или компании в целом.

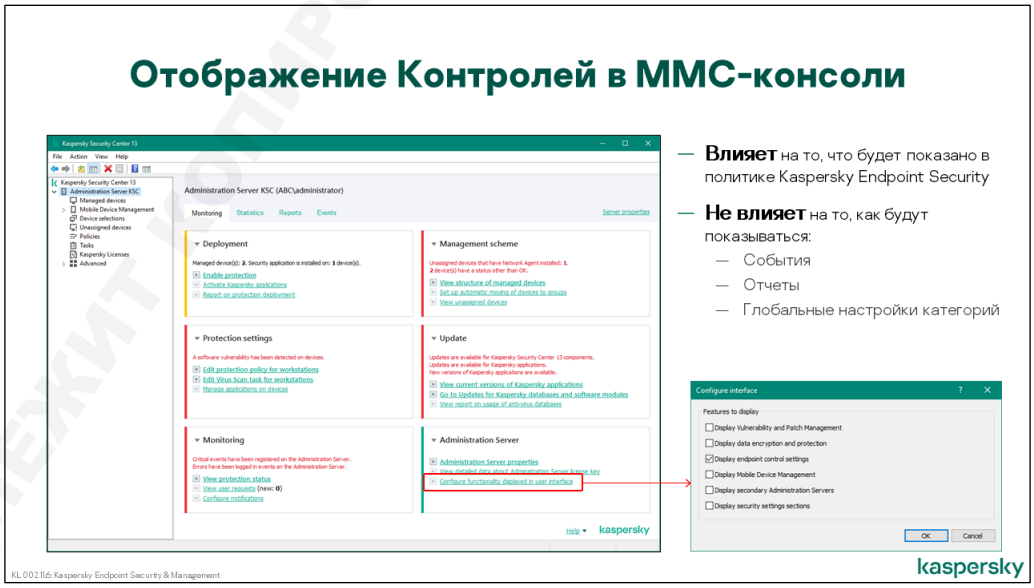
- **Контроль программ** позволяет отслеживать попытки запуска программ пользователем и регулировать запуск программ с помощью правил
- **Контроль устройств** контролирует подключение внешних устройств в соответствии с политикой компании. Входящий в состав компонент **Анти-Бриджинг** запрещает установку несанкционированных коммутаций между сетями
- **Веб-Контроль** ограничивает доступ к веб-ресурсам в зависимости от их содержания и расположения
- **Адаптивный контроль аномалий** содержит набор предустановленных правил и отслеживает нетипичное поведение на устройстве, которое чаще всего предшествует заражению, и позволяет блокировать такого рода активность

1.2 Лицензии и типы установки

В Kaspersky Security Center выделяется пять функциональных областей:

- Защита от угроз
- Компоненты контроля
- Шифрование
- Управление системами
- Управление мобильными устройствами

Компоненты контроля требуют лицензию уровня KESB *Стандартный* и устанавливаются по умолчанию. Исключение составляет новый компонент **Адаптивный контроль аномалий**, который так же устанавливается по умолчанию, но требует лицензию уровня KESB *Расширенный.*



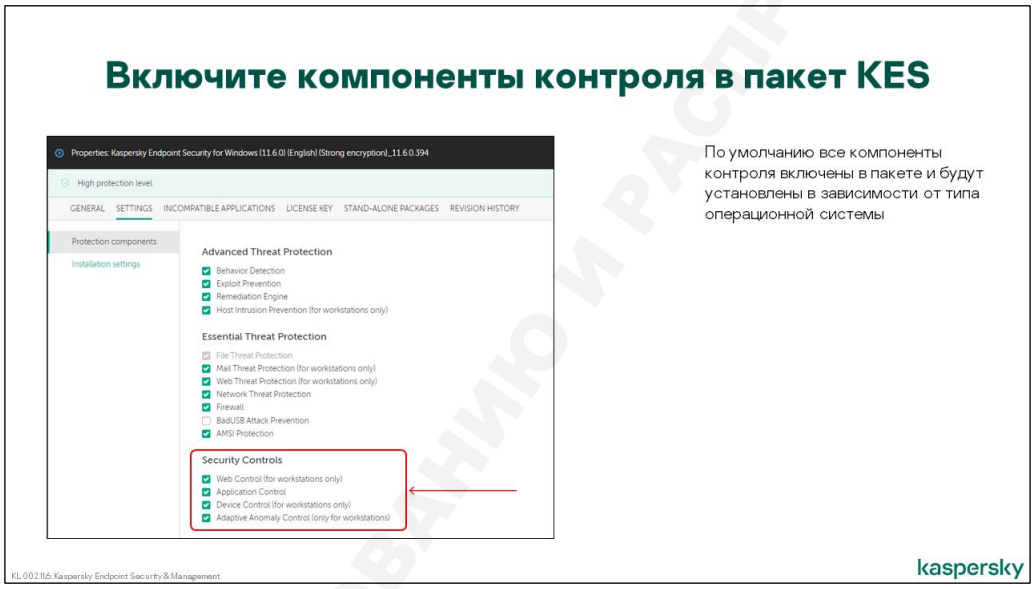
В MMC-консоли в политике Kaspersky Endpoint Security по умолчанию не отображаются настройки Шифрования и компонентов Контроля. Включить отображение этих настроек можно в главном окне

Консоли по ссылке **Настроить функциональность, отображаемую в пользовательском интерфейсе**:

- Отображать шифрование и защиту данных – отображает настройки Шифрования
- Отображать параметры контроля рабочего места – отображает настройки компонентов Контроля

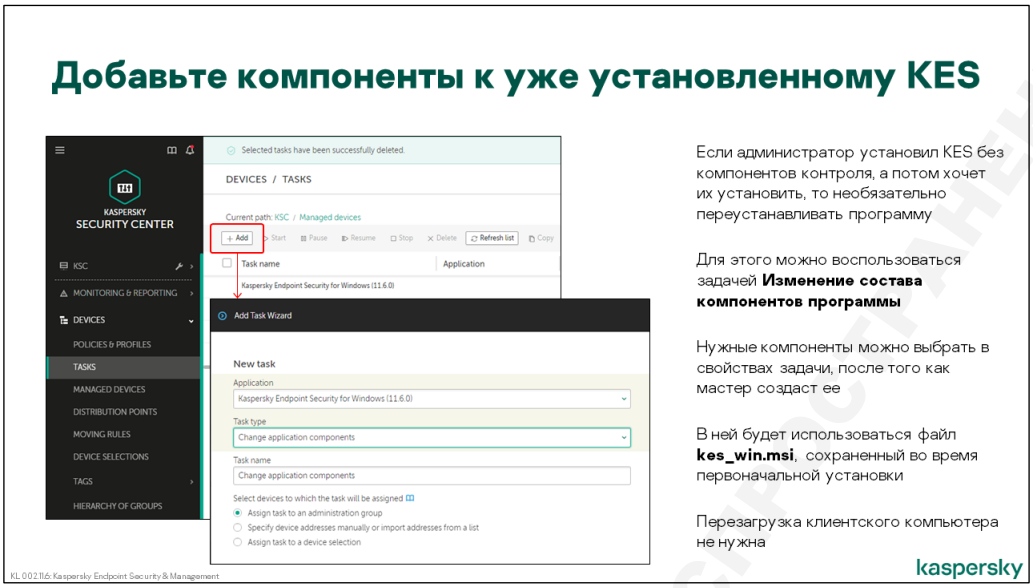
В веб-консоли никаких дополнительных настроек для отображения элементов интерфейса делать не нужно, весь возможный функционал доступен сразу.

1.3 Установка компонентов контроля



Компоненты контроля по умолчанию включены в свойствах пакета Kaspersky Endpoint Security, который создается автоматически при установке Сервера администрирования.

Единственный нюанс это при установке на серверную операционную систему, не все компоненты будут там установлены.



Если так случилось, что на компьютерах установлен не полный набор компонентов, и нужно установить дополнительные компоненты, у администратора есть возможность это сделать.

Нужно использовать задачу **Изменение состава компонентов программы**, относящуюся к Kaspersky Endpoint Security 11.6. Эта задача предназначена как раз для того, чтобы удалять или добавлять компоненты Kaspersky Endpoint Security без полной переустановки продукта. Эта задача практически не создает нагрузки на сеть, т.к. использует **.msi**-пакет Kaspersky Endpoint Security, который сохраняется на клиентском компьютере во время первоначальной установки.

В свойствах задачи, точно так же, как в инсталляционном пакете, можно выбрать список необходимых компонентов. Исключение мастер создания задачи, где выбор отдельных компонентов недоступен. Чтобы выбрать отдельные компоненты нужно завершить мастер создания задачи и открыть свойства задачи, где выбор компонентов не ограничен.

2. Контроль программ

Контроль программ нужен для воплощения политики безопасности компании в части, которая касается запуска программ на клиентских компьютерах. Одновременно **Контроль программ** снижает риск заражения компьютера, уменьшая поверхность атаки.

2.1 Как работает контроль программ

Принцип работы

Контроль программ позволяет администратору установить ограничения на запуск программ на клиентских компьютерах. Разрешения на запуск программ устанавливают с помощью правил.

При запуске любой программы **Контроль программ** анализирует:

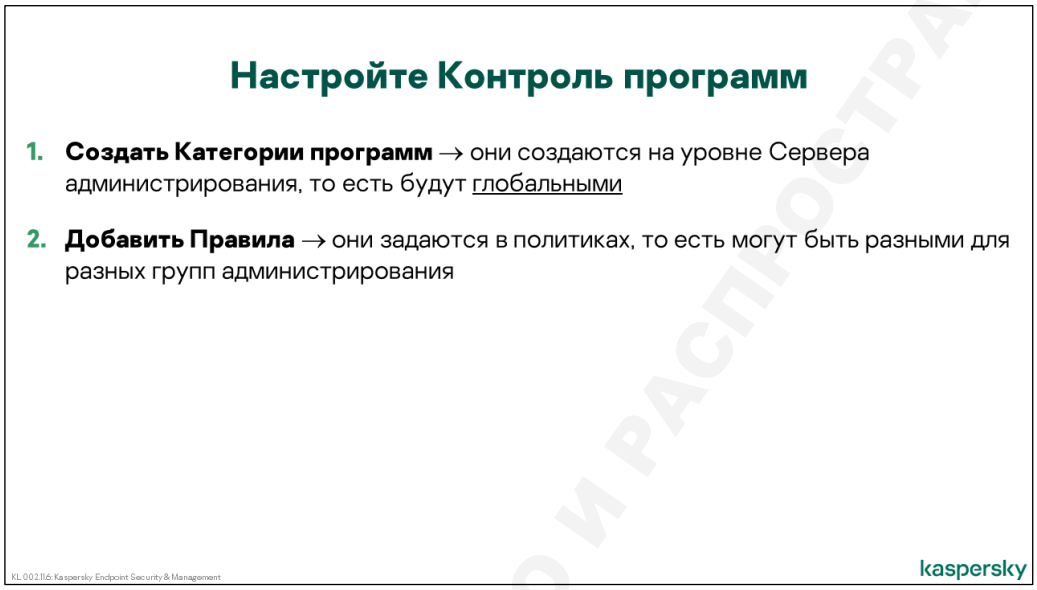
- К какой категории относится программа (категории задаются администратором)
- Учетная запись, от имени которой выполняется запуск программы
- Есть ли в политике Kaspersky Endpoint Security правила, регулирующие запуск этой категории для этой учетной записи

Далее анализирует, в каком режиме работает **Контроль программ**:

- **Запрещающий список**: по умолчанию разрешается все. Блокируются только программы, которые входят в категории, которые администратор запретил запускать в политике Kaspersky Endpoint Security. То есть если запрещающего правила нет, программа запустится
- **Разрешающий список**: по умолчанию запрещается все. Разрешаются только программы, которые входят в категории, которые администратор разрешил запускать в политике Kaspersky Endpoint Security. То есть если разрешающего правила нет, программа заблокируется

Режим разрешающего списка используется в подходе запрет по умолчанию (Default Deny). О нем будет рассказано в отдельном разделе этой главы, и намного подробней — в одноименном отдельном учебном курсе.

Как настроить Контроль программ



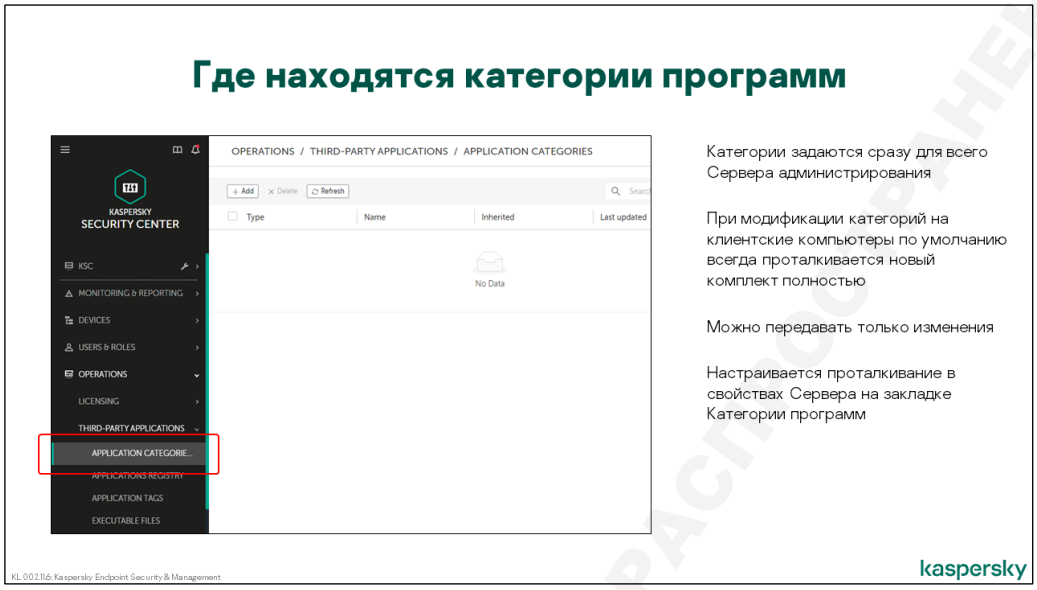
В два этапа:

1. Задать категории программ:
   1.1. Составить список категорий. Например, Веб-браузеры, Игры, Сторонние мессенджеры, Разрешенные программы, и т. п.
   1.2. Все программы, которыми мы хотим управлять, распределить по этим категориям. Тому, как это сделать, посвящен весь следующий раздел.

   Категории задаются один раз и сразу для всего Сервера администрирования во вкладке **Операции | Программы сторонних производителей | Категории программ**
2. Составить список правил. Для каждой категории программ в политике Kaspersky Endpoint Security можно выставить, что Kaspersky Endpoint Security должен делать с входящими в эту категорию программами:
   — разрешать,
   — запрещать,
   — просто уведомлять Kaspersky Security Center о запуске.

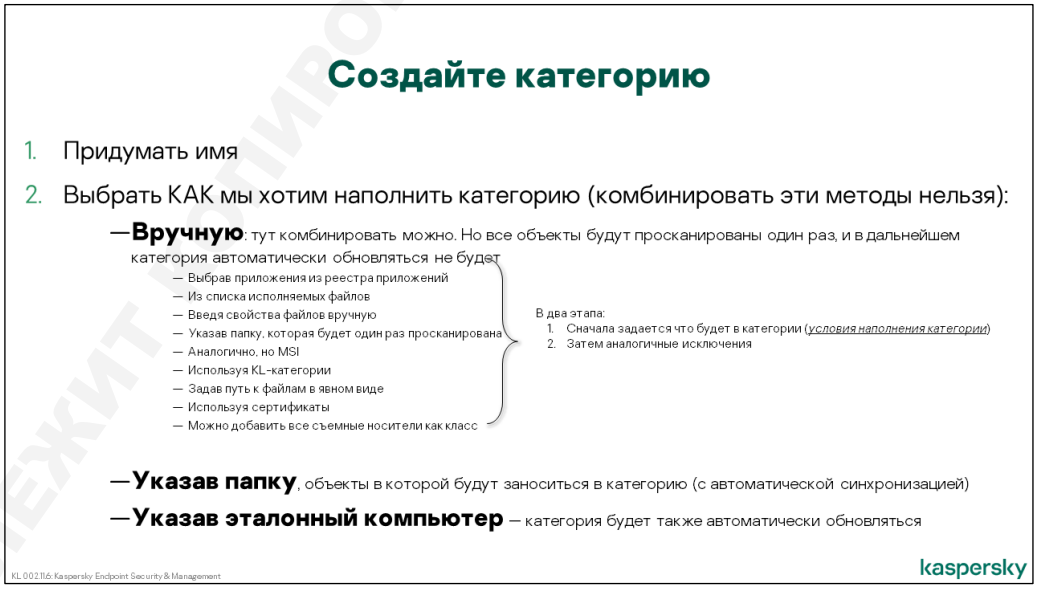
Обратите внимание, что категории задаются для всего сервера, а правила могут быть разными для каждой группы компьютеров. Например, один и тот же Skype можно по умолчанию запретить всем, но отдельным привилегированным пользователям разрешить. При этом маркетологам разрешить Skype, но каждый раз, когда они будут его запускать, администратору будет отправляться уведомление.

2.2 Как задать категории программ



Категории создаются на Сервере администрирования Kaspersky Security Center и аналогично политикам и задачам передаются на клиентские компьютеры. Можно передавать каждый раз полный список и содержание категорий, а можно только изменения. Это задается в свойствах Сервера администрирования на закладке **Категории программ**.

Опция передачи только изменений появилась, начиная с Kaspersky Security Center 10 SP2, в более ранних версиях Kaspersky Security Center при любом самом мелком изменении всегда передается полный комплект категорий), поэтому по умолчанию передается все — потому что, если в сети есть более старые клиенты, они не смогут получить только изменения, и не получат ничего.



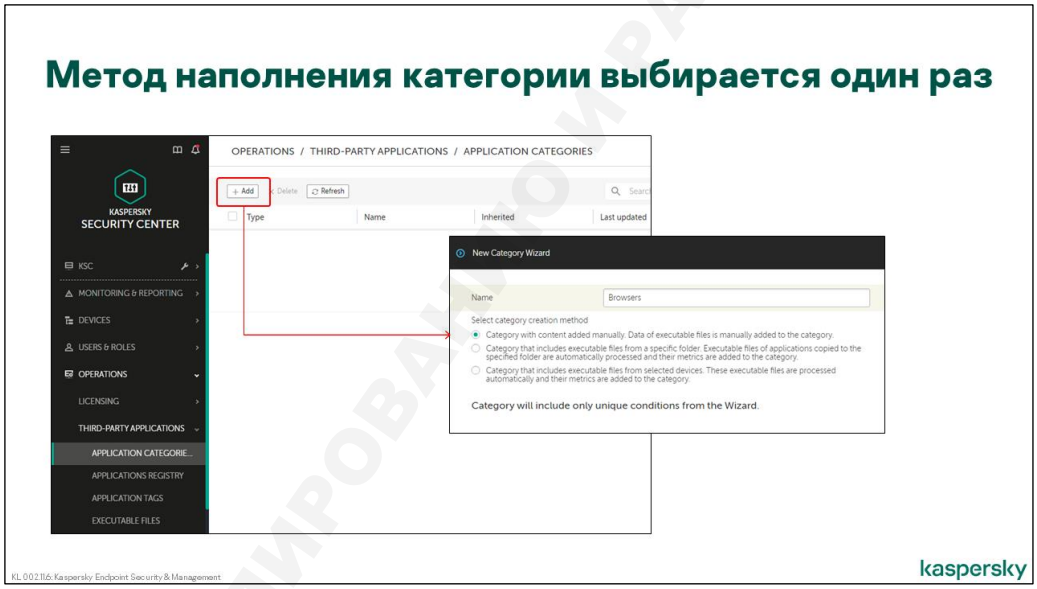
Категория программ — это набор условий и исключений, позволяющих идентифицировать программу или группу программ. Список отображается во вкладке **Операции | Программы**

сторонних производителей | Категории программ и по умолчанию пуст. Новые категории создаются с помощью отдельного мастера и бывают трех видов:

— **Наполняемые вручную** — условия для включения программ в категорию добавляются и изменяются только вручную. Например, все программы со строкой «zombies» в названии, или все программы, подписанные определенным сертификатом

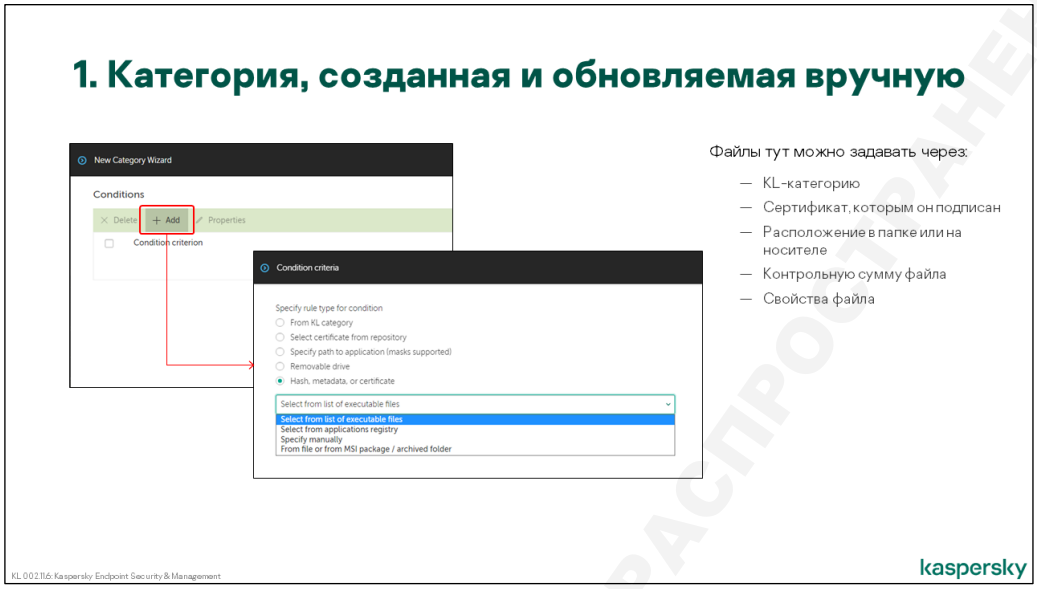
— **Наполняемые автоматически из папки** — администратор выбирает каталог, который сканируется на наличие файлов следующих форматов: EXE, COM, DLL, SYS, BAT, PS1, CMD, JS, VBS, REG, MSI, MSC, CPL, HTML, HTM, DRV, OCX, SCR. После чего Сервер администрирования по расписанию перепроверяет каталог, вычисляет контрольные суммы исполняемых файлов SHA256 и/или MD5 и обновляет список условий в категории. Удобно, когда в сети есть папка, куда копируются все запрещенные или наоборот, разрешенные программы

— **Наполняемые автоматически с выбранных устройств** — администратор выбирает один или несколько управляемых компьютеров, а Сервер администрирования автоматически заносит в категорию все исполняемые файлы, найденные на устройстве. То есть можно задать эталонный компьютер, на котором находятся, например, все разрешенные программы



На первом шаге мастер создания категории просит задать имя категории и выбрать метод наполнения. В дальнейшем, если метод наполнения не устраивает и нужно его изменить, то придется создавать категорию заново.

Категория, созданная и обновляемая вручную



Для категории, наполняемой вручную, условия для программ задаются в виде списка, при этом каждое условие может содержать несколько параметров. Если программа соответствует хотя бы одному условию, считается, что она принадлежит к категории. Условия можно задавать разными способами, но все они сводятся к следующим видам.

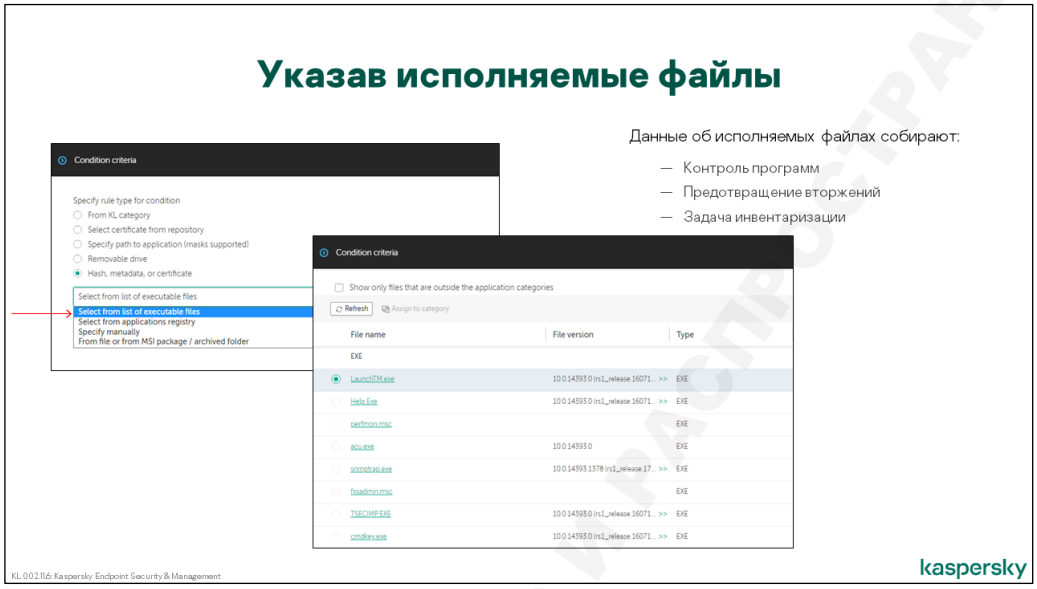
- **KL-категория** — разрешающие списки группируются специалистами Лаборатории Касперского в категории в соответствии с назначением и классификацией программ. Каталог категорий позволяет определить, к какой категории относится программа или отдельный файл. В большинстве случаев Kaspersky Endpoint Security определяет категорию локально, используя базу сигнатур или запрашивает вердикт в Kaspersky Security Network
- **Сертификат** — функция доступна начиная с Kaspersky Endpoint Security 10 SP2. Можно указать папку на клиентском устройстве, которая содержит исполняемые файлы, подписанные сертификатами. Сертификаты исполняемых файлов считываются и добавляются в условия категории. Или можно добавить сертификаты из хранилища сертификатов
- **Папка программы** — все программы из указанной папки будут добавлены в категорию
- **Съемный диск** — специальный параметр, который позволяет выделять в отдельную категорию файлы, которые запускаются со сменного носителя
- **Метаданные** — имя файла, его версия, название программы и производителя. Указывать версию не обязательно точно. Можно выбрать все файлы, старше или младше определенной версии. Различные характеристики файла являются частями одного условия, а не отдельными условиями. Указывая метаданные можно разрешать только подписанные действительным сертификатом файлы, или те, для которых KSN вернет доверительный вердикт
- **Контрольная сумма** — результат применения к файлу функции SHA-256

Примечание: в версии Kaspersky Endpoint Security 10 SP1 MR3, и более ранних, для идентификации файлов в Контроле программ вместо SHA-256 использовалась MD5 сумма. Начиная с Kaspersky Endpoint Security 10 SP2 используется только SHA-256.

Если в сети есть разные версии Kaspersky Endpoint Security, нужно в свойствах категории отметить соответствующий флаг — например, собирать не только SHA-256, но и MD5 суммы тоже. Тогда одну и ту же категорию можно будет использовать для политик разных версий Kaspersky Endpoint Security.

А если категории программ получаются объемные, можно создать разные категории для разных версий Kaspersky Endpoint Security.

Указав исполняемые файлы

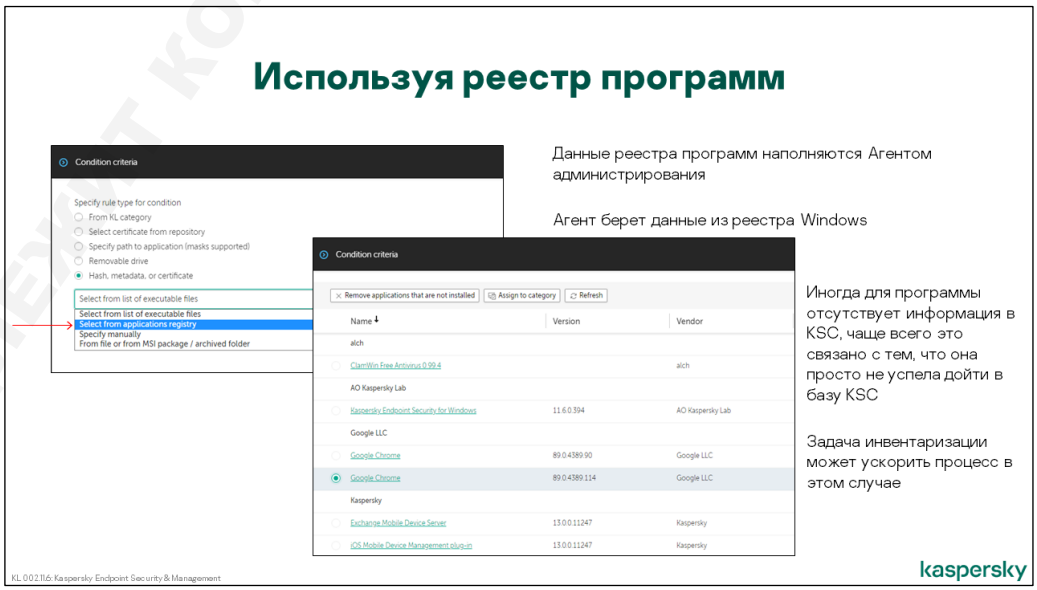


Администратор может создавать условия на основе **Списка исполняемых файлов**. Это список исполняемых файлов, которые когда-либо были запущены на клиентских компьютерах или обнаружены задачей **Инвентаризация**.

Примечание: В Kaspersky Endpoint Security 11.6 информация о запускаемых исполняемых файлах начинает передаваться только после включения компонента Контроль программ.

Список уже обнаруженных файлов отображается во вкладке **Операции | Программы сторонних производителей | Исполняемые файлы**.

Используя реестр программ



В контейнер **Реестр программ** попадают программы, которые считаются установленными на компьютере и отображаются в оснастке Программы и компоненты. Названия и атрибуты этих программ собирают Агенты администрирования и передают Серверу администрирования. Собранная информация об установленных программах не включает сведений о том, какие исполняемые файлы относятся к этим программам, но именно сведения об исполняемых файлах нужны, чтобы создать условие. Для этого Сервер администрирования сопоставляет сведения об установленных программах и сведения об исполняемых файлах, обнаруженных на компьютерах, после чего создает условия на базе хэш-сумм исполняемых файлов, относящихся к выбранной установленной программе.

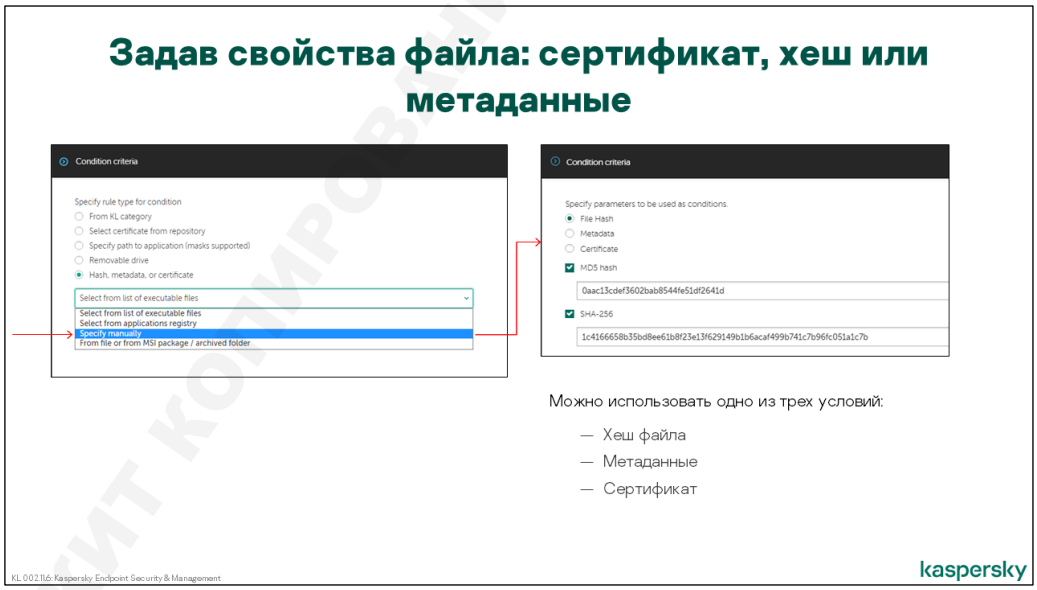
При этом бывает так, что программа числится установленной по ошибке, или программа установлена, но запускается крайне редко и данные об ее исполняемых файлах на Сервере администрирования отсутствуют.

В этом случае администратор может получить сообщение о невозможности создать условие для этой программы. С другой стороны, если у программы несколько исполняемых файлов, использование реестра программ упрощает создание правил. Сервер администрирования автоматически добавляет условия для всех исполняемых файлов, ассоциированных с программой.

В случае если программа установлена, но ее исполняемые файлы еще не переданы на Сервер администрирования, администратор может запустить задачу **Инвентаризация**, чтобы ускорить процесс.

Подробней задачу инвентаризации рассмотрим чуть позже.

Задав свойства файла



Выбирая файл на диске, администратор может задать для него простое условие на базе SHA-256 (MD5), или более гибкое условие на базе метаданных или сертификата.

Хэш-суммой идентифицируется один и только один файл. Такое условие удобно, если важно точное совпадение. Например, в автоматически наполняемых категориях, рассмотренных выше, используются хэш-суммы, потому что важно разрешить запуск именно тех версий файлов, которые установлены на эталонном компьютере или входят в одобренный дистрибутив. Любое изменение в файле в результате действий вредоносных программ или пользователей приведет к изменению хэш-суммы и к тому, что запуск файла больше не будет разрешен.

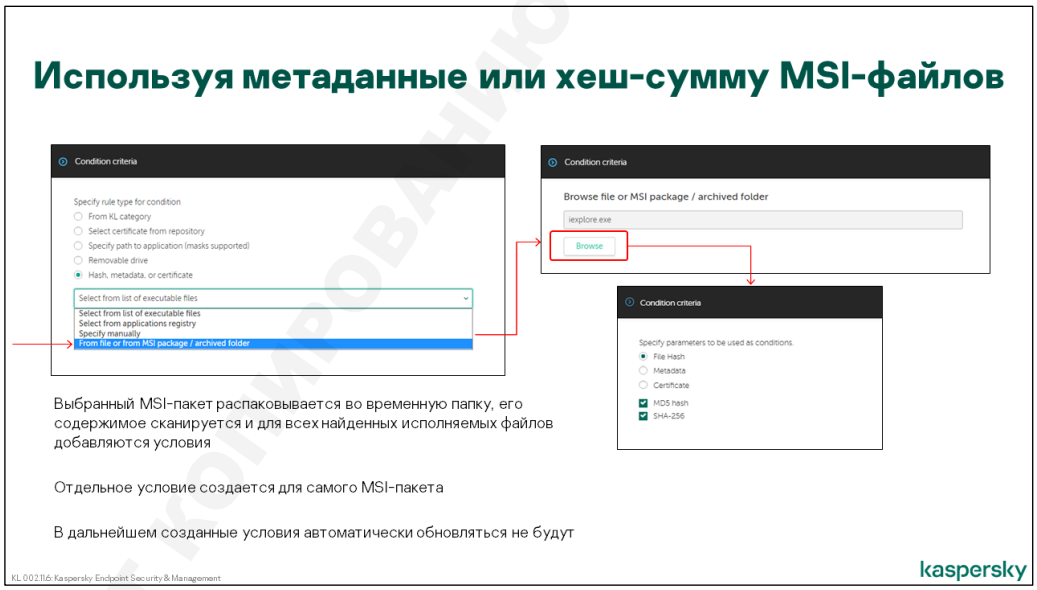
Хэш-суммы удобны также, если нужно запретить запуск файла в условиях, когда пользователи могут переименовывать файл. Переименование не влияет на хэш-сумму, и правило запрета по-прежнему будет на него распространяться.

В то же время есть ситуации, когда нужно включить в категорию файлы разных версий одного и того же приложения. В этом случае удобнее основывать условие на метаданных файла, таких как имя, название производителя, номер версии. При этом в номере версии можно требовать не только совпадения, но, и чтобы номер версии был, например, больше, чем указанное значение, или меньше. Таким образом, можно отсечь слишком старые версии программы или слишком новые, еще не прошедшие процедуру одобрения.

Условия на основе метаданных применяются только к подписанным файлам. Когда Kaspersky Endpoint Security применяет условия на основе метаданных, неподписанные файлы (без сертификата безопасности) игнорируются. Т.е. неподписанные файлы никогда не соответствуют критериям на основе метаданных. Это в первую очередь касается программ с открытым кодом и бесплатных утилит. Можно создать критерий на основе имени файла и обнаружить, что файл с подходящим именем не обрабатывается в соответствии с ожиданиями. Чаще всего это означает, что файл не подписан.

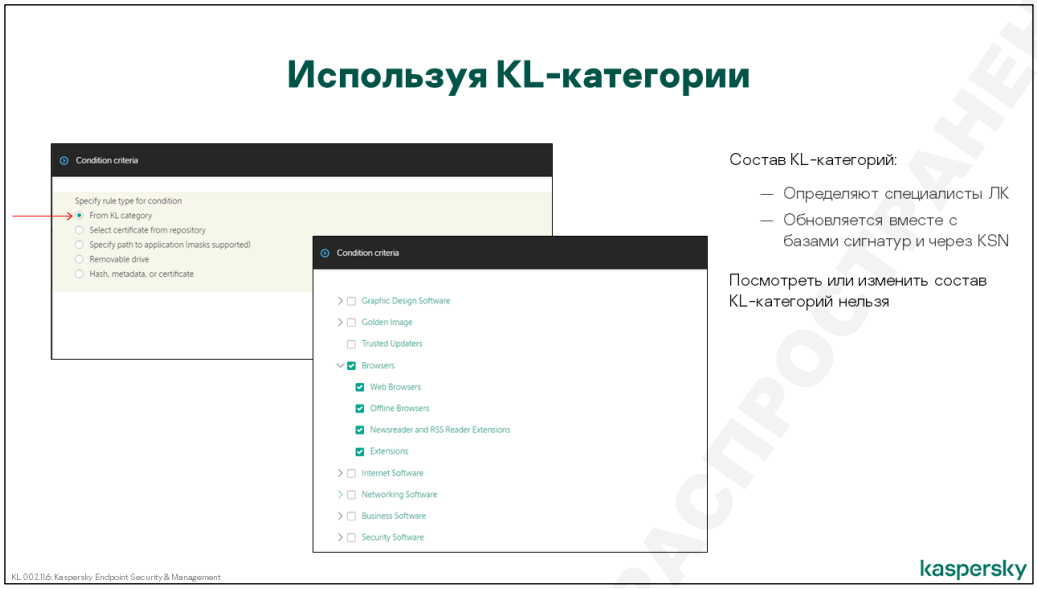
В целом, метаданные следует использовать при создании категорий для коммерческих программ, которые обычно подписаны сертификатом производителя. Чтобы контролировать программы с открытым кодом, необходимо использовать другие типы условий.

Используя метаданные или хэш-сумму MSI-файлов



Если указывать папку или MSI-пакет при настройке условий вручную, выбранная папка или пакет сканируется один раз при создании категории, и в дальнейшем не пересканируется. При этом администратор может добавлять в категорию и любые другие интересующие его условия.

Используя KL-категории



Рассмотренные выше условия позволяют администратору разрешить или запретить известные программы — программы, для которых он знает, или может узнать, хэш-сумму, атрибуты, расположение на диске и т.п.

На практике нередко возникает задача запретить неизвестные программы, например, все игры, или все браузеры, кроме одного, разрешенного, и т.п. С помощью рассмотренных выше средств эта задача легко не решается.

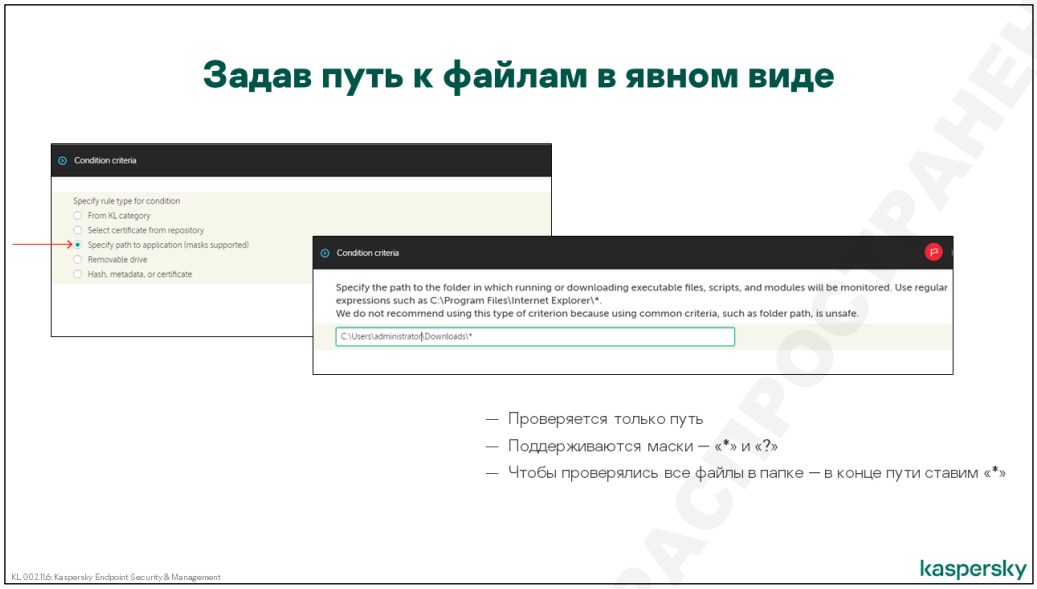
Специально для решения такой задачи есть возможность добавлять условия на базе KL-категорий, которые как раз и определяют класс или тип программы — почтовые программы, браузеры, инструменты для разработки, электронные платежные системы и т.д. Термин KL-категория означает, что принадлежность той или иной программы к категории определили специалисты Лаборатории Касперского.

Информация о том, какие программы относятся к каким категориям, является частью загружаемых баз. Поэтому, прежде чем создавать условия на основе KL-категорий, нужно чтобы задача **Загрузка обновлений в хранилище** выполнилась хотя бы один раз.

Каждый компьютер независимо проверяет соответствие запускаемых программ условиям, и поэтому если на разных компьютерах разные версии баз, применение правил контроля запуска может иметь разный эффект. Кроме этого, если для компьютера включено использование KSN, он будет пытаться получить самые свежие данные о принадлежности программы к KL-категориям в реальном режиме времени.

Специалисты Лаборатории Касперского, конечно же, не могут обработать абсолютно все исполняемые файлы, существующие в мире, и приписать их к KL-категориям. Все некатегоризированные файлы автоматически относятся к KL-категории **Другие программы**.

Задав путь к файлам в явном виде



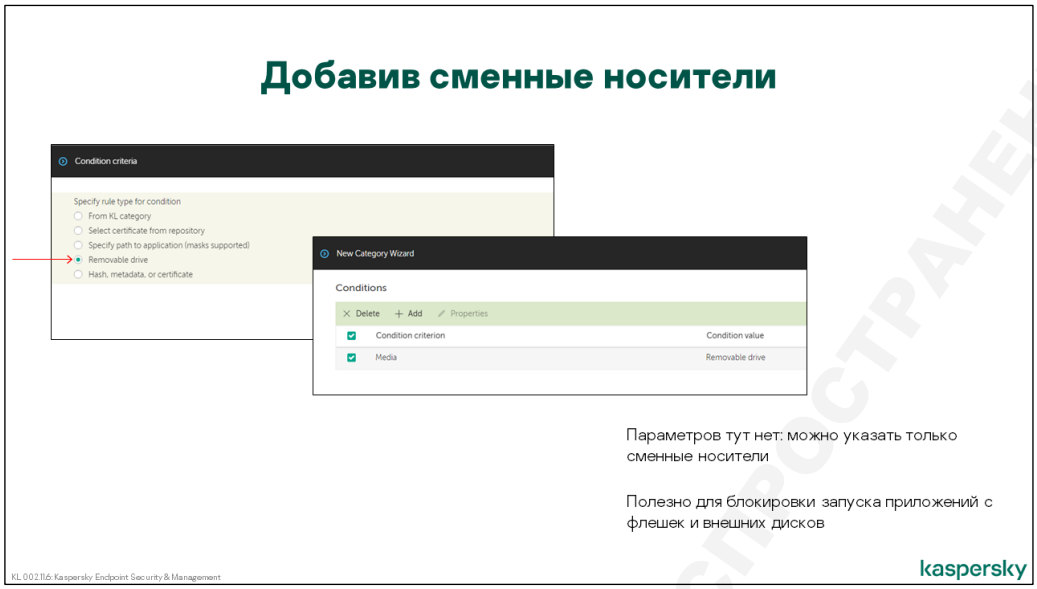
До этого все условия сводились к проверке хэш-суммы файла или его атрибутов. Выполнение этих условий не зависит от того, где расположен файл. Если пользователь или вредоносная программа скопирует или переместит исполняемый файл, это не повлияет на возможность запуска согласно вышеприведенным условиям.

Следующие два типа условий являются полной противоположностью. Они учитывают только расположение файла:

— **Папка программы** — определяет локальный путь к файлу. Администратор может, например, запретить запуск исполняемых файлов с рабочего стола или из домашней папки пользователя.

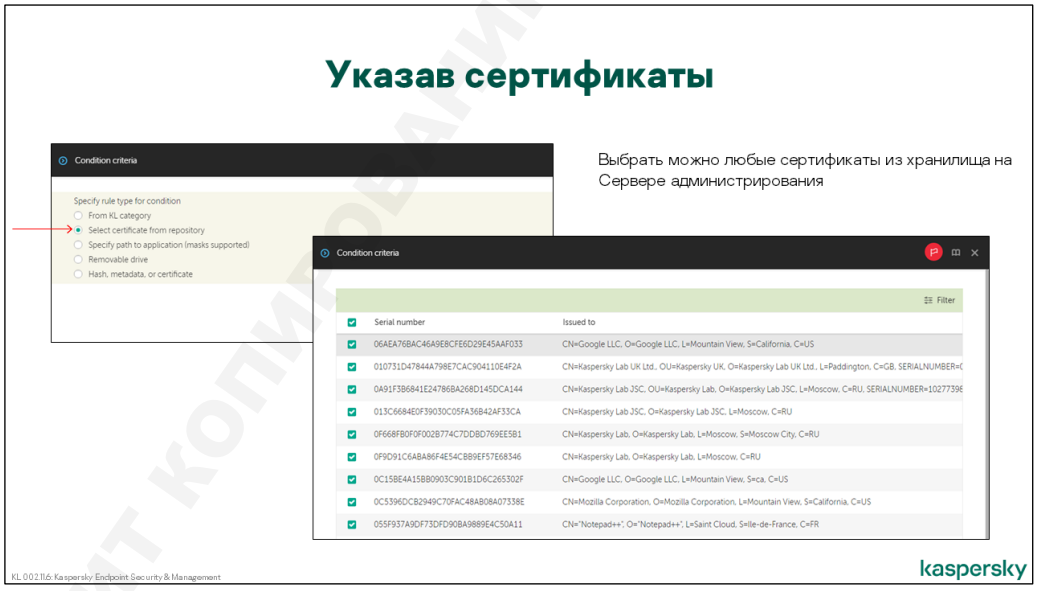
  Или, наоборот, администратор может разрешить запуск исполняемых файлов из системных папок: C:\Windows, C:\Program Files и запретить запуск из всех остальных мест на компьютере.

  Условие является рекурсивным, т.е. для файлов в подпапках указанной папки оно выполняется.



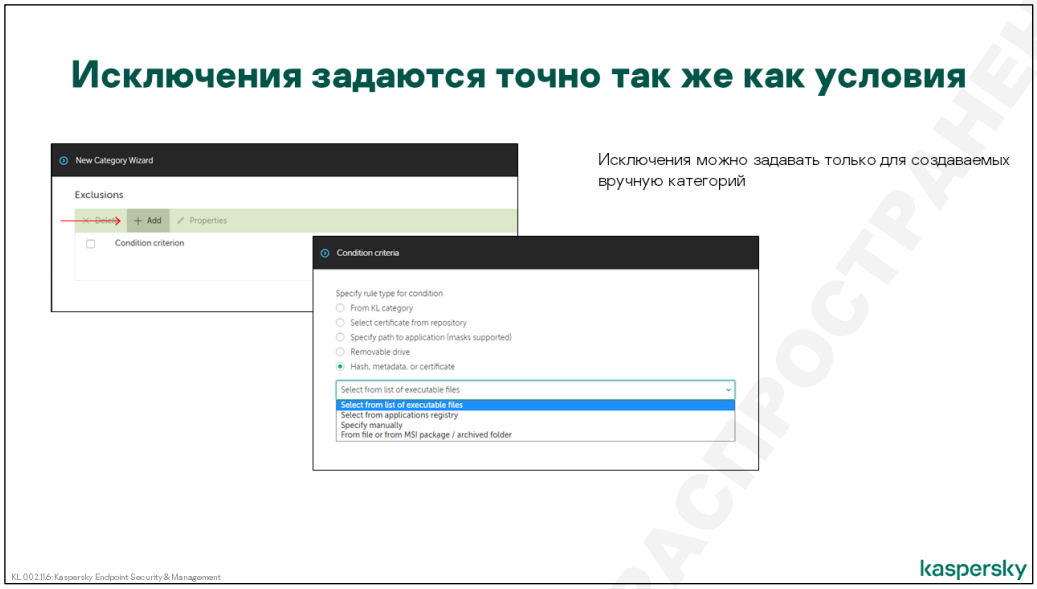
— **Тип носителя** — может иметь только одно значение *Сменный носитель*. В сущности, преследует одну цель — дать администратору простую возможность запретить запуск программ со сменных носителей.

Указав сертификаты



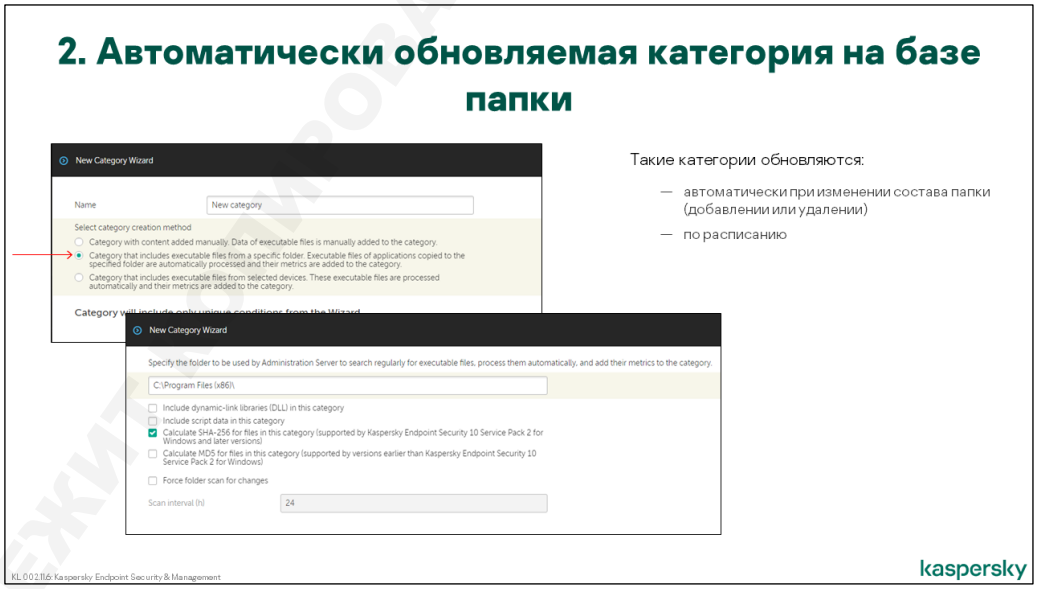
Более надежный способ, чем по пути к файлу, но менее надежный, чем SHA-256 — выбрать файлы по сертификатам. Выбирать можно из сертификатов на Сервере администрирования.

Как задать исключения из категории

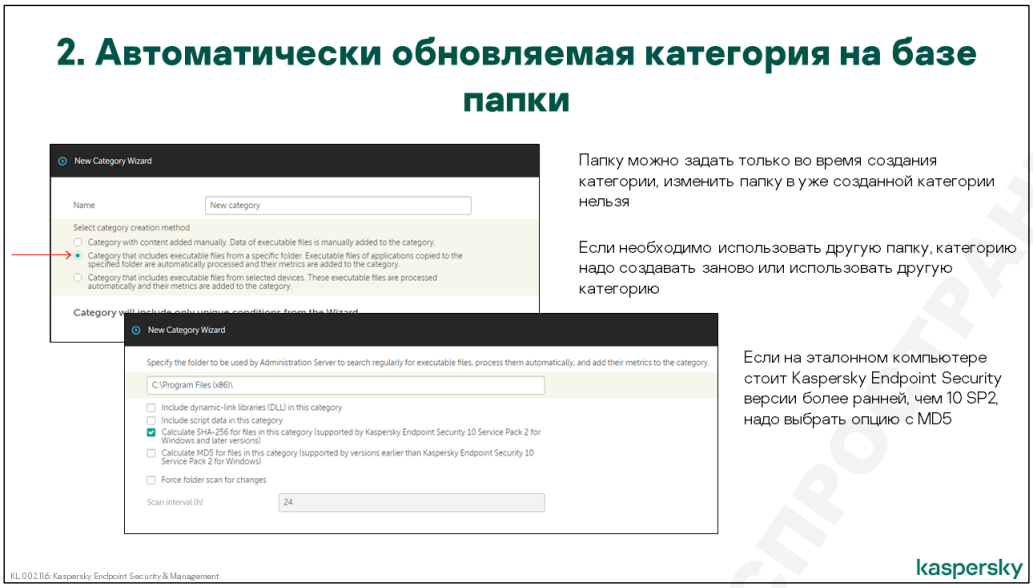


В случае, если нужно запретить все программы, соответствующие заданным условиям, кроме одной, в категорию нужно добавить исключение. Исключения задаются с помощью списка условий, таких же, как и для включения в категорию. Программы, соответствующие хотя бы одному исключению, будут исключены из категории.

Автоматически наполняемая категория на базе папки



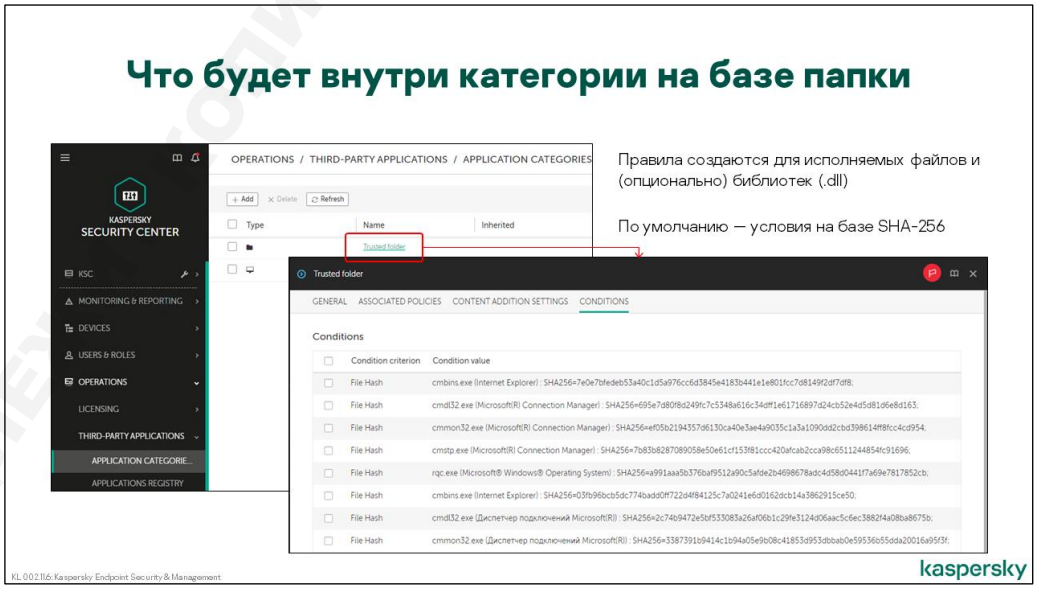
Содержимое автоматически пополняемой категории обновляется при добавлении или удалении из папки-источника исполняемых файлов. Кроме того, можно включить принудительное обновление категории по расписанию.



Если в указанной папке находятся архивы или инсталляционные пакеты (например, ***.msi**), Сервер администрирования автоматически распаковывает их (во временную папку) и включает в категорию данные об исполняемых файлах внутри архива или пакета. Таким образом, если поместить в папку дистрибутив программы, в категорию попадет не только установочный файл, но и файлы самой программы.

Такой способ создания категории удобен, если есть хранилище дистрибутивов программ, используемых для установки на компьютеры организации. Запуск таких программ должен быть разрешен. Администраторы могут время от времени пополнять список используемых программ или заменять их более новыми версиями.

Чтобы не обновлять вручную правила для категорий, описывающих эти разрешенные дистрибутивы, проще поместить их все в одну папку и поручить Серверу администрирования автоматически отслеживать изменения и заносить параметры обнаруженных файлов в одну категорию. После этого администратору достаточно будет создать в политике одно разрешающее правило для этой категории, чтобы разрешить запуск сразу всех используемых программ.



Параметр **Включать в категорию динамически подключаемые библиотеки (DLL)** соответствует своему названию. Если его включить, Kaspersky Security Center при сканировании

папки будет вычислять контрольные суммы dll-файлов и добавлять их в категорию наравне с другими исполняемыми файлами.

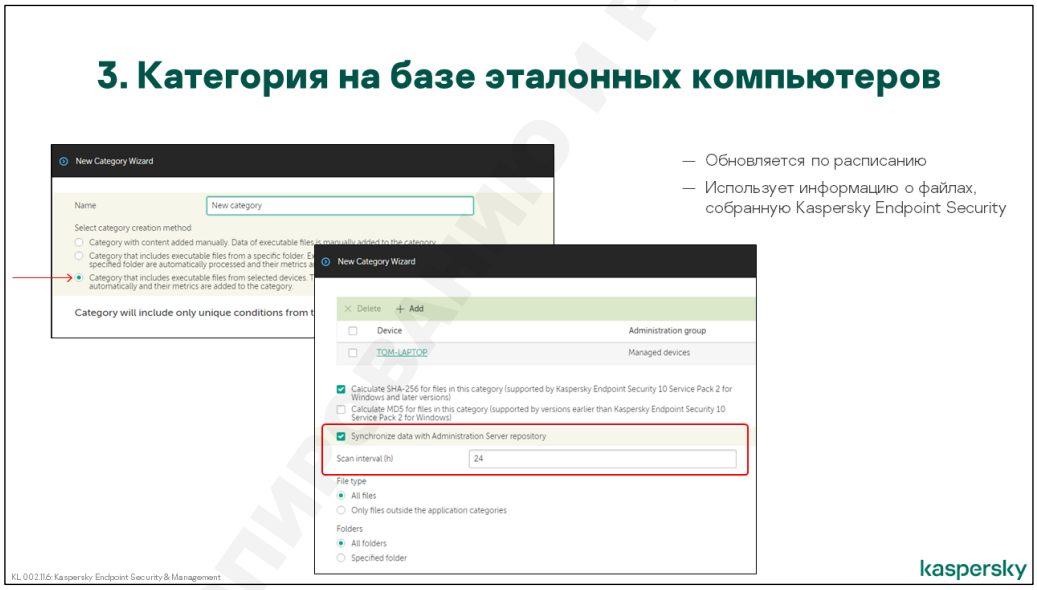
Смысл перечисления dll-файлов в том, что Windows позволяет запускать процессы прямо из таких файлов при помощи утилиты **rundll32.exe**. В общем случае какие-то из процессов, запускаемых из файлов библиотек, могут быть разрешены, а другие запрещены.

В этом смысле dll-файлы не сильно отличаются от файлов сценариев (*.js или *.vbs) которые не являются исполняемыми сами по себе, запускаются через утилиту **cscript.exe** (или **wscript.exe**), но могут быть тоже разрешены или запрещены.

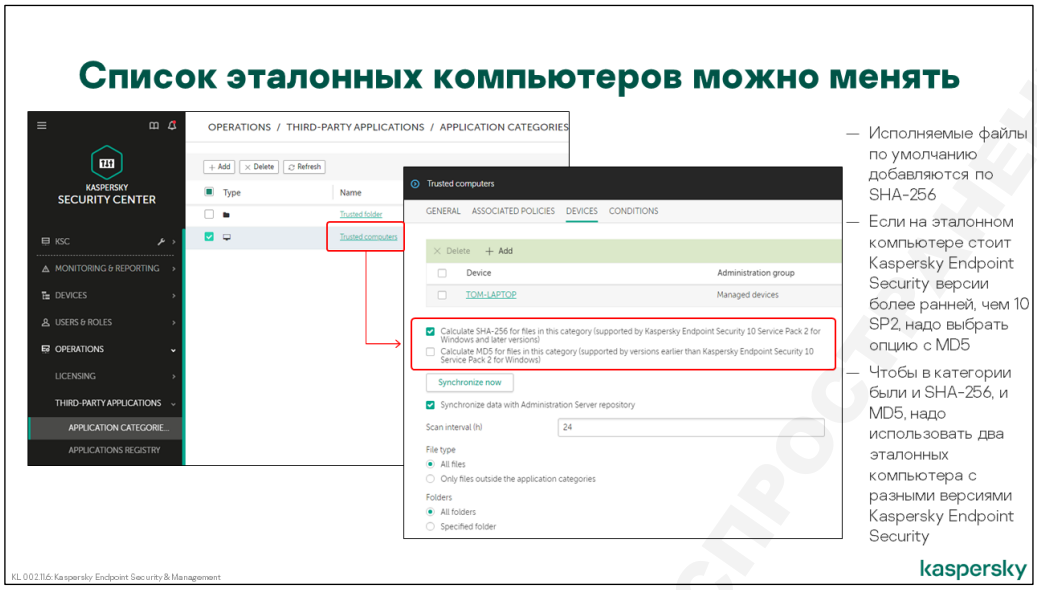
Для включения в категорию скриптов нужно отметить флаг **Включать в категорию данные о скриптах**.

Точно также, как и для остальных типов создания категорий, можно использовать хэш-суммы. Если в сети есть и KES10 SP2, и более старые, можно выбрать оба флага. Тогда категория будет больше, но зато будет работать для всех версий Kaspersky Endpoint Security.

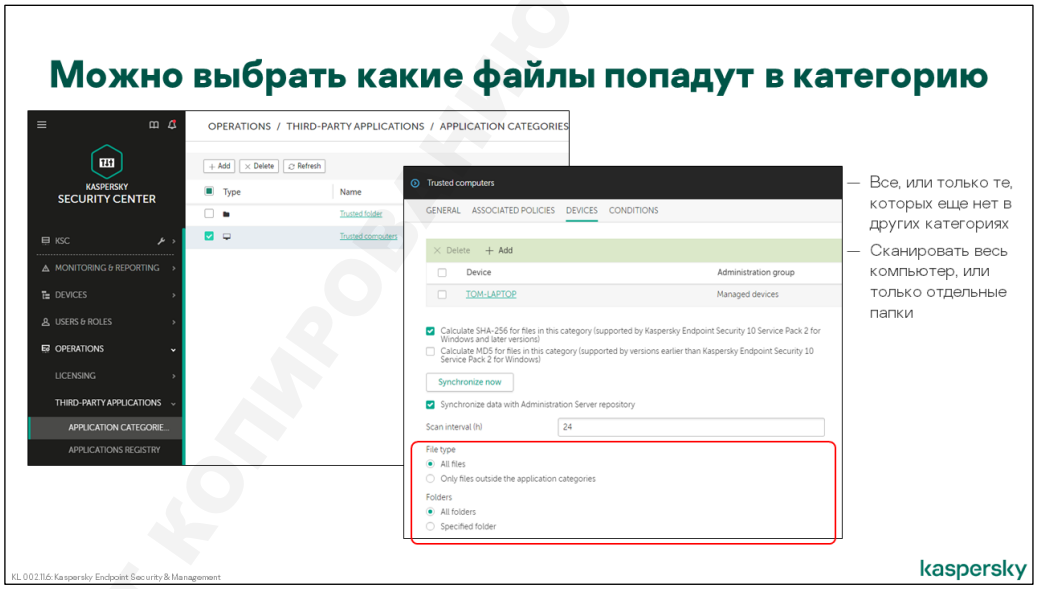
Категория на базе эталонных компьютеров



Кроме хранилища дистрибутивов разрешенных программ, в организации может быть эталонный компьютер, на котором эти программы установлены. Такой эталонный компьютер, как правило, используется для создания образов и последующего развертывания их на новые компьютеры. В результате развертывания образа получается компьютер с установленной операционной системой и всеми необходимыми для работы программами, и это значительно быстрее, чем устанавливать все из дистрибутивов. Администраторы время от времени обновляют программы на эталонном компьютере и соответственно обновляют образ.



При таком подходе удобно автоматически считать все программы на эталонном компьютере разрешенными. А для этого нужно просканировать компьютер и внести все программы в одну категорию, для которой потом создать разрешающее правило в политике. Именно это и делает категория, автоматически пополняемая файлами с выбранных компьютеров.



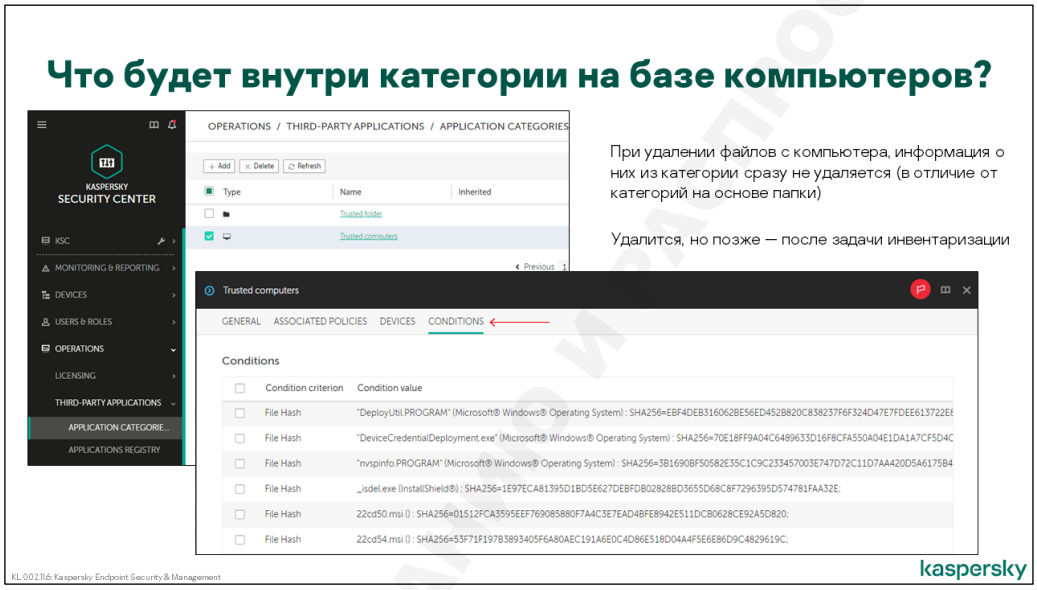
Иногда удобно разделить файлы эталонного компьютера на несколько категорий. Например, файлы Windows учитывать отдельно, а файлы из папки Program Files отдельно. В таком случае в категории на основе эталонного компьютера можно настроить фильтр на основе папки, в которой расположен файл. В категорию будут попадать только те файлы, которые найдены на компьютере в указанной папке.

В отличие от категории на основе папки, когда изменения отслеживаются Сервером администрирования, категория на основе эталонного компьютера наполняется на основе данных об исполняемых файлах, обнаруженных Kaspersky Endpoint Security. Это означает, на эталонном компьютере должен быть установлен Kaspersky Endpoint Security с компонентом **Контроль программ**, для составления списка исполняемых файлов, и Агент администрирования, для пересылки списка файлов на Сервер. Более детально этот механизм будет рассмотрен позже в этой главе.

Как и для категории, пополняемой из папки, администратор может задать интервал сканирования.

Обнаруженные файлы заносятся в категорию и в дальнейшем идентифицируются по SHA-256 (для последних версий Kaspersky Endpoint Security), или MD5 суммам (для Kaspersky Endpoint Security 10 SP1 MR3 и более старых) — в зависимости от версии Kaspersky Endpoint Security, установленной на эталонном компьютере.

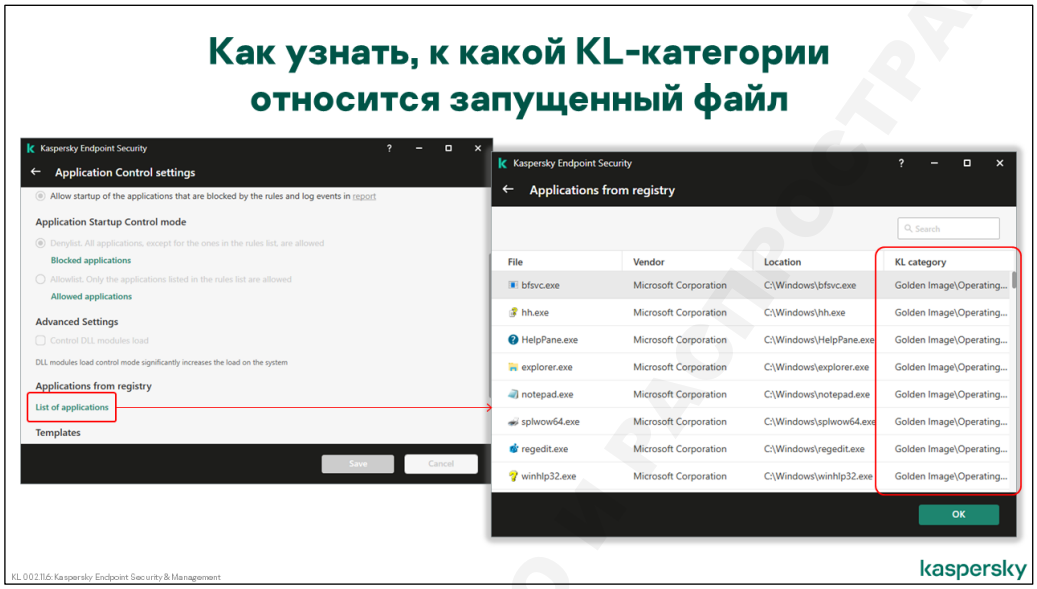
Обратите внимание: в отличие от категории на основе папки, здесь надо выбрать или SHA-256, или MD5 (в зависимости от установленной на эталонном компьютере версии Kaspersky Endpoint Security). То есть если в сети есть Kaspersky Endpoint Security разных версий, для категории нужно использовать два эталонных компьютера



Внутри категории на базе компьютеров будет список обнаруженных файлов и соответствующее каждому файлу значение SHA-256 или MD5.

Что можно делать с программами и категориями после первоначальной настройки

Как узнать к какой KL-категории относится запущенный файл



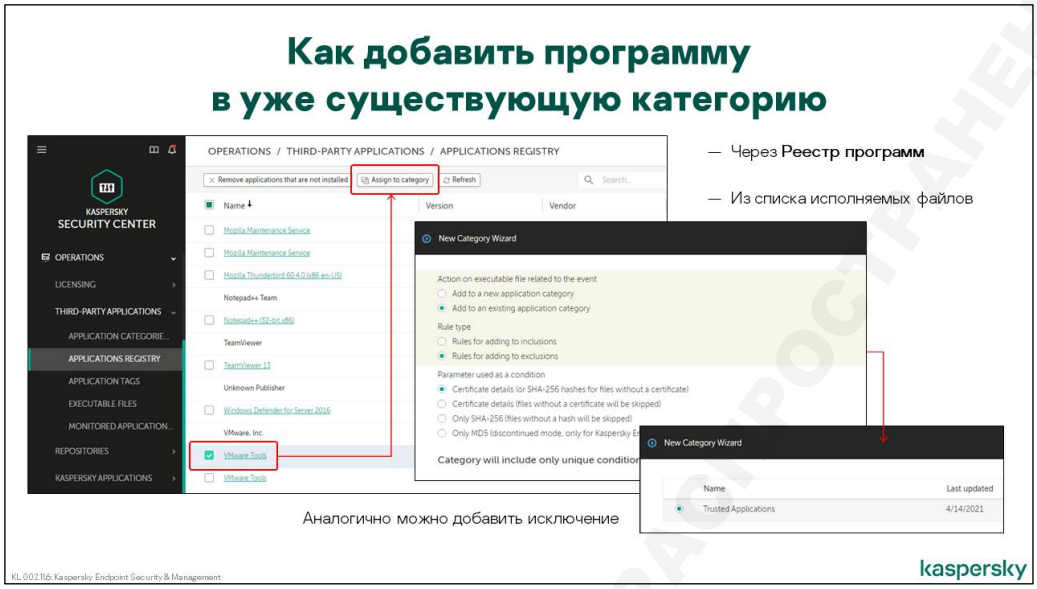
Если администратору нужно узнать, к какой KL-категории относится конкретный исполняемый файл, он может сделать это как из локального интерфейса Kaspersky Endpoint Security, так и из консоли управления. Локальные вердикты (которые изредка могут отличаться на разных компьютерах из-за разницы в версиях баз) доступны в окне **Мониторинг активности программ**.

Информация из Консоли администрирования может использоваться как для расследования, почему правила не работают, как ожидается, так и при планировании категорий и правил. Список исполняемых файлов находится во вкладке **Операции | Программы сторонних производителей | Исполняемые файлы**. В свойствах каждой записи отображаются метаданные и KL-категория соответствующего файла.

Поскольку файлов в списке может быть достаточно много (файлы со всех компьютеров в сети), функции поиска и фильтрации списка могут быть весьма полезны. Можно искать файлы по маске имени или отфильтровать содержимое списка по принципу соответствия определенным метаданным.

Список исполняемых файлов можно использовать не только для определения KL-категории, метаданных и другой статистики, как например, когда файл был впервые обнаружен в сети, но также для включения или исключения файла из ранее созданной категории. Для добавления файла в категорию существует специальная кнопка. Файл можно добавить к уже существующей категории, или создать новую. И при изменении существующей категории файл можно добавить либо в список условий, либо в список исключений. В любом случае итоговое условие будет основываться на контрольной сумме файла SHA-256 или MD5 или данных сертификата.

Как добавить программу в уже существующую категорию



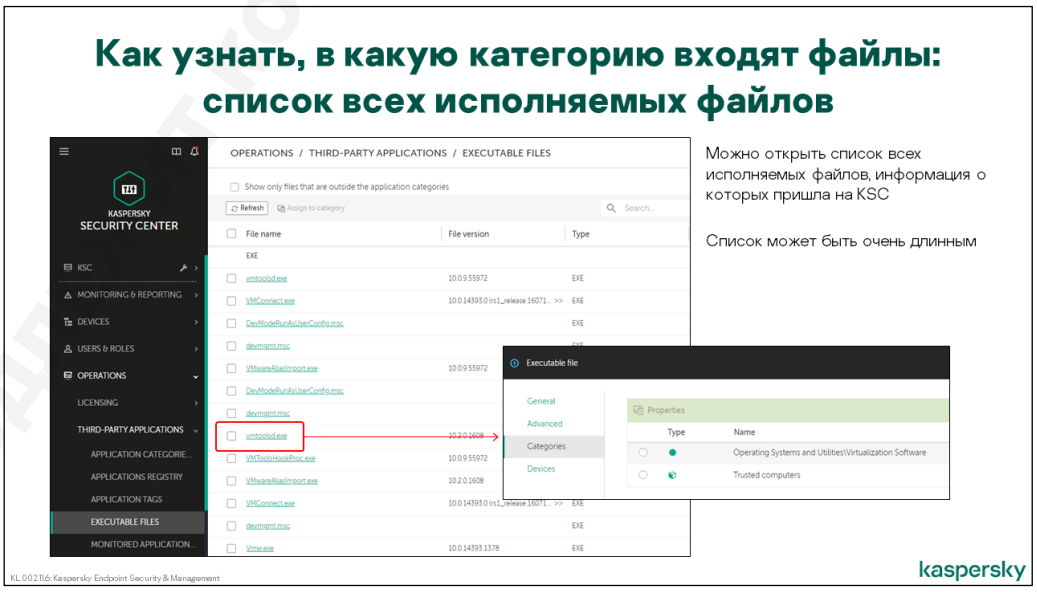
Если администратор, просматривая список исполняемых файлов, которые были обнаружены на подключенных к Kaspersky Security Center компьютерах, увидел что-то новое и решил добавить программу в одну из категорий, не нужно запоминать что и именно нужно добавить и идти в контейнер с категориями программ. Можно просто выбрать исполняемый файл или программу и выполнить команду **Назначить категорию**.

Затем нужно выбрать как добавить, в существующую категорию или создать новую. Куда добавить, программы можно добавлять как в сами категории, так и в исключения для категорий.

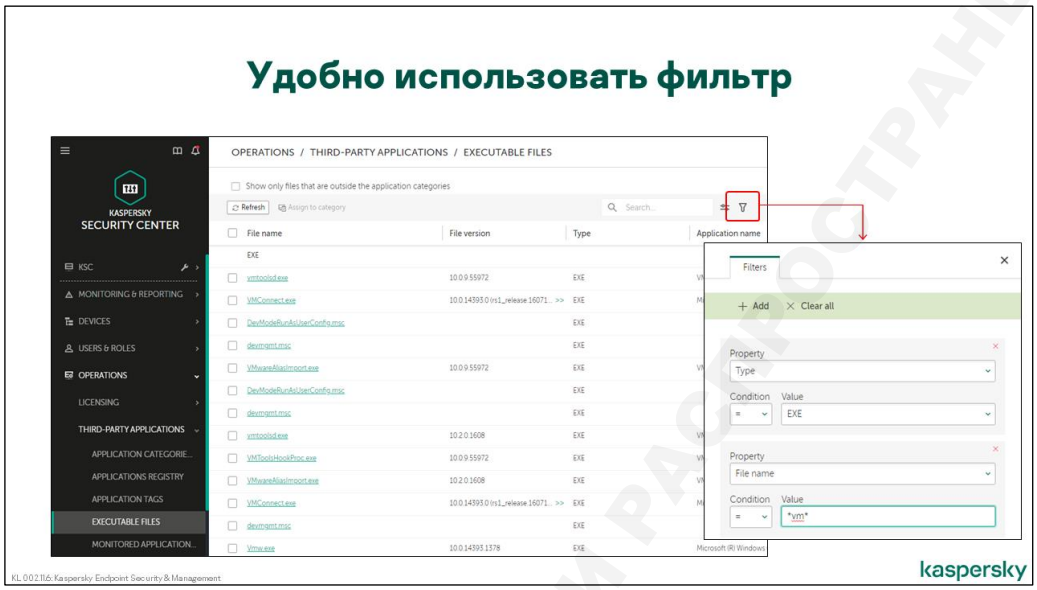
Программа будет добавлена по хэш-сумме или сертификату, которым подписан исполняемый файл.

Как узнать, в какую категорию входят файлы

Через список всех исполняемых файлов

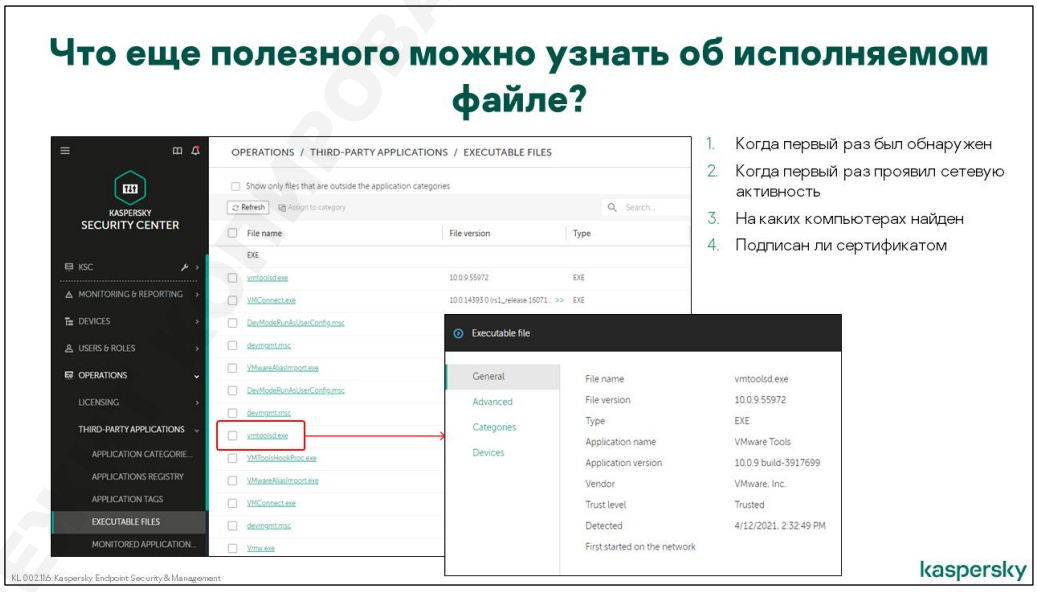


Список исполняемых файлов, который мы видим на Сервере администрирования Kaspersky Security Center — это все исполняемые файлы, обнаруженные Kaspersky Security Center и Kaspersky Endpoint Security на всех подключенных к этому Серверу администрирования компьютерах. То есть этот список может быть очень большим.



Но когда вы знаете, что искать, удобно использовать именно его. Можно просто отсортировать по имени, или использовать фильтры.

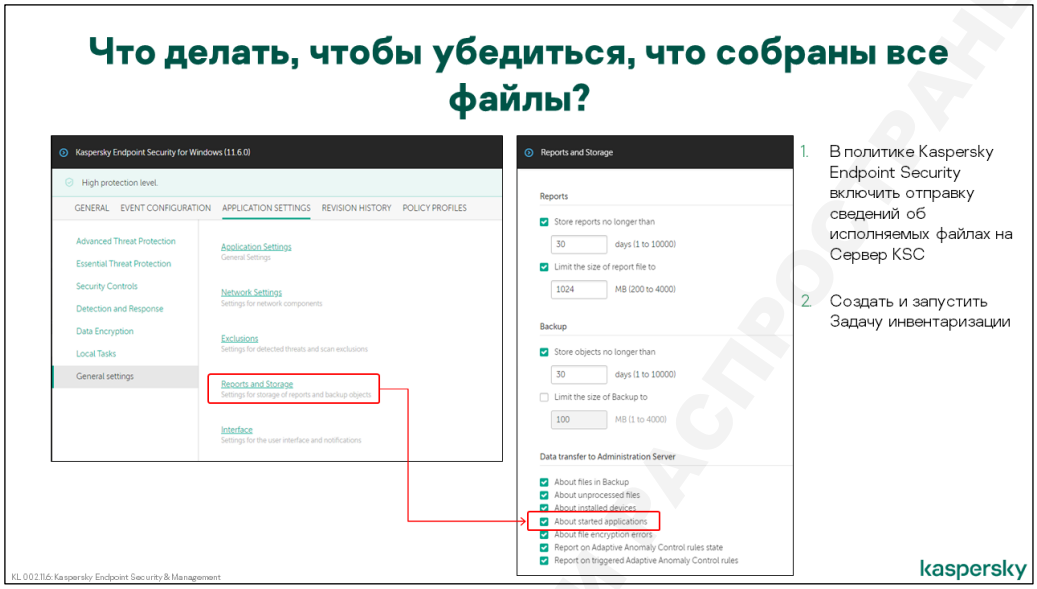
Что еще полезного можно узнать о файле



На каких компьютерах и когда первый раз был обнаружен (но не как), когда первый раз проявил сетевую активность, подписан ли сертификатом.

Что делать, чтобы убедиться, что собраны все файлы

Где включается пересылка информации о найденных исполняемых файлах



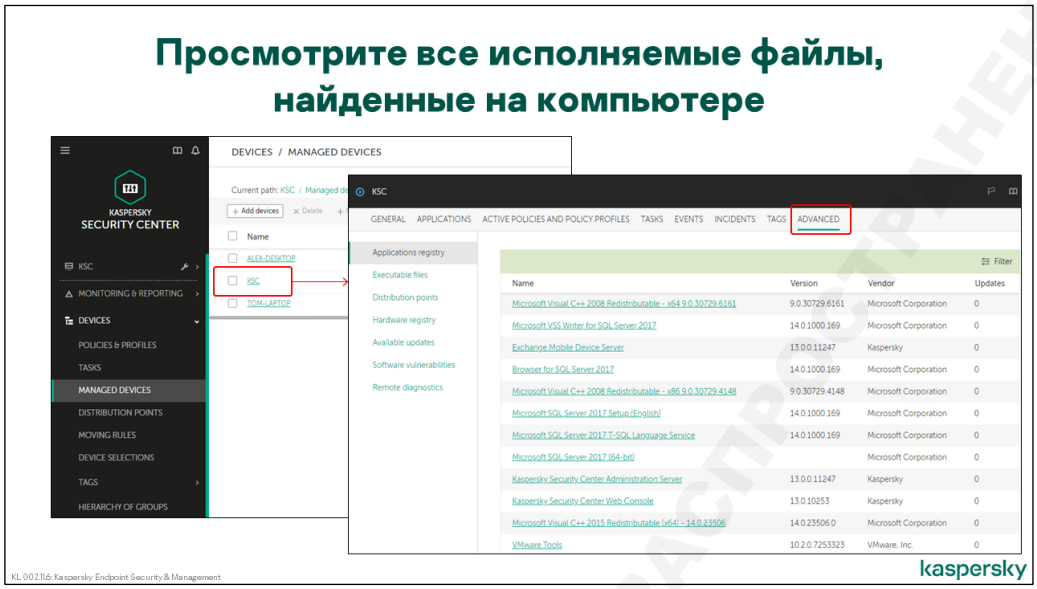
Сразу после установки Сервера администрирования контейнер исполняемых файлов будет пуст. По мере подключения новых клиентов на Сервер администрирования будут поступать новые данные, однако обязательным условием в Kaspersky Endpoint Security 11.6 является наличие включенного компонента Контроль программ.

Важно: Если Контроль программ выключен, данные об исполняемых файлах не будут передаваться при запуске приложений.

Кроме того, в политике Kaspersky Endpoint Security есть опция о пересылке информации о найденных исполняемых файлах, по умолчанию она включена. Находится она в политике Kaspersky Endpoint Security на вкладке **Параметры программы | Общие настройки | Отчеты и хранилище**, опция **О запускаемых программах**. Эта настройка касается как пересылки информации о запущенных приложениях, так и результатов работы задачи инвентаризации.

Примечание: включать пересылку информации об установленных приложениях на всех клиентских компьютерах, на слабых компьютерах или на непостоянных виртуальных машинах в общем случае не рекомендуется.

Как просмотреть все найденные на компьютере исполняемые файлы



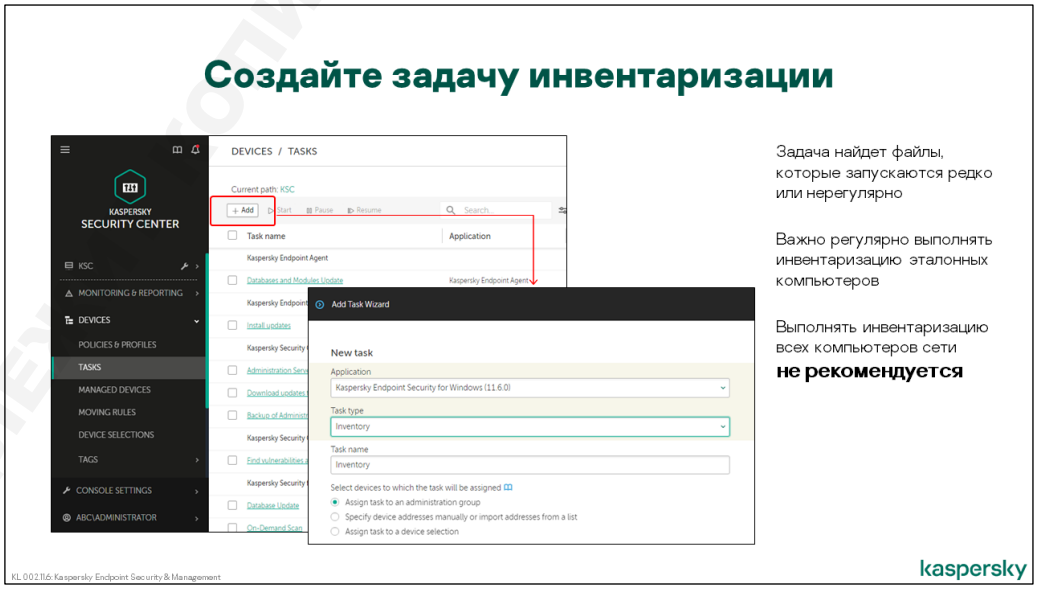
В свойствах каждого из управляемых компьютеров есть список найденных на нем исполняемых файлов. Этот список пополняется:

1. Задачей инвентаризации, которая сканирует заданные в ее свойствах папки на клиентских компьютерах

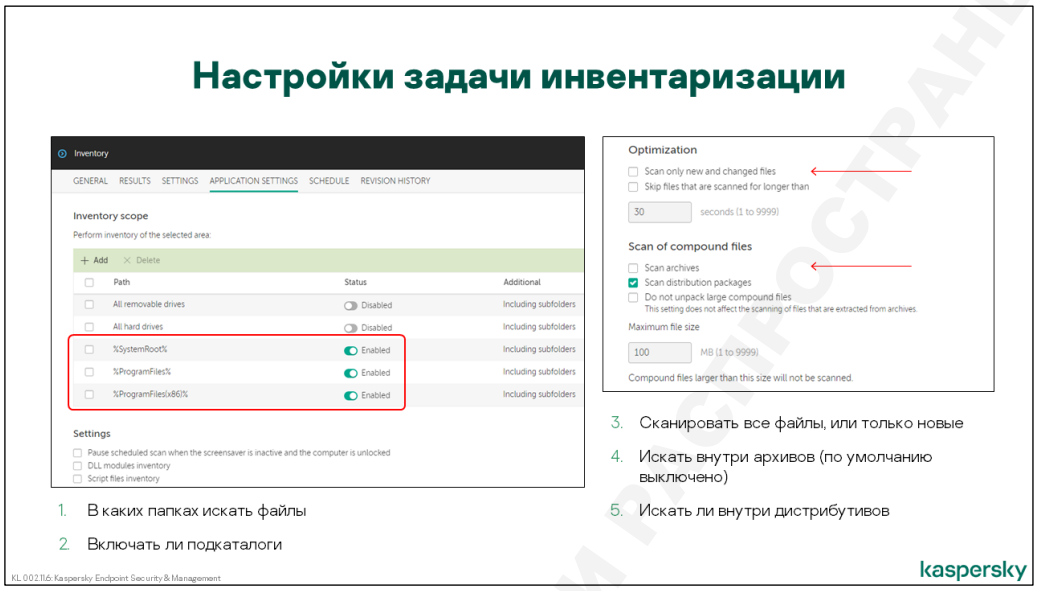
2. Контролем программ, если компонент включен, собирает информацию обо всех исполняемых файлах, которые запускаются на клиентских компьютерах.

Агент администрирования тоже собирает информацию о программах — но только об установленных приложениях, для этого он сканирует реестр.

Задача инвентаризации



По умолчанию не создается. Это означает, что в список исполняемых файлов попадают только те, которые запускались на компьютерах с работающим компонентом **Контроль программ**. Может пройти немало времени, пока та или иная программа станет доступной через список на Сервере администрирования. Чтобы не ждать, нужно создать и запустить задачу инвентаризации.



Эта задача относится к задачам Kaspersky Endpoint Security, может быть групповой или для наборов компьютеров. При стандартных настройках задача выполняет поиск исполняемых файлов в каталогах:

- *%SystemRoot%*
- *%ProgramFiles%*
- *%ProgramFiles(x86)%*

Список проверяемых папок можно изменить или дополнить. Информация о найденных файлах поступает на Сервер администрирования и доступна через Web Console во вкладке **Операции | Программы сторонних производителей | Исполняемые файлы**.

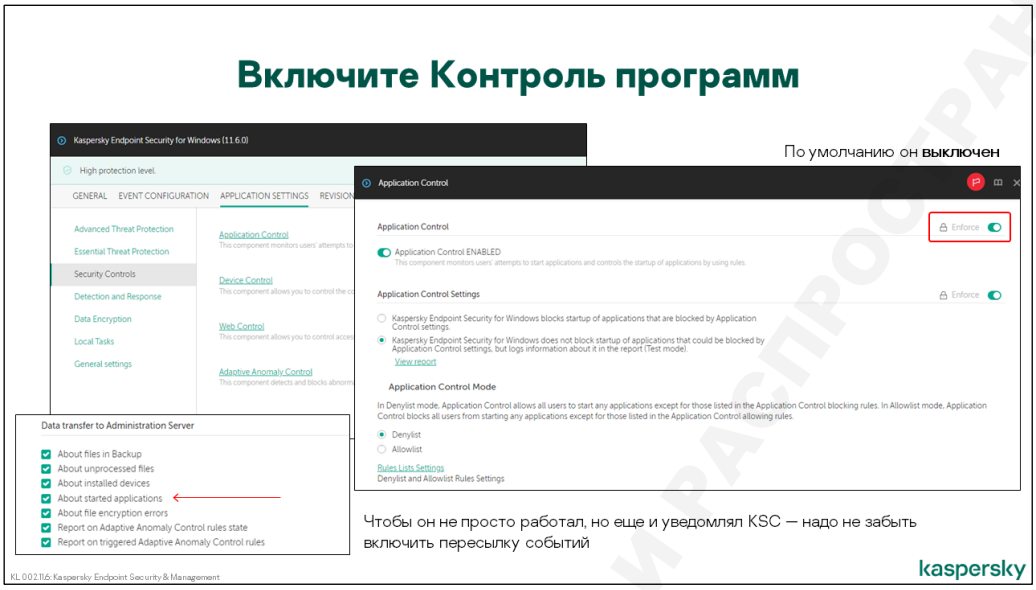
В отличие от компонентов, осуществляющих мониторинг, задача может обнаруживать исполняемые файлы внутри архивов и инсталляционных пакетов. Для этого нужно включить опции **Проверять архивы** и **Проверять дистрибутивы**.

Поиск исполняемых файлов сопровождается вычислением их контрольных сумм, что может сказаться на быстродействии компьютеров. Чтобы снизить потребление ресурсов, можно **Проверять только новые и изменённые файлы**. Информация об изменениях поставляется в рамках технологии iSwift и не требует практически никаких вычислений.

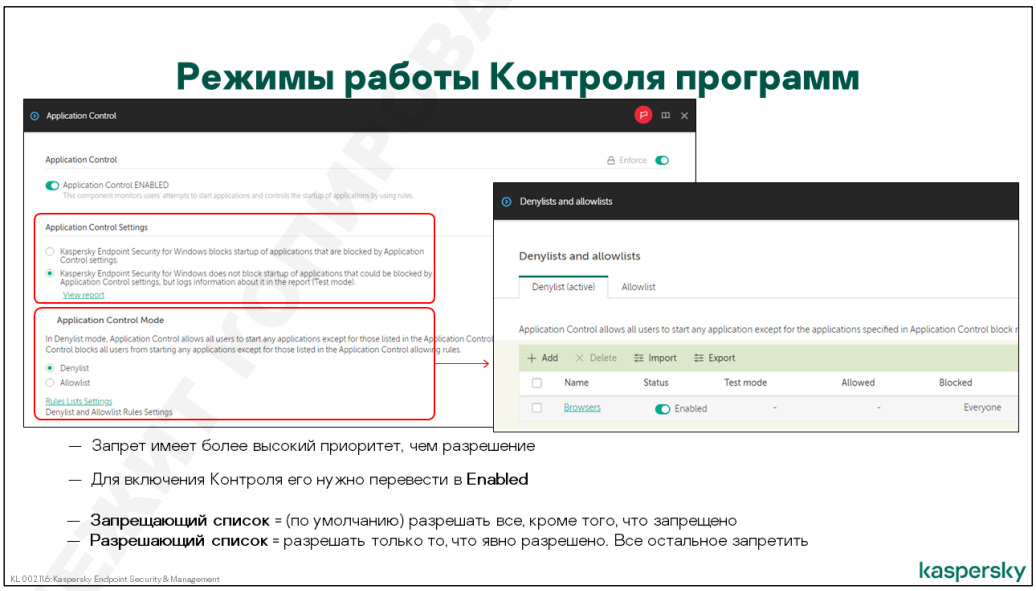
В качестве альтернативы, можно запланировать выполнение задачи в нерабочее время, или использовать опцию, которая приостанавливает сканирование, когда компьютер активен, и возобновляет его, когда пользователь блокирует свою сессию или когда запускается экранная заставка.

2.3 Как создавать правила контроля

Режимы работы Контроля программ



Обратите внимание, что в Kaspersky Endpoint Security начиная с версии 10 SP1 **Контроль программ** по умолчанию выключен. Поэтому информация о запускаемых файлах изначально не пересылается. Первое, что нужно сделать администратору перед настройкой правил, — это включить компонент, и выбрать режим: Разрешающий список или Запрещающий список (подробнее о режимах в главе 2.1 «Как работает Контроль программ»)



По умолчанию, сразу после включения **Контроля программ**, будет включен режим тестирования. Рекомендуется сначала протестировать правила. Вместо реальных блокировок на Сервер администрирования будут приходить события **Запуск программы запрещен в тестовом режиме** или **Запуск программы разрешен в тестовом режиме**. По событиям можно сгенерировать отчет, проанализировать его, если требуется, изменить правила, после чего перевести их в режим блокировки. В дальнейшем, чтобы протестировать новые правила и не нарушить работу уже действующих, администратор может добавлять правила со статусом **Тестовый режим**.

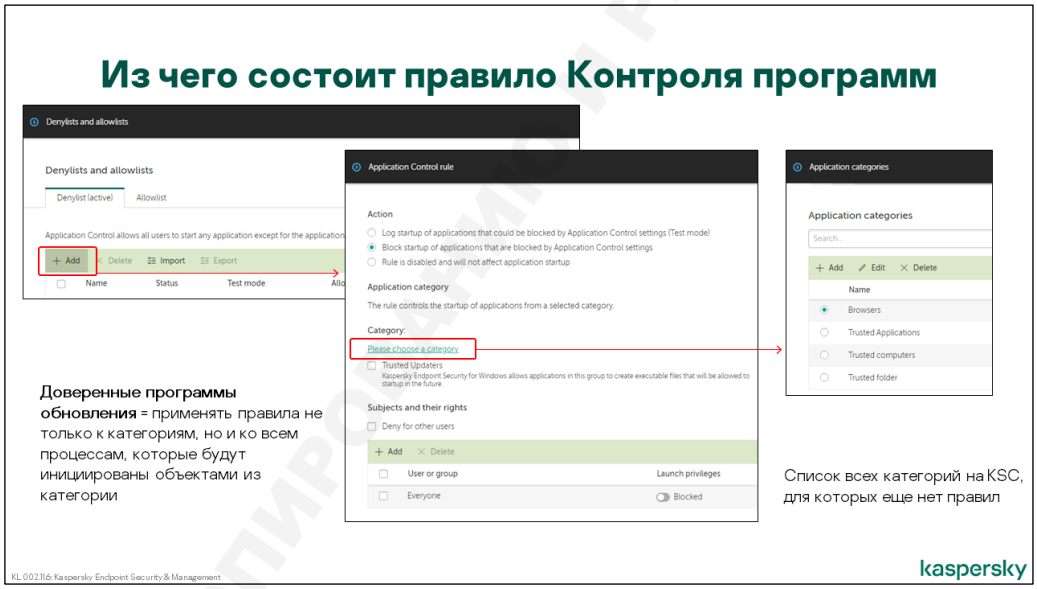
Убедиться, что они корректно работают с полезными приложениями, переключить новые правила в статус **Включено**.

Каждое правило (вне зависимости от выбранного режима – Разрешающий список или Запрещающий список) может использовать один из трех статусов:

- **Включено** — означает, что правило используется во время работы компонента Контроль программ.
- **Включено** — означает, что правило не используется во время работы компонента Контроль программ.
- **Тестовый режим** — означает, что Kaspersky Endpoint Security всегда разрешает запуск программ, на которые распространяется действие этого правила, но передает информацию о запуске этих программ на Сервер администрирования.

Опция **Контролировать DLL и драйверы** отслеживает запуск библиотек DLL и драйверов, но это увеличивает нагрузку на компьютер, и включать ее рекомендуется только когда это действительно необходимо. Например, при строгом Default Deny.

Правила контроля программ



Правил может быть сколько угодно, запрет всегда имеет более высокий приоритет. Набор правил для запрещающего списка и разрешающего списка разный. Например, если вы сначала выбрали Запрещающий список, добавили правило, а потом переключились в Разрешающий список, то ваше правило вы тут не увидите.

Каждое правило задается такими параметрами:

- **Категория**— одна из категорий программ, предварительно заданных на Сервере администрирования. Для каждой категории в одной политике можно создать не более одного правила.
- **Пользователи и / или группы, получающие разрешение** — список локальных пользователей и групп или пользователей и групп домена, которым разрешается запуск программ из выбранной категории. Если требуется указать больше чем одну сущность, они перечисляются через точку с запятой ";"
- Параметр, дополняющий список пользователей, получающих разрешение, — **Запретить остальным пользователям**. При включении этого параметра, категория автоматически запрещается для всех пользователей, не внесенных в список получающих разрешение на

запуск. Все версии Kaspersky Endpoint Security 10 предшествовавшие SP1 работали так, как будто для всех правил параметр **Запретить остальным пользователям** был всегда включен. В версии Kaspersky Endpoint Security 11 параметр задается открыто и по умолчанию отключен. Таким образом, разрешение или запрет на запуск для пользователей, не указанных в правиле определяются остальными правилами.

- **Пользователи и / или группы, получающие запрет** — параметр, аналогичный предыдущему, т.е. список пользователей и групп, которым запрещается запуск программ
- **Доверенные программы обновления** — считать все программы категории доверенными программами обновления[1]

Запрет имеет более высокий приоритет, чем разрешение. Например, если в правиле настроено разрешение для всех пользователей и запрет для пользователя Tom, этот пользователь не сможет запускать программы согласно правилу.

Список правил изначально для режима запрещающего списка пуст, а для разрешающего списка содержит два системных правила, удалить которые нельзя:

- **Доверенные программы обновления** — если это правило включено, приложения, установленные доверенными программами обновления, не будут блокироваться, даже если для них нет разрешающих правил. Доверенные программы обновления — это специальная[2] KL-категория, к которой относятся программы, загружающие и устанавливающие обновления модулей, например, Adobe Updater, Google Update и т.п. По умолчанию правило включено — то есть Доверенные программы обновления разрешены
- **Операционная система и ее компоненты** — содержит исполняемые файлы необходимые для работы операционной системы, а также исполняемые файлы, которые поставляются вместе с операционной системой — всевозможные стандартные утилиты и приложения. Чтобы Kaspersky Endpoint Security случайно не заблокировал важные для операционной системы файлы

В списке нет кнопок для перемещения правил по списку, поскольку порядок правил не имеет значения. При запуске программы на компьютере, Kaspersky Endpoint Security оценивает все включенные правила совокупно. Разные правила определяют возможность запуска для разных категорий программ, но конкретная программа может входить в несколько категорий. Если существует хотя бы одно правило, согласно которому запуск программы должен быть запрещен, он будет запрещен, независимо от настроек других правил.

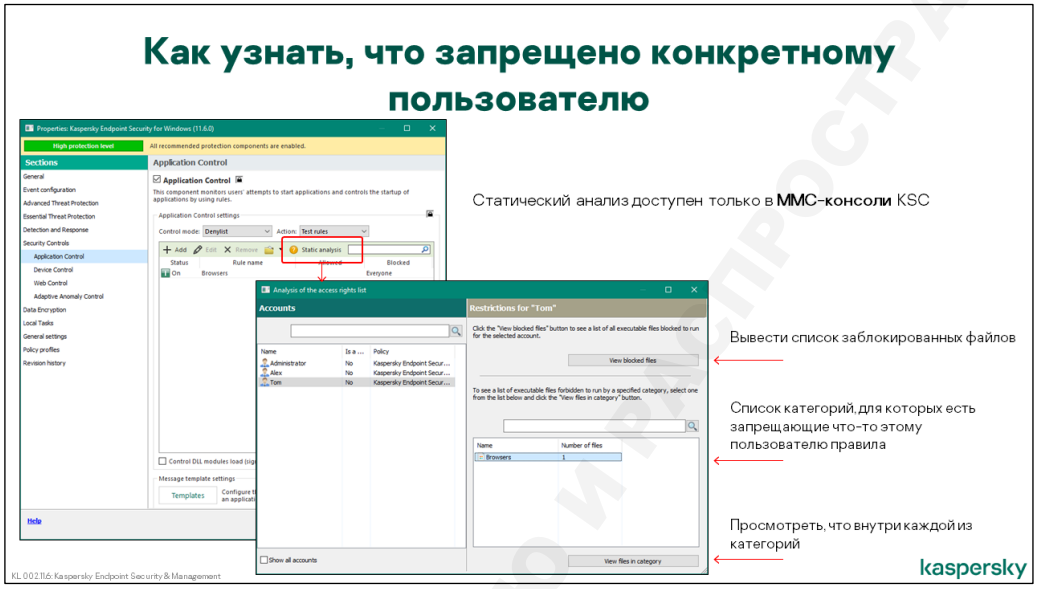
Если программа не входит ни в одну из категорий, то в режиме запрещающего списка она будет разрешена, а в режиме разрешающего списка — запрещена.

[1] Подробнее об этой опции рассказано ниже, в этой же главе

[2] Выбрать эту KL-категорию при настройке условий для категории программ нельзя

2.4 Как это будет работать

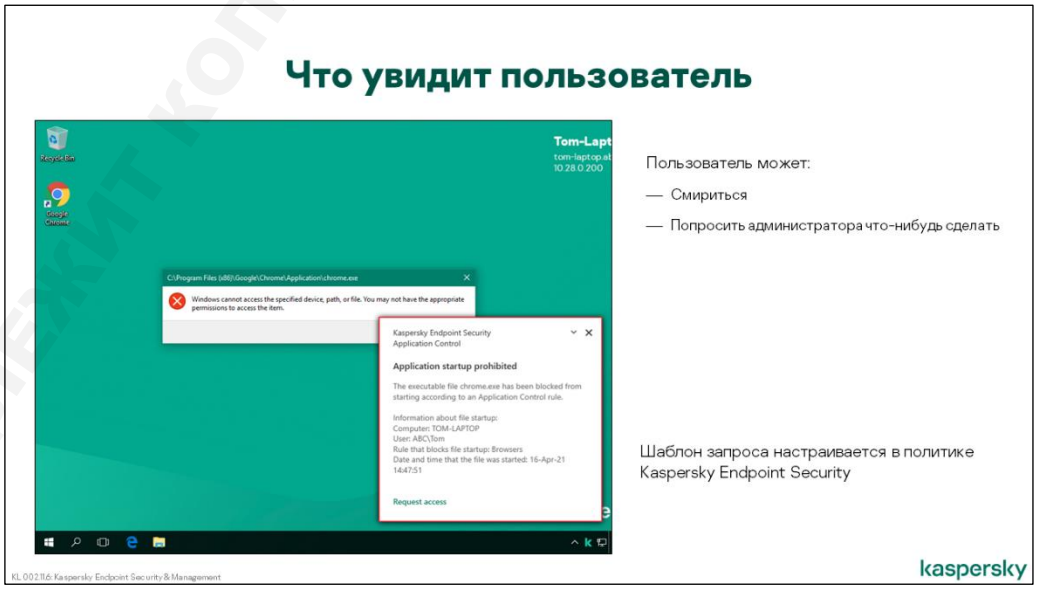
Как определить, что именно запрещено конкретному пользователю



В политике Kaspersky Endpoint Security рядом со списком правил контроля запуска есть кнопка **Статический анализ**. Если ее нажать, откроется окно. В нем можно в левой части выбрать пользователя или группу, и в правой получить список категорий, которые ему будут запрещены, и список непосредственно файлов.

Статический анализ доступен только через MMC-консоль.

Локальные уведомления и запросы пользователей

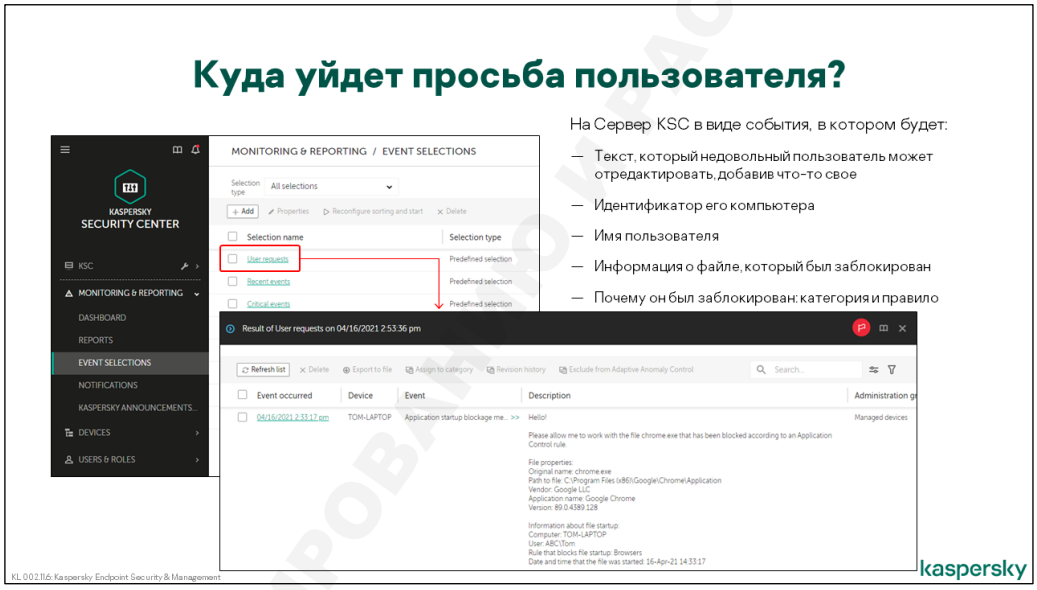


Когда на клиентском компьютере блокируется запуск программы, Kaspersky Endpoint Security открывает всплывающее окно с уведомлением о том, что программа была заблокирована. Это делается, чтобы у пользователя не возникло заблуждения относительно причин, по которым программу нельзя запустить.

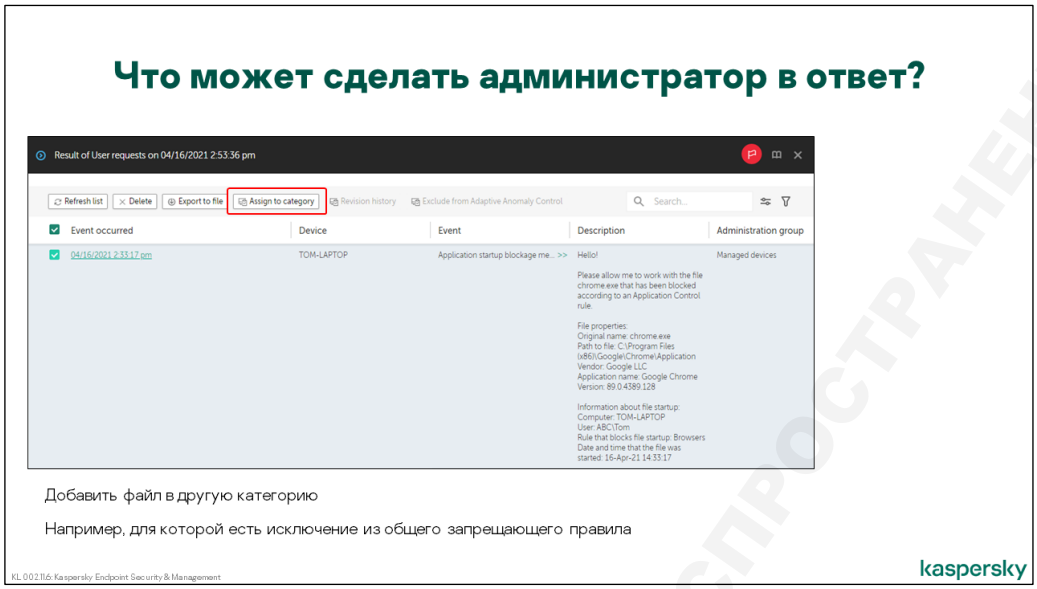
Если программа необходима пользователю для выполнения работы, он может использовать всплывающее уведомление, чтобы отправить администратору запрос о разрешении запуска программы. Для этого нужно нажать в окне уведомления ссылку **Запросить доступ** и нажать кнопку **Отправить**.

Текст шаблонов уведомления о запрете и запроса о разрешении запуска программы можно изменить в политике Kaspersky Endpoint Security. В тексте допускается использование переменных, передающих информацию о конкретном событии. Например, имя заблокированной программы, компьютер, на котором произошло событие и т.п.

Выборка Запросы от пользователей



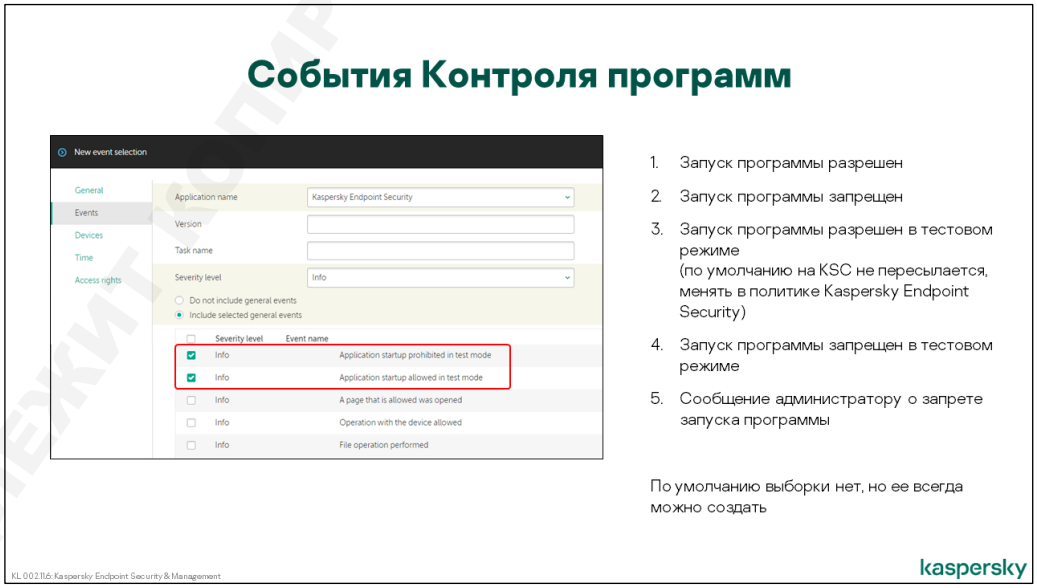
Стандартная выборка событий **Запросы пользователей** содержит события **Сообщение администратору о запрете запуска программы**, зарегистрированные за последние 7 дней. Событие Сообщение администратору о запрете запуска программы регистрируется, когда пользователь отправляет запрос о разрешении запуска, и содержит в себе текст самого запроса. Таким образом, событие содержит информацию о компьютере, имени пользователя и программе, которую требуется разрешить — т.е. всю информацию, необходимую администратору для принятия решения.



Вполне может оказаться, что программа требуется пользователю срочно. Поэтому, если администратор заглядывает в выборку **Запросы пользователей** не часто, имеет смысл настроить почтовое уведомление для события **Сообщение администратору о запрете запуска программы**. Это позволит администратору отреагировать на запрос сразу после того, как он будет отправлен.

Запросы от пользователей можно использовать для внесения изменений в категории. Событие содержит всю важную информацию о заблокированном файле, включая его SHA-256 (MD5 для старых версий Kaspersky Endpoint Security). Администратор может использовать команду **Назначить категорию** чтобы включить исполняемый файл в список условий либо в список исключений.

События



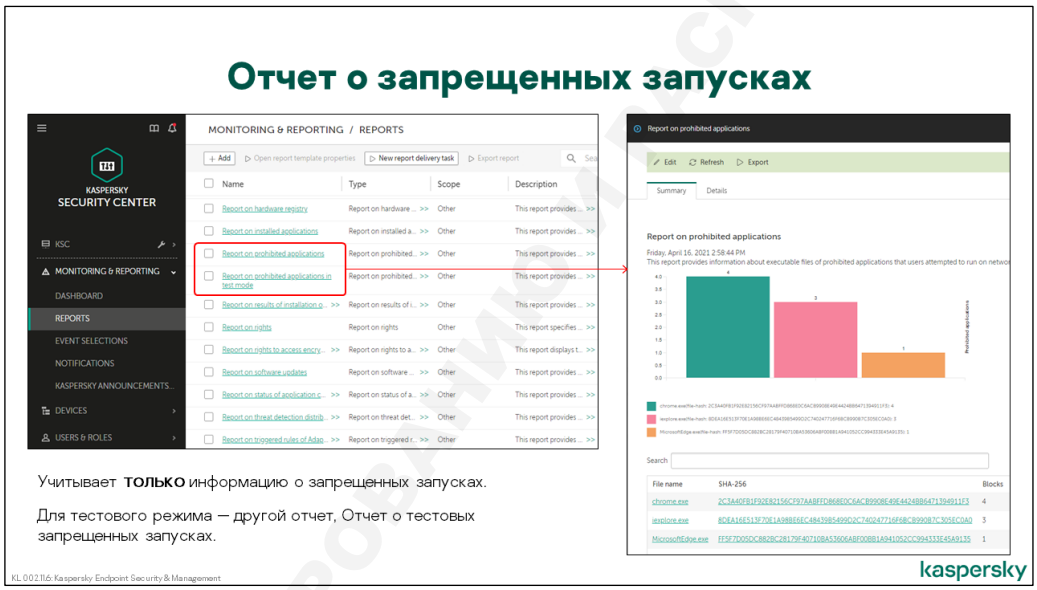
Работа **Контроля программ** описывается всего пятью типами событий:

- Запуск программы разрешен
- Запуск программы запрещен
- Запуск программы разрешен в тестовом режиме
- Запуск программы запрещен в тестовом режиме
- Жалоба на запрет запуска программы

По умолчанию все события, кроме **Запуск программы разрешен**, передаются на Сервер администрирования.

При использовании тестового режима применения правил, имеет смысл создать отдельную выборку для событий **Запуск программы запрещен в тестовом режиме**.

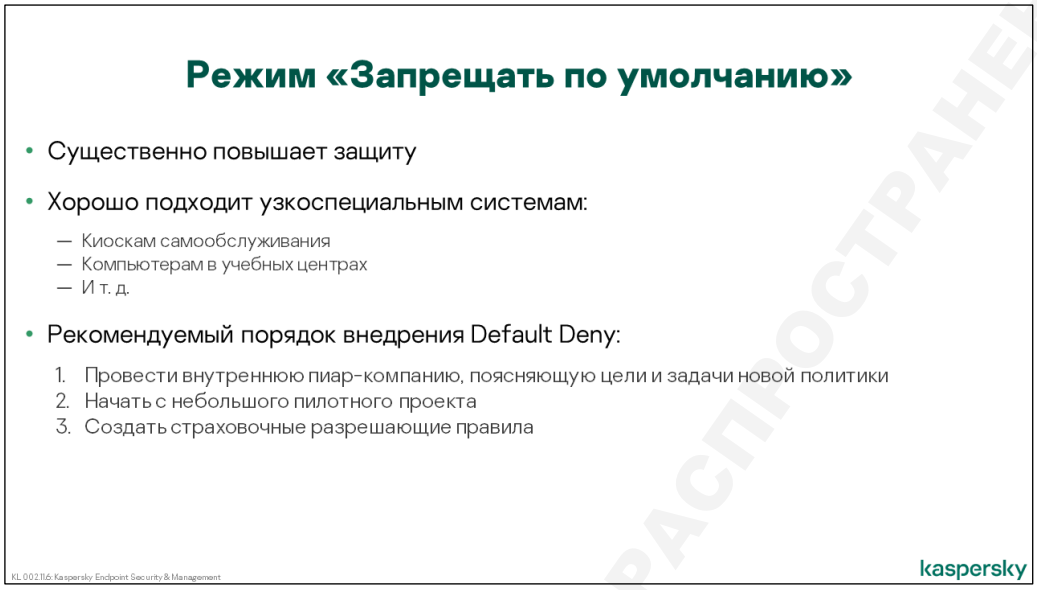
Отчет о запрещенных запусках



На основе событий **Запуск программы запрещен** Kaspersky Security Center строит отчет о запрещенных запусках, в котором показано распределение количества заблокированных запусков на клиентских компьютерах по приложениям. Если перейти на вкладку Details, то откроется список, содержащий информацию обо всех компьютерах и программах, на которых сработал Контроль программ.

Начиная с версии KSC10 SP2 MR1 можно сгенерировать Отчет о запрещенных запусках программ в тестовом режиме. В нем будут события только о запрещенных запусках, вне зависимости от выбранного режима: запрещающий список или разрешающий список.

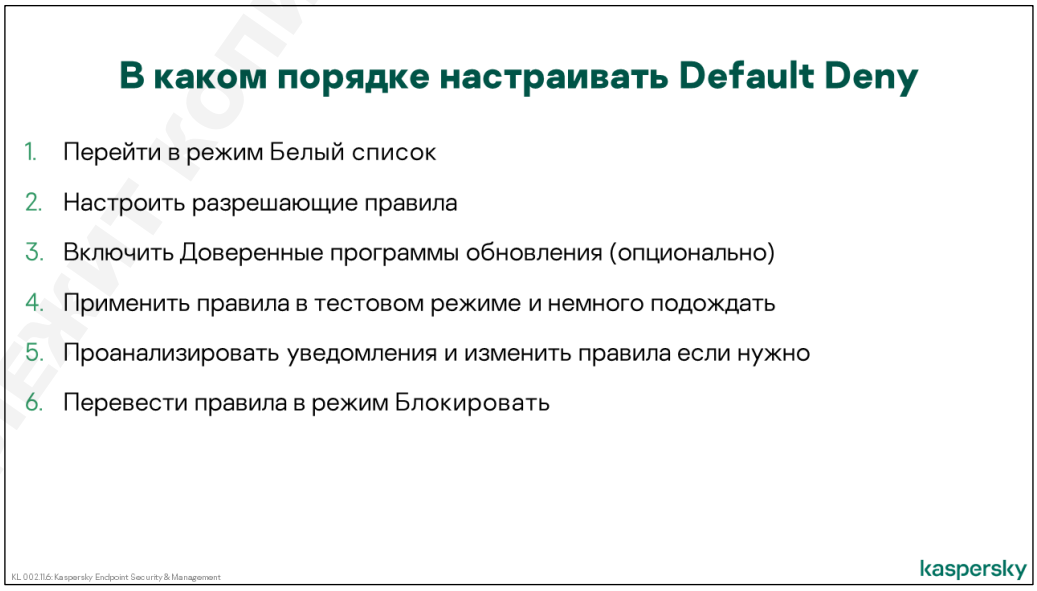
2.5 Режим Default Deny (запрет по умолчанию)



Default Deny (запрет по умолчанию) — сценарий, при котором Контроль программ запрещает на устройстве запуск любых программ, кроме тех, которые указаны в разрешающих правилах Разрешающего списка в Контроле программ.

Главной сложностью при работе в режиме разрешающего списка, когда запуск некатегоризированных программ по умолчанию запрещен, является обеспечение нормальной работы операционной системы, поскольку системные файлы, для которых не установлены разрешения, будут блокироваться так же, как обычные программы. Поэтому разрешающее правило для файлов операционной системы в разрешающем списке есть по умолчанию.

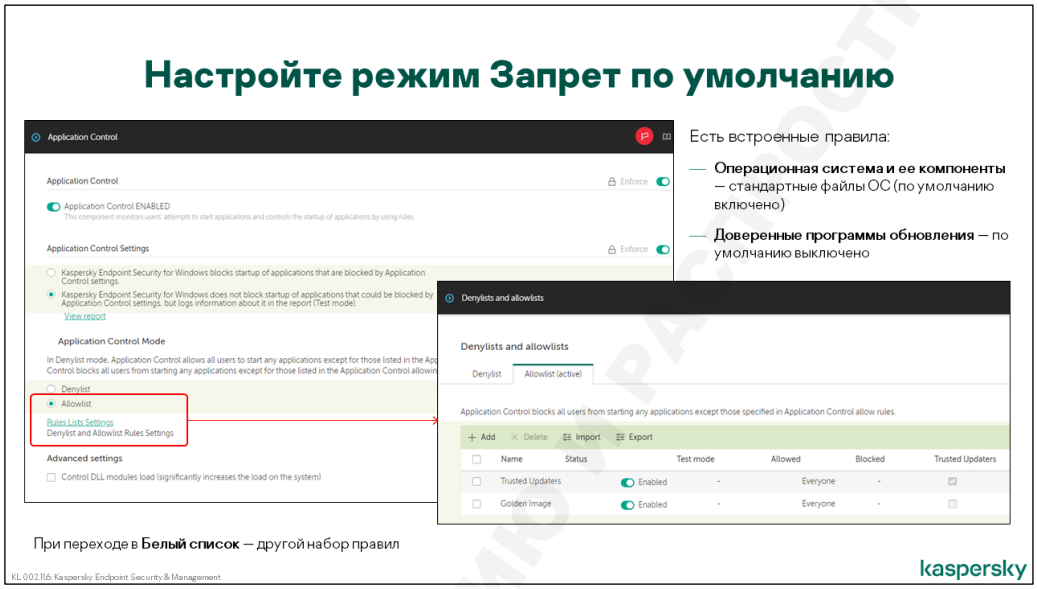
Одним из примеров может быть политика использования программ на компьютерах, являющихся кассовыми терминалами. На них должны запускаться только специализированные программы, а запуск любых неизвестных программ недопустим.



Подходы к настройке разрешающих правил могут быть различны, но в любом случае потребуется создать одну или несколько категорий, для системных исполняемых файлов, и настроить для них разрешающие правила. Категорию можно задать следующими способами:

— Использовать эталонный компьютер с установленной операционной системой и разрешенными программами для создания автоматически наполняемой категории

— Использовать каталог с дистрибутивами разрешенных программ для создания автоматически наполняемой категории

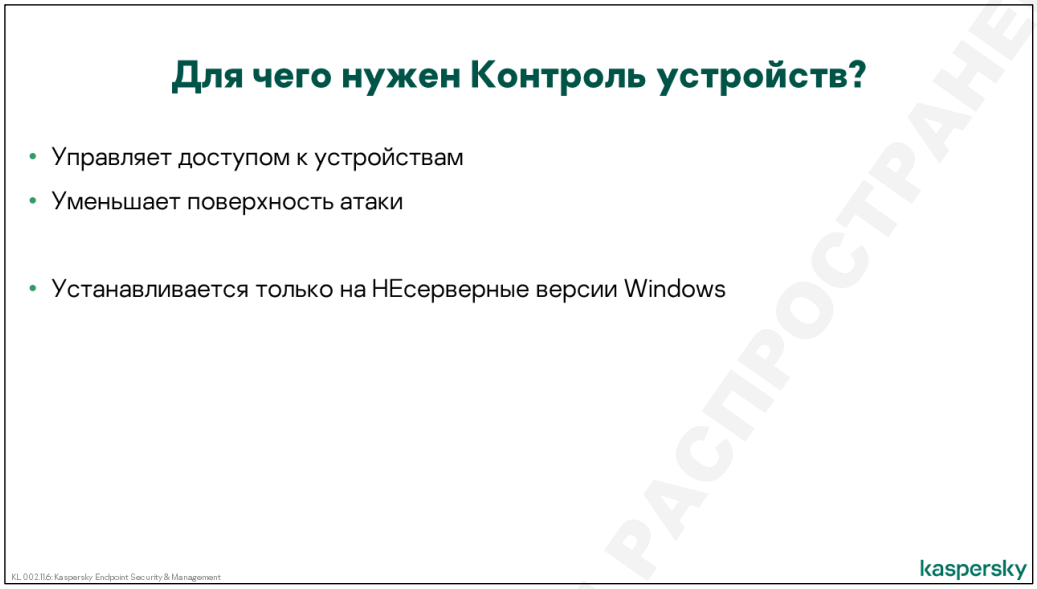


Для того чтобы программы, для которых установлены разрешающие правила, не блокировались при обновлении версии нужно использовать стандартное правило **Доверенные программы обновления**. Это правило присутствует в списке изначально и его нельзя удалить, но по умолчанию оно отключено. Если его включить, программы, загруженные и установленные программами из специальной KL-категории **Доверенные программы обновления**, не будут блокироваться, даже при отсутствии разрешающих правил.

Кроме того, администратор имеет возможность вручную назначать отдельные категории доверенными программами обновления. Для этого в свойствах разрешающего правила нужно включить опцию **Доверенные программы обновлений**.

Более подробно о настройке Kaspersky Endpoint Security для Default Deny рассказывается в отдельном однодневном курсе.

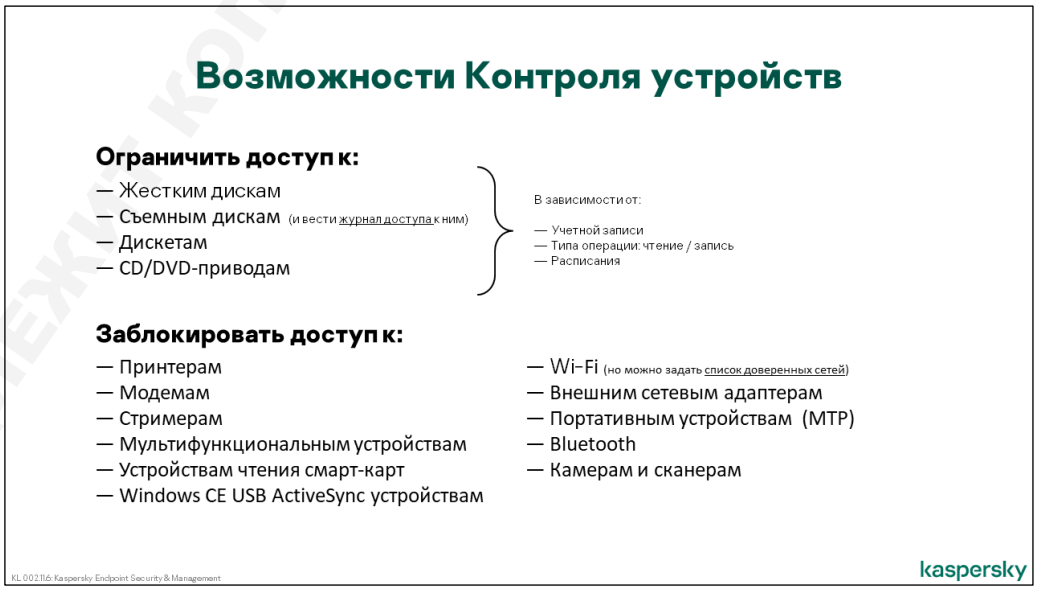
3. Контроль устройств



Основная задача Контроля устройств легко угадывается из названия — обеспечить администратора средством, которое позволяет отследить и, при необходимости, запретить использование в корпоративной сети устройств разных типов.

Компонент Контроль устройств позволяет администратору ввести корпоративный стандарт, указав кому, когда и какие устройства можно использовать на своем компьютере. Правила могут применяться к съемным носителям, принтерам, CD/DVD, подключению к посторонним сетям, Wi-Fi, Bluetooth и т.п.

Наиболее известный сценарий использования компонента — запрет на подключение флэш-накопителей. Пользователь может принести из дома зараженный файл, случайно или преднамеренно унести домой на флэш-накопителе или USB-диске файлы, представляющие коммерческую ценность для компании. Подключить рабочий компьютер к сети Интернет с помощью смартфона. Во избежание подобных проблем и вводятся различные запреты.



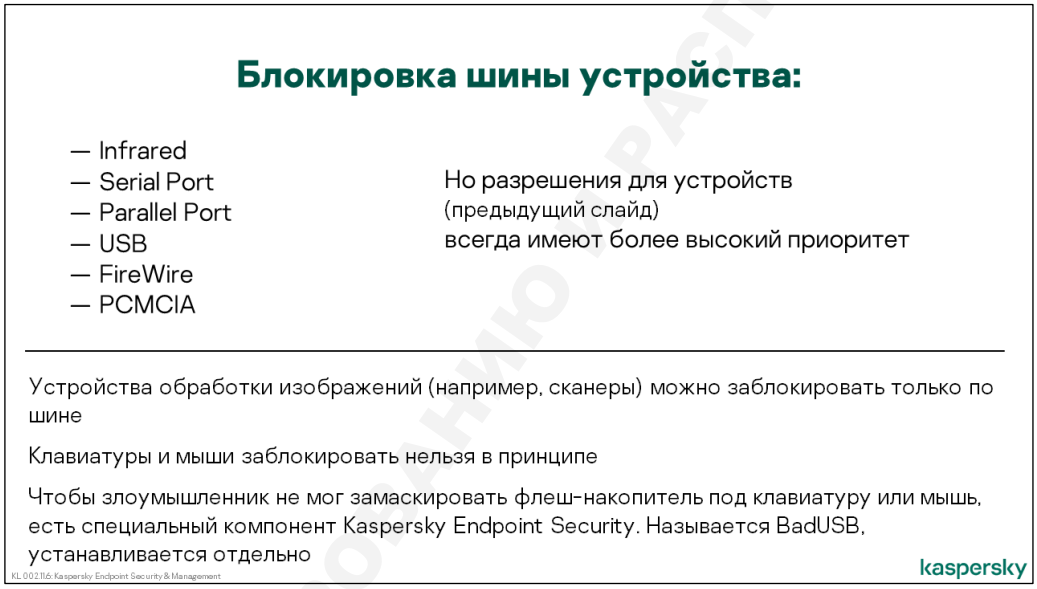
Для разных типов устройств доступны разные настройки. Максимально гибкие настройки доступны для таких устройств хранения данных, как:

- Жесткие диски
- Съемные диски
- Дискеты
- CD/DVD-приводы

Можно указать учетные записи, которым будет разрешен/запрещен доступ, можно разрешить только копировать информацию с устройства, но запретить записывать на него или можно вообще настроить расписание, чтобы доступ к устройствам был разрешен только в рабочее время.

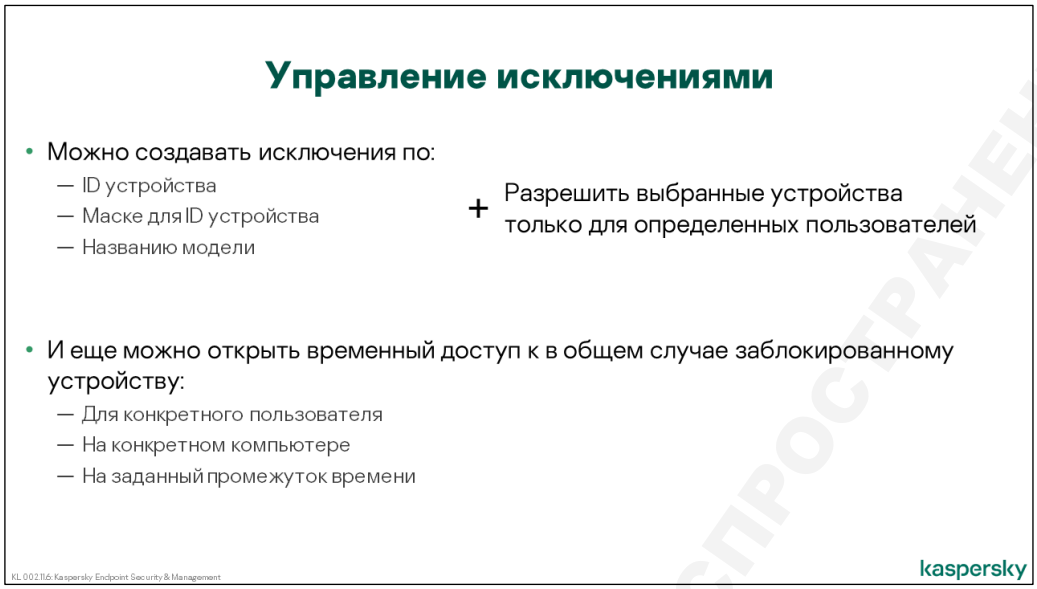
К остальным типам устройств можно применить только действие разрешить/запретить доступ, без гибких настроек.

Отдельно стоит сказать о типе устройства Wi-Fi, но об этом чуть позже.



Более глобально Контроль устройств может заблокировать целиком шину подключения, т.е. все устройства, которые будут подключаться к определенному физическому порту компьютера будут недоступны.

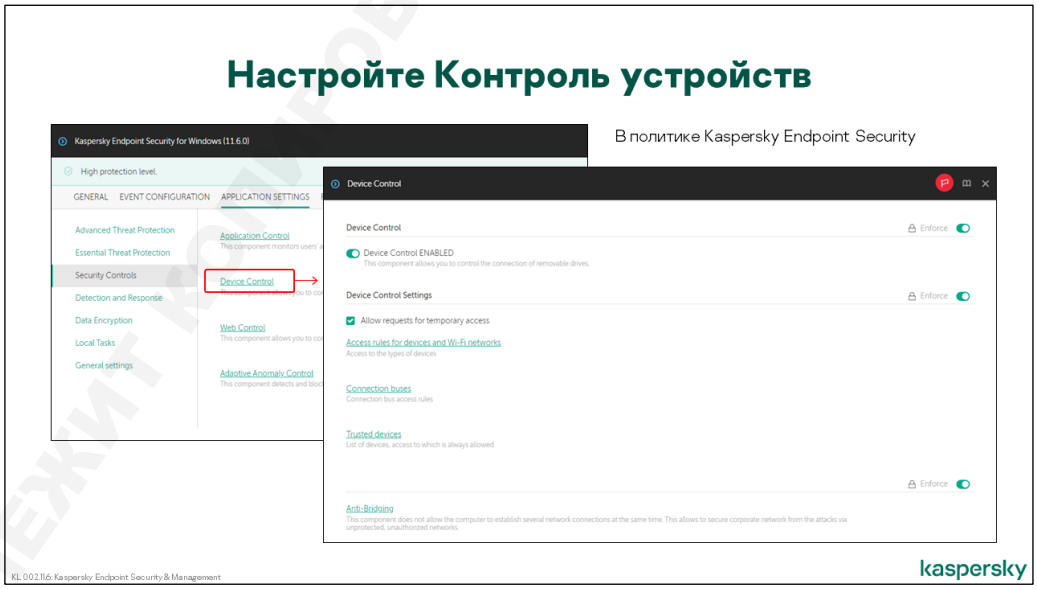
Примечание: клавиатуру и мышь заблокировать нельзя, на них правила контроля устройств не действуют. Для защиты от атак, когда зараженная флешка имитирует, что она клавиатура, нужно установить и использовать отдельный компонент — BadUSB



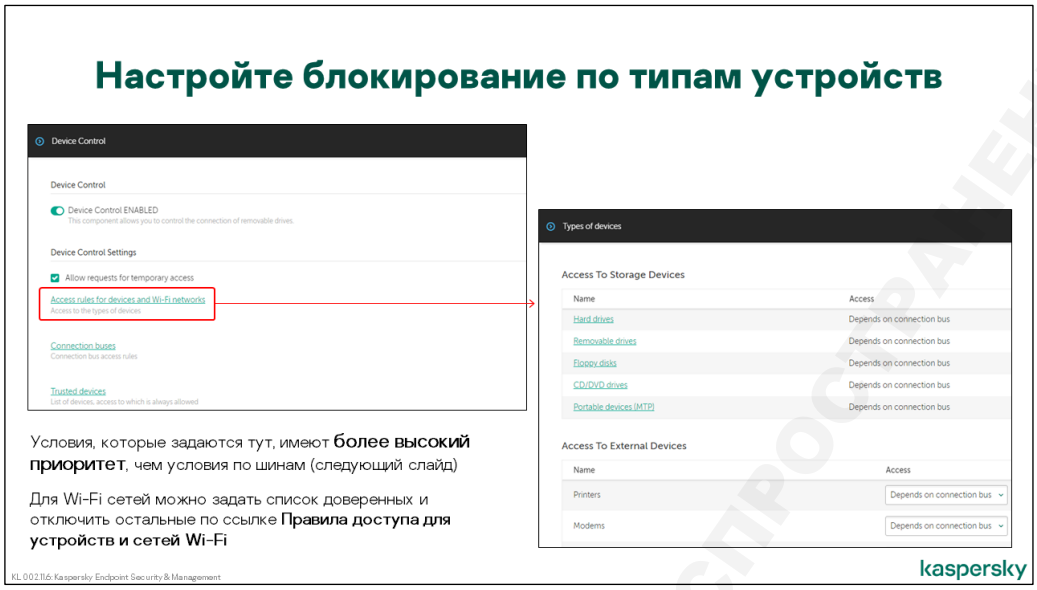
Компонент Контроль устройств позволяет вести список доверенных устройств, доступ к которым будет всегда разрешен, независимо от правил. Плюс для доверенного устройства можно добавить определенных пользователей, которые смогут работать с этим устройством.

Также при необходимости администратор сможет предоставлять временный доступ к заблокированным устройствам, если пользователю нужно срочно для работы воспользоваться таким устройством.

3.1 Что можно заблокировать и как это сделать



Контроль устройств настраивается в политике Kaspersky Endpoint Security. Из свойств компонента можно сразу попасть в настройки правил по типам устройств, по шинам подключения, открыть список доверенных устройств или перейти к настройке фукционала Анти-Бриджинг.



Для некоторых из устройств можно явно задать время действия запрета, ввести его только для отдельных операций или сделать исключение для ряда пользователей. Фактически, такие устройства будут разрешены, но с ограничениями. Это можно сделать для:

- Жестких дисков
- Съемных дисков
- Дискет
- CD/DVD-диски

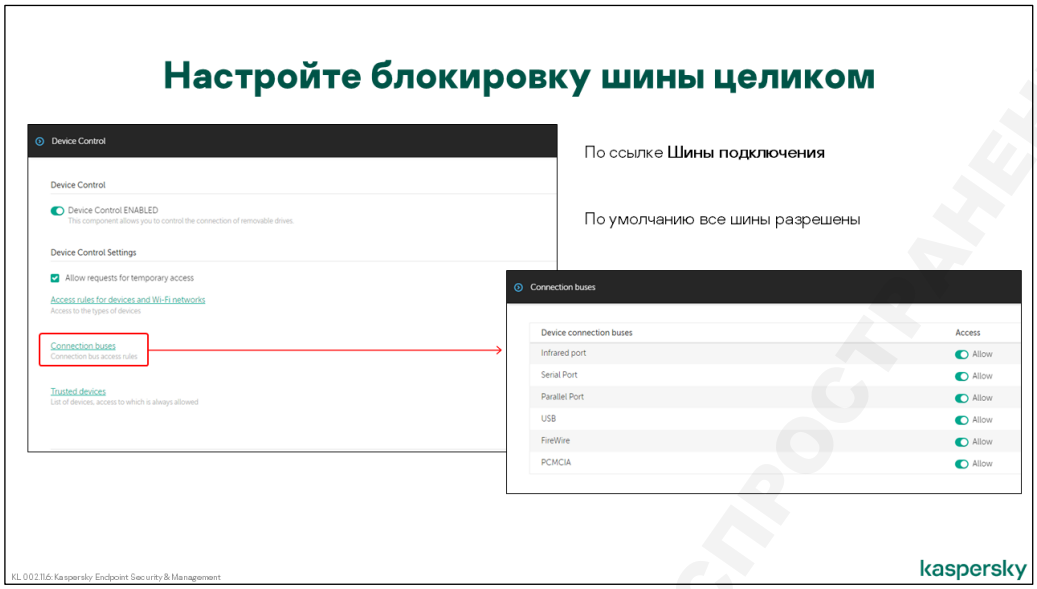
Остальные типы устройств можно только отключить целиком:

- Принтеры
- Модемы
- Стримеры
- Мультифункциональные устройства
- Устройства для чтения смарт-кард
- Windows CE USB ActiveSync устройства
- Сканеры и камеры
- Устройства чтения смарт-карт
- Портативные устройства (MTP)
- Bluetooth

В отдельную группу выделен доступ к Wi-Fi сетям, о нем немного позже.

Мобильные телефоны, планшеты, плееры и другие портативные устройства могут относиться к Портативным устройствам (MTP) или к Сменным дискам, если подключаются просто как внешние носители информации.

Приведенный список не содержит устройства для обработки изображений, в частности, сканеров. Их тоже можно запретить, но только отключив шину, по которой они подключаются.



Kaspersky Endpoint Security позволяет блокировать устройства, подключаемые по типу интерфейса (шине):

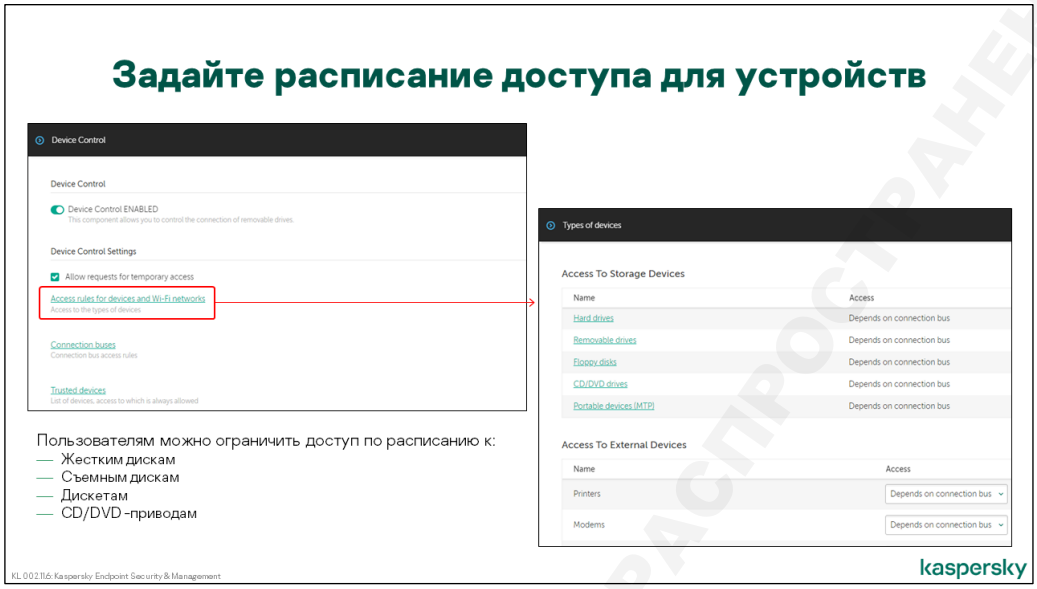
- USB
- FireWire
- Infra-Red
- Serial Port
- Parallel Port
- PCMCIA

То есть администратор может полностью отключить, например, все устройства, работающие через USB.

Правила для устройств имеют больший приоритет. Если запретить шину USB, но разрешить Съемные диски, USB флэш-накопители работать будут.

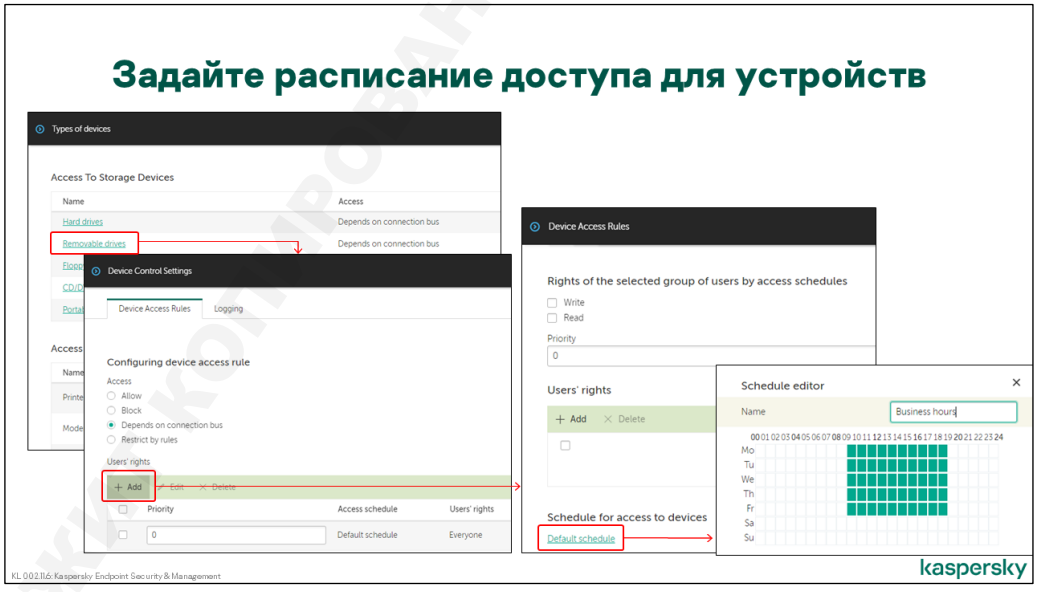
По умолчанию все устройства работают «*в зависимости от настроек шин*», по которым они подключаются, и все шины в свою очередь разрешены.

Дополнительные параметры



Kaspersky Endpoint Security позволяет блокировать только те типы устройств, которые есть в списке. Самостоятельно отредактировать этот список, чтобы добавить новые устройства, нельзя.

Для флеш-накопителей, CD/DVD, жестких дисков и дискет можно задать гибкие ограничения на их использование.



Доступны следующие ограничения:

— **Что можно с ними делать: можно отдельно запретить только чтение или запись**

— **Пользователи и/или группы пользователей,** для которых они будут доступны. Выбирать можно из учетных записей домена, в который входит компьютер с запущенной консолью администрирования, или локальных пользователей, если домена нет. Разрешение будет действовать на любом компьютере, находящимся под действием этой политики. Всегда доступна только универсальная запись **Все**

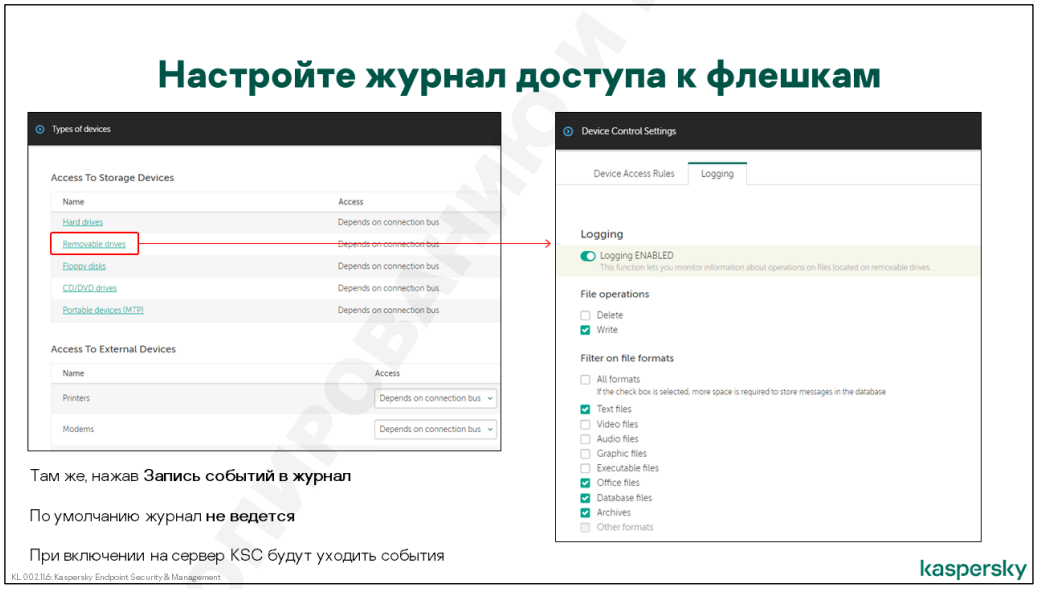
— **Расписание доступа** — когда доступ запрещен или наоборот, разрешен. Можно независимо управлять чтением и записью. Время задается с точностью до часа и дня недели. Например, можно разрешить операции чтения с флэш-накопителей и дисков каждый рабочий день с 8-00 до 21-00, а операции записи позволить лишь администраторам и только в рабочее время

Если пользователь попадает одновременно под несколько правил, будет применено наиболее жесткое из них. Если устройство «*разрешено*», это значит «*всегда всем разрешать любые операции*».

Комбинируя перечисленные правила, можно, например, запретить USB-устройства и все съемные диски, но для администраторов сделать исключение — в рабочее время разрешить им использовать флэш-накопители.

Измененная политика начнет действовать сразу же после ее применения. Если, например, запретить съемные носители в то время, как пользователь уже успел подключить себе флэш-накопитель и что-то на нее скопировать, сразу после применения политики она станет недоступна и следующая операция заблокируется.

Журнал доступа к флешкам



Если в компании флешки в принципе разрешены, но компания их использование не приветствует, можно настроить ведение журнала доступа к флешкам. Тогда при каждой из выбранных операций на Сервер администрирования будет отправляться соответствующее событие — **Выполнена операция с файлом**. В нем будет указано кто (под какой учетной записью) и какой файл скопировал или удалил.

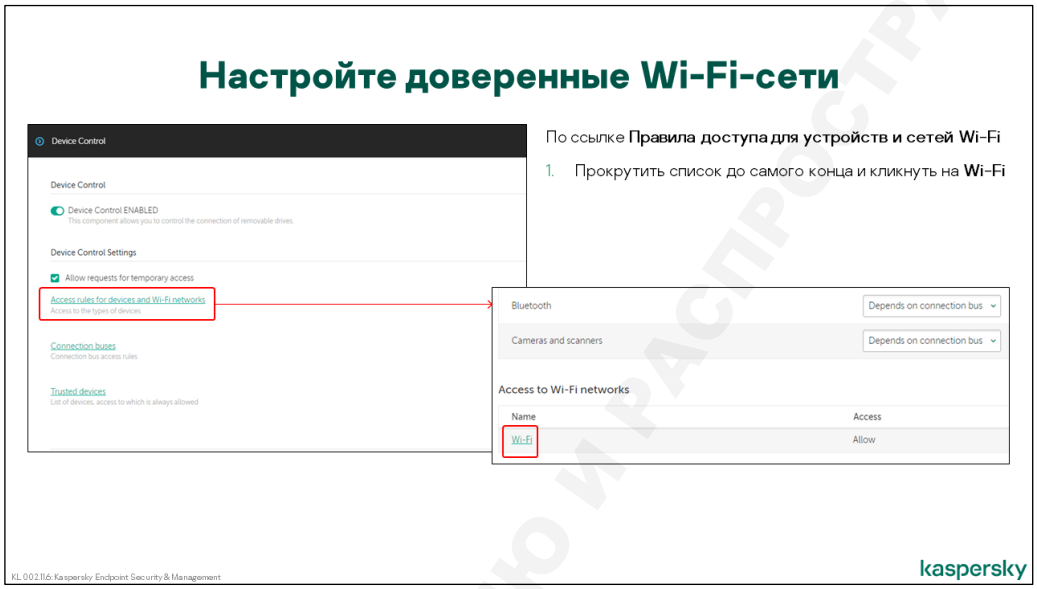
В отличие от других событий, это событие локально храниться не будет.

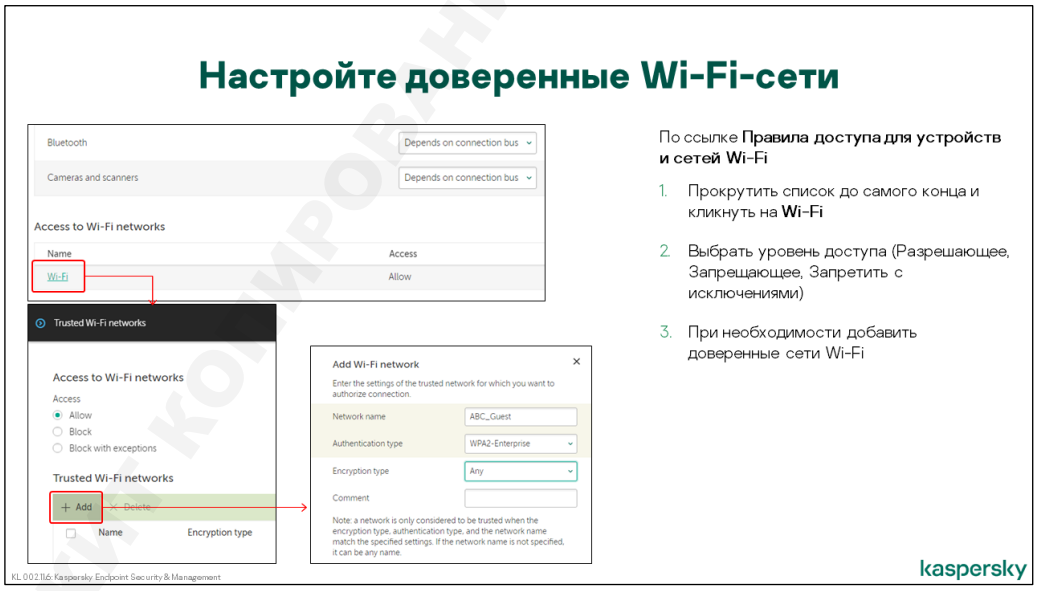
По умолчанию журнал доступа к флешкам отключен. Включается он нажатием кнопки **Запись событий в журнал**. Кнопка появляется только при выборе флешек. Можно выбирать между операциями: запись и/или удаление, и форматами файлов:

— текстовые файлы
— видео-файлы
— аудио-файлы
— графические файлы

— исполняемые файлы
— файлы офисных форматов
— базы данных
— архивы

Как задать доверенные Wi-Fi-сети



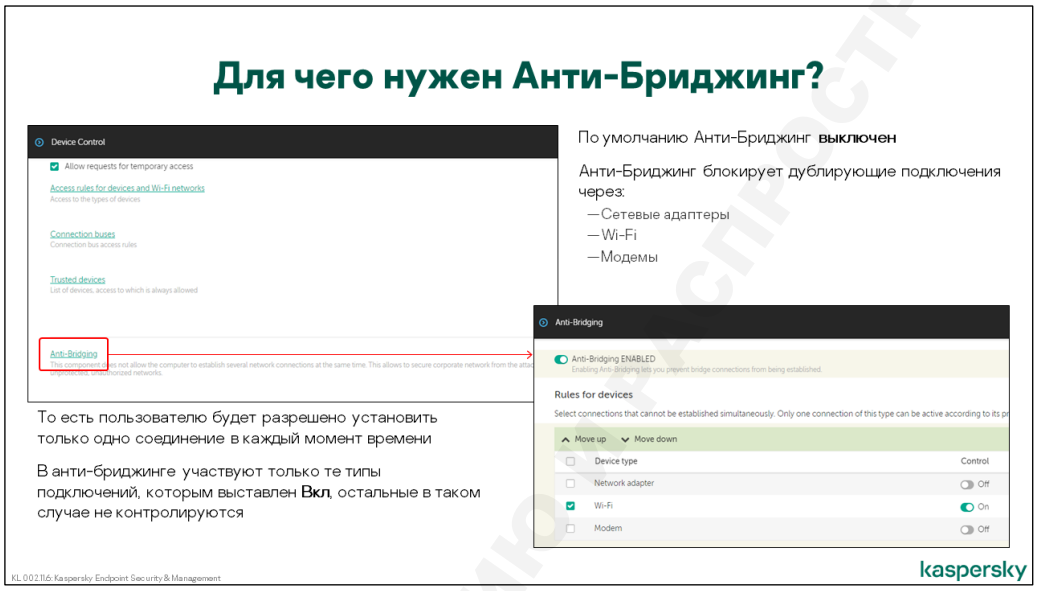


Контроль устройств позволяет контролировать Wi-Fi сети, возможны три варианта действия при подключении к сети:

— **Разрешать**
— **Запрещать**
— **Запрещать с исключениями** — этот параметр содержит дополнительные настройки, которые позволяют сформировать список доверенных Wi-Fi сетей используя параметры: имя сети, тип аутентификации, тип шифрования. Сеть считается доверенной только при совпадении всех указанных параметров. Если имя сети не задано, то оно может быть любым.

Подключение к публичным сетям Wi-Fi с корпоративных ноутбуков не всегда желательно. С помощью **Контроля устройств** можно отключить Wi-Fi. Но для ноутбуков, которые пользователи могут забирать домой, это не самый оптимальный вариант. Для них логичней будет в общем случае применить правило **Запрещать с исключениями**, включив в него список доверенных сетей: например, корпоративную и домашнюю.

Что делает Анти-Бриджинг



В состав **Контроля устройств** входит компонент **Анти-Бриджинг**, который позволяет запретить пользователям одновременно устанавливать два сетевых соединения, чтобы предотвратить несанкционированное создание мостов к внутренней сети в обход средств защиты периметра.

Например, компьютер пользователя подключен к корпоративной сети. Пользователь подключил Wi-Fi адаптер к своему компьютеру и настроил его в роли беспроводной точки доступа. К этой точке доступа могут подключиться не только те, для кого она предназначалась, но и злоумышленник, который может использовать эксплоиты для конкретного адаптера, подобрать логин/пароль или другие способы обхода защиты. В итоге компьютер пользователя будет скомпрометирован и у злоумышленника появится стартовая площадка для дальнейшего развития вектора атаки. В данном случае **Анти-Бриджинг** является одной из ступеней защиты, которая не позволит злоумышленникам сразу получить доступ к внутренней сети организации, т.к., когда пользователь включит Wi-Fi адаптер, **Анти-Бриджинг** автоматически разорвет все сетевые соединения, в том числе доступ к локальной сети, и активной останется только Wi-Fi сеть.

Аналогичная угроза безопасности корпоративной сети может возникнуть, если ноутбук пользователя подключен к сети предприятия с помощью проводного соединения. Пользователь, чтобы обойти средства защиты организации, включил свой смартфон в режиме точки доступа и по Wi-Fi подключил к нему ноутбук. После чего случайно или целенаправленно зашел на какую-либо страницу в сети Интернет содержащую эксплоит-пак, который скомпрометировал пользовательский ноутбук, и злоумышленник получили возможность из сети Интернет сразу атаковать внутреннюю сеть предприятия.

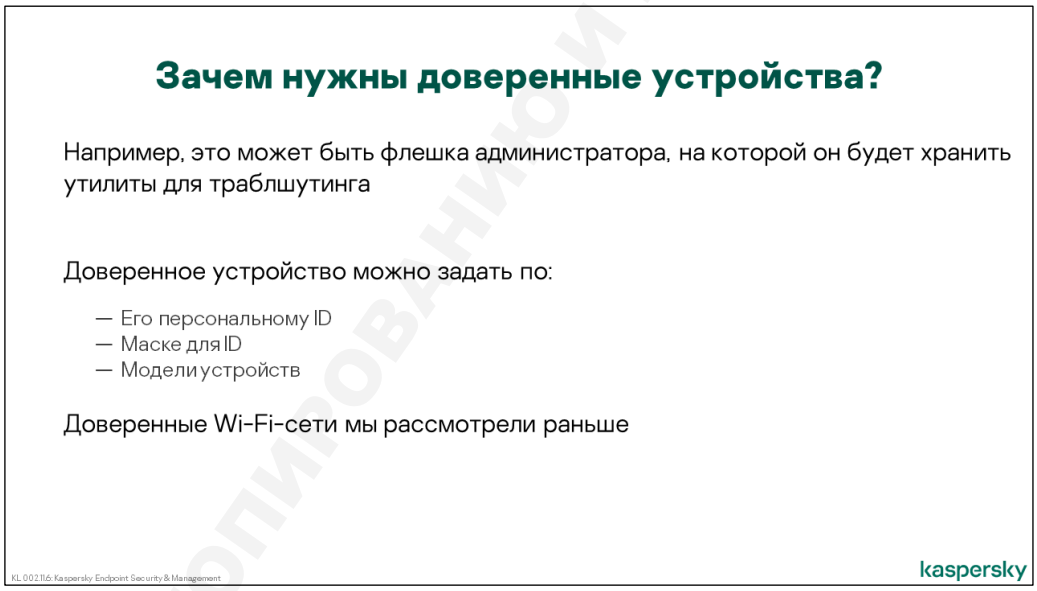
В обоих случаях на компьютере пользователя, подключенного к сети организации, появляются две сети — локальная и Wi-Fi. Чтобы исключить одновременную работу двух сетей и отдать предпочтение, например, проводному подключению, администратор в настройках **Анти-Бриджинг** должен все контроли перевести в режим **Вкл**. при этом установить максимальный приоритет сетевому адаптеру. В этом случае пока пользователь не отключит проводную сеть, на его компьютере Wi-Fi сеть не включится.

По умолчанию компонент **Анти-Бриджинг** выключен, чтобы его включить в свойствах **Контроль устройств** нажмите одноименную ссылку и в открывшемся окне переведите компонент в состояние **Включен**. После включения **Анти-Бриджинг** Kaspersky Endpoint Security блокирует уже установленные соединения в соответствии с правилами установки соединений. Чем выше правило в списке, тем выше у него приоритет. **Анти-Бриджинг** может блокировать все соединения, кроме одного соединения с максимальным приоритетом. Для этого в окне **Анти-Бриджинг** включите все контроли в режим **Вкл**. и определите приоритеты для всех устройств, которые можно контролировать:

- Сетевой адаптер
- Wi-Fi
- Модем

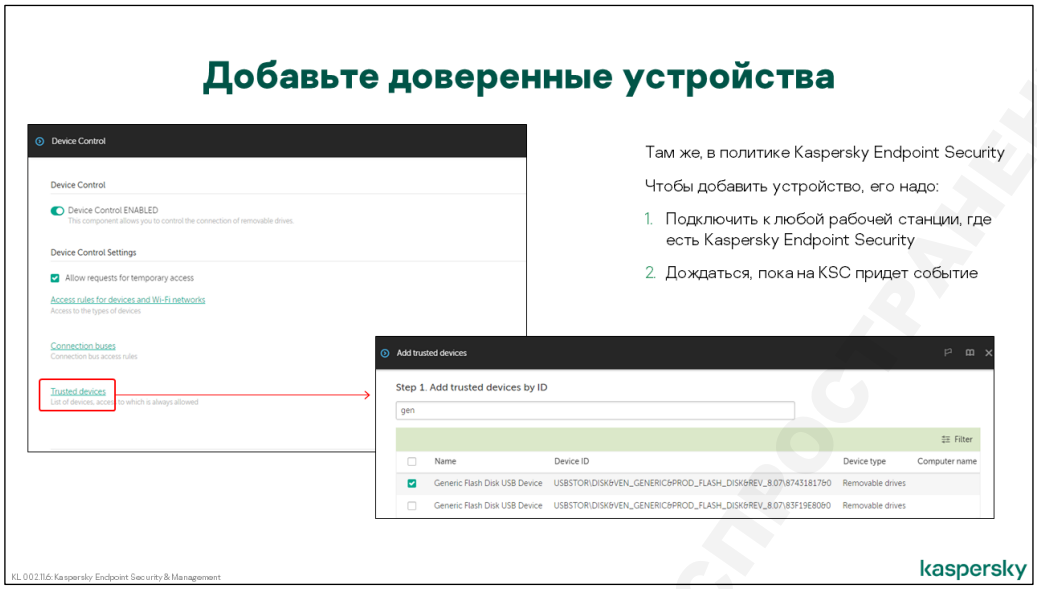
Примечание: Если проводных соединений несколько, разрешает одно из них (произвольное). Если адаптер Wi-Fi не подключен к сети, он не блокируется и не выглядит заблокированным, пока пользователь не пытается подключиться к сети.

3.2 Как задать доверенные устройства



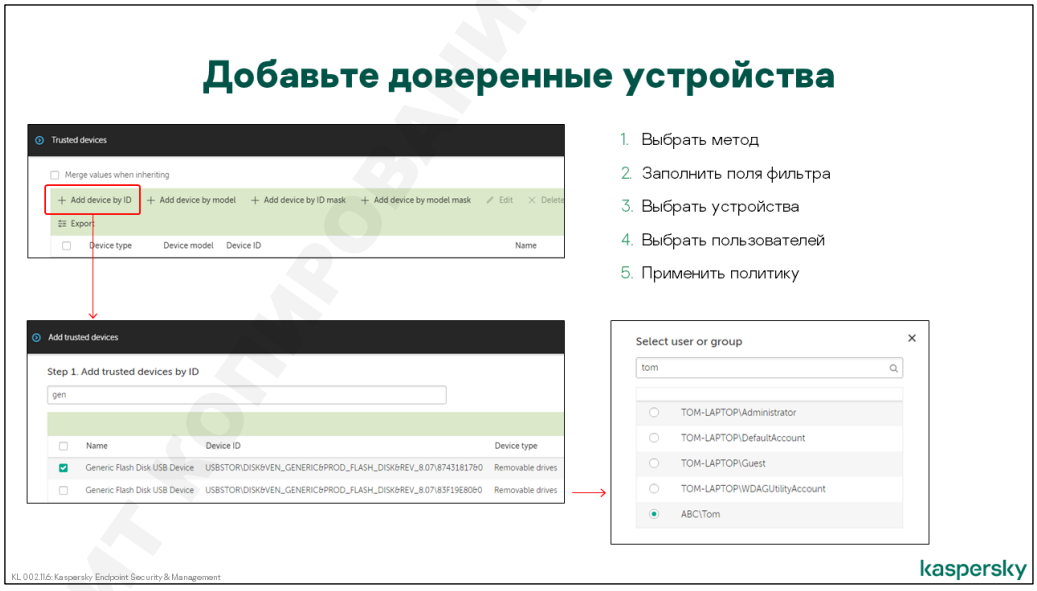
Если в компании есть набор администраторских съемных дисков, которые должны быть разрешены всегда и везде, имеет смысл сделать их доверенными.

Устройства могут назначаться доверенными на основании ID (идентификатора), маски ID или модели.



Доверенные устройства указываются в политике Kaspersky Endpoint Security, компонент **Контроль устройств**, ссылка **Доверенные устройства**.

Чтобы информация об устройстве была доступна в политике, его нужно сначала подключить к рабочей станции, где есть Kaspersky Endpoint Security с установленным компонентом Контролем устройств и затем дождаться пока на Сервер администрирования придет событие о подключении.



Доступны три опции:

- Устройство по идентификатору
- Устройство по модели
- Устройство по маске идентификатора

Первые две опции позволяют выбрать устройство, которое нужно сделать доверенным, и модель и ID (идентификатор) будут добавлены в список. При выборе устройство должно числиться в базе данных Kaspersky Security Center. Если устройство Серверу администрирования неизвестно сделать его доверенным не получится.

Опция **Устройство по маске идентификатора** позволяет указать ID устройства или его часть. Этот процесс не зависит от того, знает ли об устройстве Сервер администрирования, и зависит только от знания самим администратором номера идентифицирующего устройства. Посмотреть ID можно в свойствах устройства Диспетчере устройств Windows на закладке **Сведения**. Откройте атрибут Путь к экземпляру устройства. Он будет выглядеть приблизительно так:

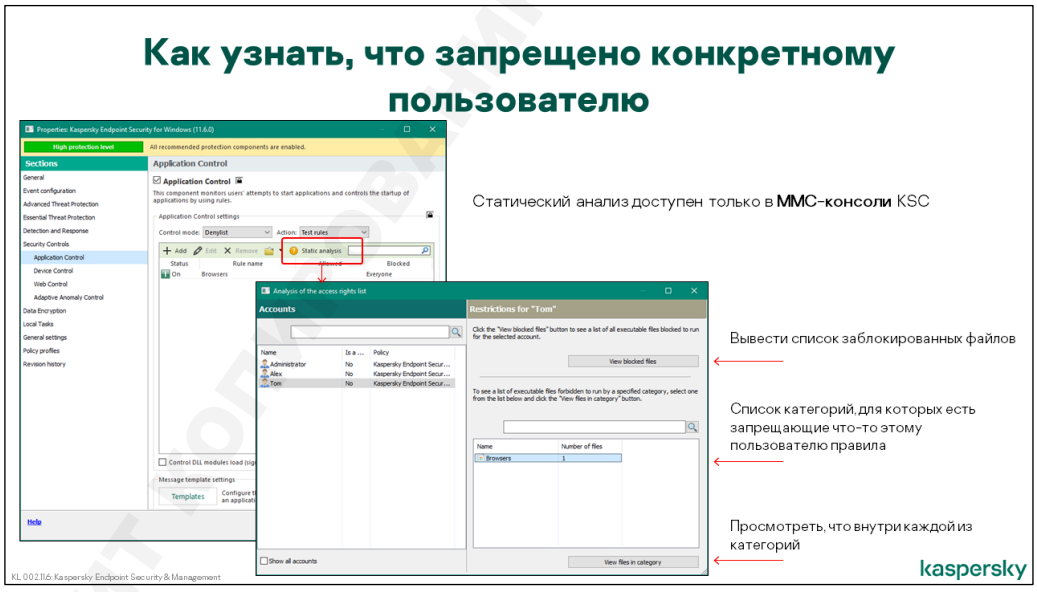
USBSTOR\DISK&VEN_&PROD_USB_FLASH_DRIVE&REV_1.01\574B17001160&0

При добавлении маски часть ID можно заменить символами «*» или «?», чтобы сделать доверенными сразу группу устройств, например, ‘*NEC*CDR??*’. Это удобно, когда у компании есть группа устройств, со схожими ID, которые нужно сделать доверенными. Добавить устройство в список доверенных по модели в этом случае тоже поможет, если все устройства однотипны и изготовлены одним производителем.

В поле **Комментарий** можно разместить объяснение, почему устройство (или группа устройств) было сделано доверенным.

Чтобы добавить устройство по модели или ID, не набирая их на клавиатуре, подключите его к управляемому компьютеру, на котором установлен Kaspersky Endpoint Security. Компонент Контроль устройств также должен присутствовать. Затем, требуется некоторое время подождать, пока информация об устройстве будет передана на Сервер администрирования, и добавить его по ID или модели.

Чтобы упростить поиск устройства можно указать его тип или имя, или имя компьютера, к которому оно было подключено. Затем следует нажать кнопку **Обновить**, чтобы увидеть результаты фильтрации.

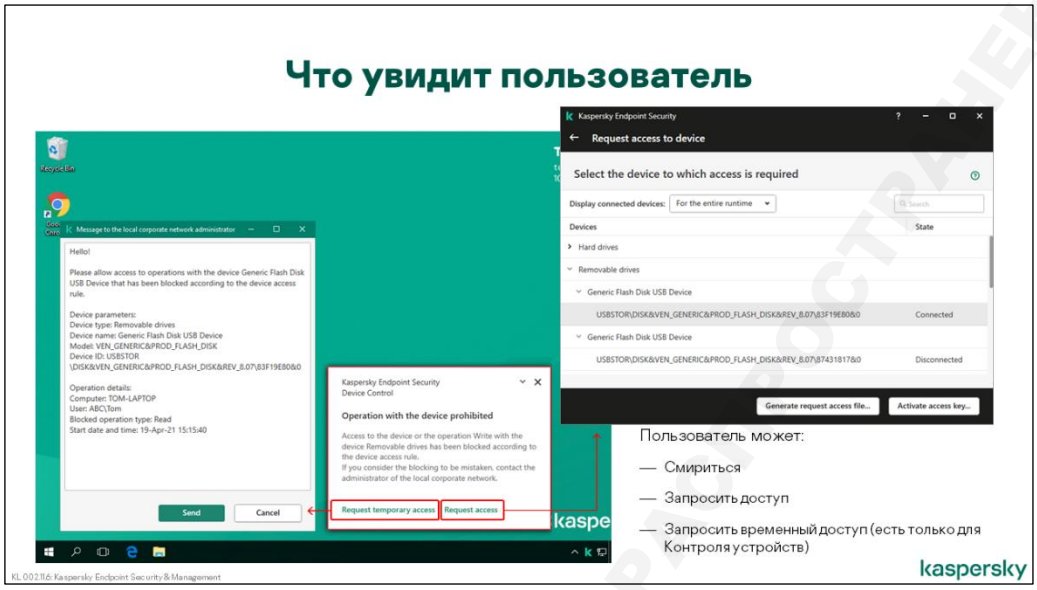


Также есть возможность импорта/экспорта списка доверенных устройств в формате XML. Может быть полезным, например, когда в интерфейсе Kaspersky Security Center требуется отредактировать отображаемое имя доверенного устройства, добавить большое количество однотипных устройств, сохранить резервную копию списка доверенных устройств, перенести список на другой сервер.

Перед добавлением устройства можно ограничить перечень пользователей, у которых будет к нему доступ. Вполне может оказаться, что доступ к доверенному устройству следует предоставлять не всем. Например, только администраторам.

Импорт/экспорт списка устройств доступен только через ММС-консоль.

3.3 Как настроить взаимодействие с пользователем

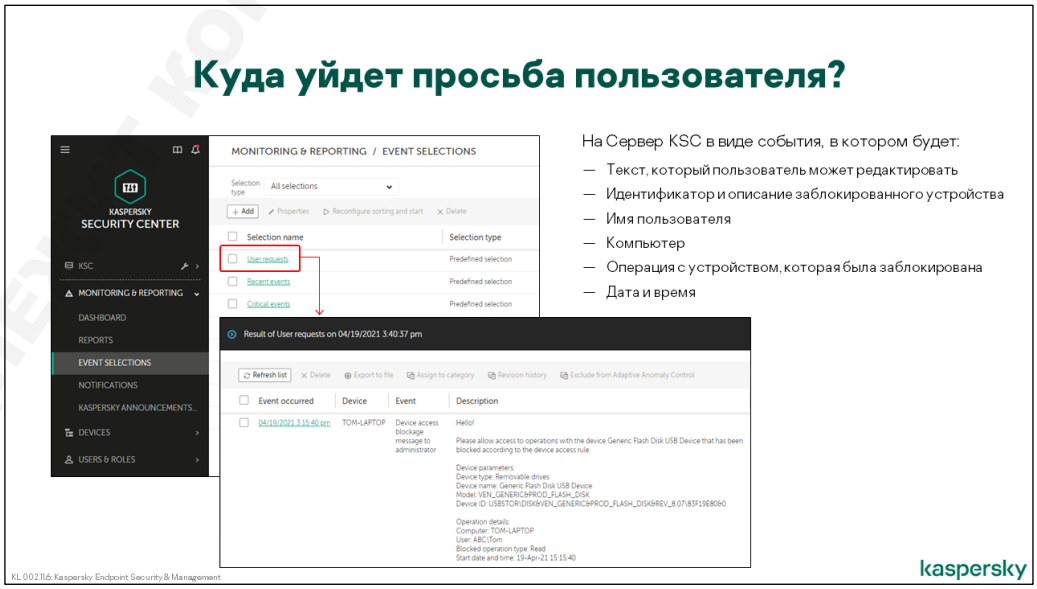


При попытке подключить заблокированное устройство пользователь увидит всплывающее уведомление.

Если его отключить, пользователь может ошибочно подумать, что что-то не в порядке с аппаратным обеспечением. Как следствие, обратиться к технической службе, или пытаться разобраться самому, что может быть еще хуже. Но администратор может изменить текст уведомления, указав, куда и кому звонить за помощью, написать номер телефона и адрес электронной почты.

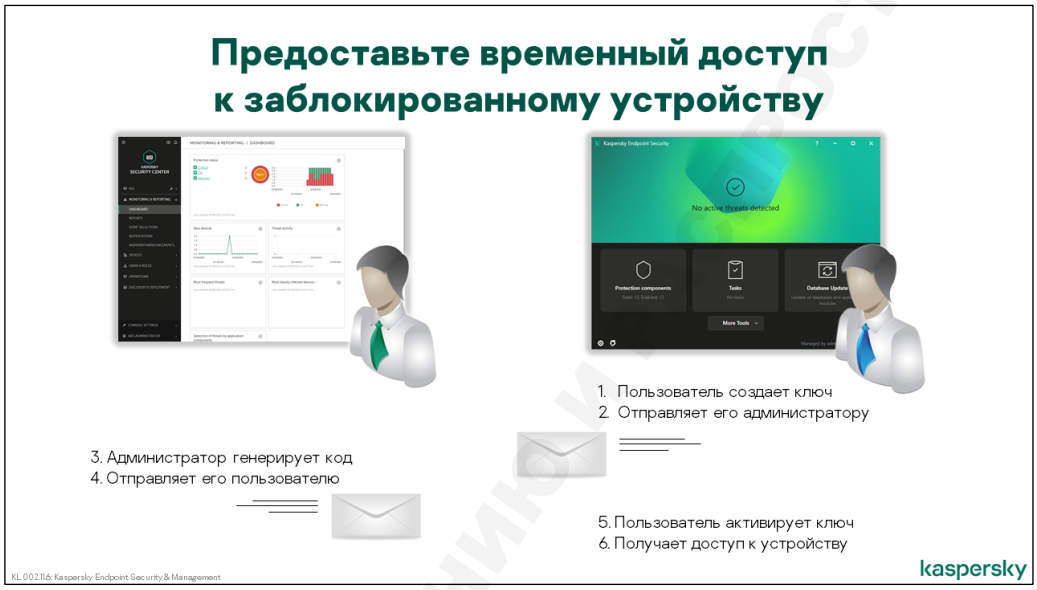
Шаблоны уведомлений доступны в политике Kaspersky Endpoint Security в настройках **Контроля устройств**. При редактировании можно использовать переменные, например, явно упомянуть название устройства, заблокированную операцию.

Если всплывающее уведомление о блокировке включено, в нем по умолчанию будет ссылка *Запросить доступ*. Отключить или спрятать ее нельзя.



Если пользователь отправил запрос, он придет на Сервер в виде события с уровнем важности *Предупреждение*. Как и в случае других компонентов контроля, для запросов предусмотрена отдельная выборка — **Запросы пользователей**. Администратору не обязательно реагировать на запросы, но при желании он может, например, настроить себе уведомление по электронной почте. Это можно сделать в политике Kaspersky Endpoint Security.

3.4 Как настроить временный доступ



В Kaspersky Endpoint Security предусмотрена процедура получения пользователем временного доступа к заблокированному устройству. Оформление запроса и предоставление доступа выполняется следующим образом:

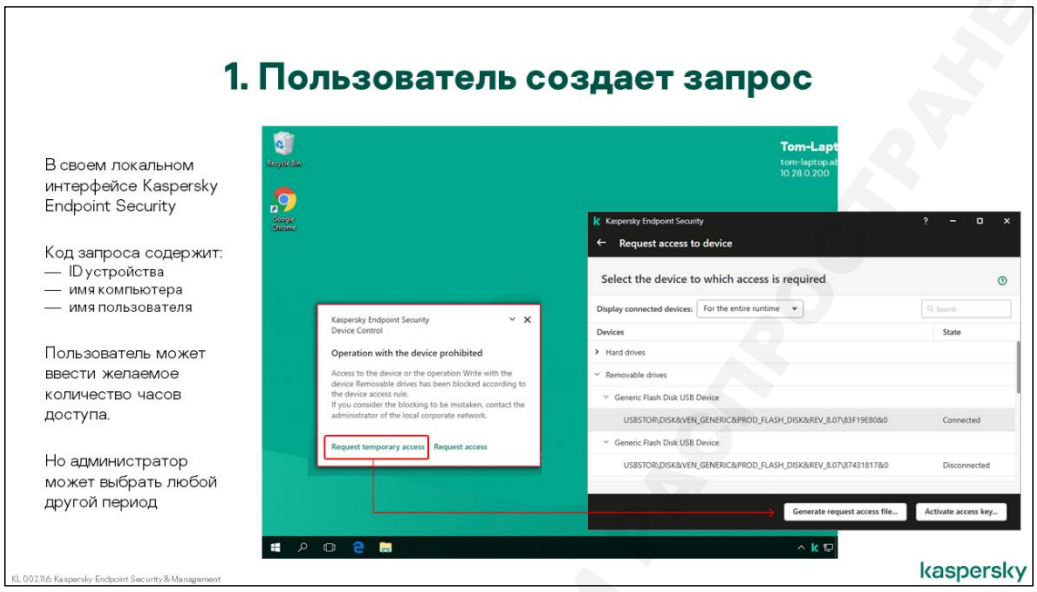
1. Пользователь обнаруживает, что нужное ему устройство заблокировано
2. Используя локальный интерфейс Kaspersky Endpoint Security, генерирует для него файл запроса
3. Отправляет файл запроса администратору по электронной почте
4. Администратор рассматривает запрос, и при положительном ответе создает и высылает пользователю специальный ключ доступа

   Важно: Создать специальный ключ доступа можно только в MMC-консоли.

5. Пользователь активирует полученный ключ. После этого доступ к выбранному устройству, и только к нему, будет временно открыт — на период времени, указанный администратором. Приостановить, чтобы потом запустить, или наоборот, удаленно закрыть, временный доступ нельзя

Разумеется, многие пользователи решат, что их устройства заблокированы ошибочно, и захотят запросить у администратора временный доступ. Чтобы избежать потока запросов, администратор может отключить эту возможность. Для этого в политике Kaspersky Endpoint Security на закладке Контроля устройства нужно снять флаг **Разрешать запрашивать временный доступ**.

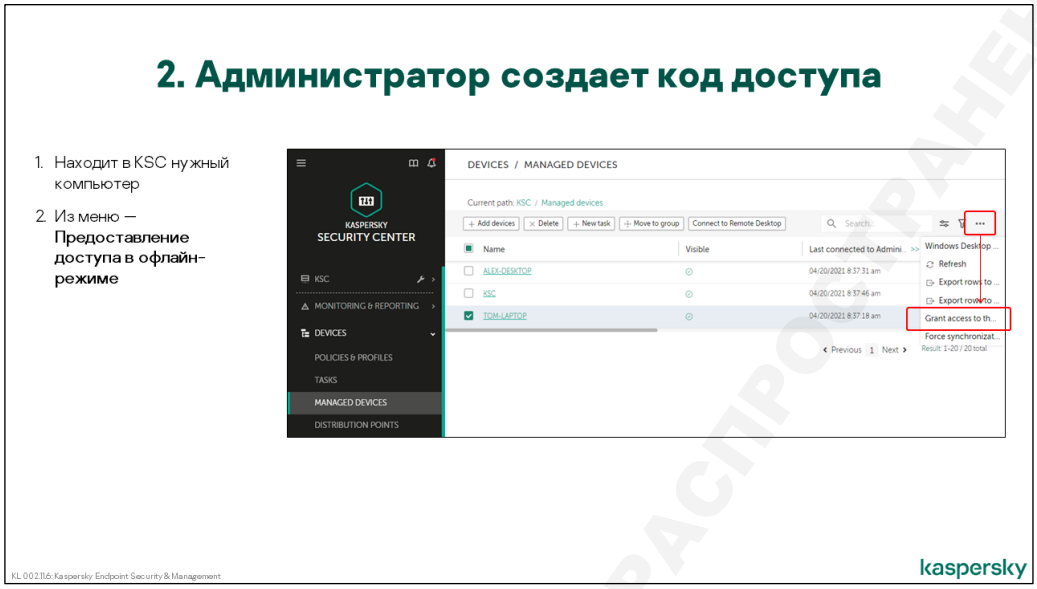
Как пользователю отправить запрос, чтобы получить доступ к заблокированному устройству?



В локальном интерфейсе Kaspersky Endpoint Security нажать кнопку **Настройка**, перейти к разделу **Контроль безопасности | Контроль устройств**. Нажать кнопку **Запросить доступ к устройству**. В открывшемся окне по умолчанию будут перечислены устройства, которые подключены в данный момент, в том числе заблокированные (можно увидеть все когда-либо подключенные к компьютеру устройства, если применить фильтр **За все время работы)**. Выбрать устройство, к которому требуется получить временный доступ, выделить его и нажать кнопку **Сформировать файл запроса**. Указать необходимую длительность доступа к устройству в часах (по умолчанию 24 часа), нажать кнопку **Сохранить** и полученный .**akey**-файл передать администратору.

Примечание: Если администратор запретил запрашивать временный доступ, кнопка **Запросить доступ** будет неактивна.

Как создать код активации



Временный доступ открывается определенному пользователю для определенного устройства на конкретном компьютере. Поэтому ключ генерируется не в политике или свойстве группы, а непосредственно через контекстное меню клиентского компьютера.

Важно: Создать специальный ключ доступа можно только в MMC-консоли.

Для поиска клиентского компьютера в Консоли администрирования удобно воспользоваться утилитой поиска. Затем администратору нужно открыть его контекстное меню и выбрать команду **Предоставление доступа в офлайн-режиме**. В отрывшемся окне нужно будет перейти на закладку **Контроль устройств** и с помощью кнопки **Обзор** выбрать .**akey**-файл полученный от пользователя.

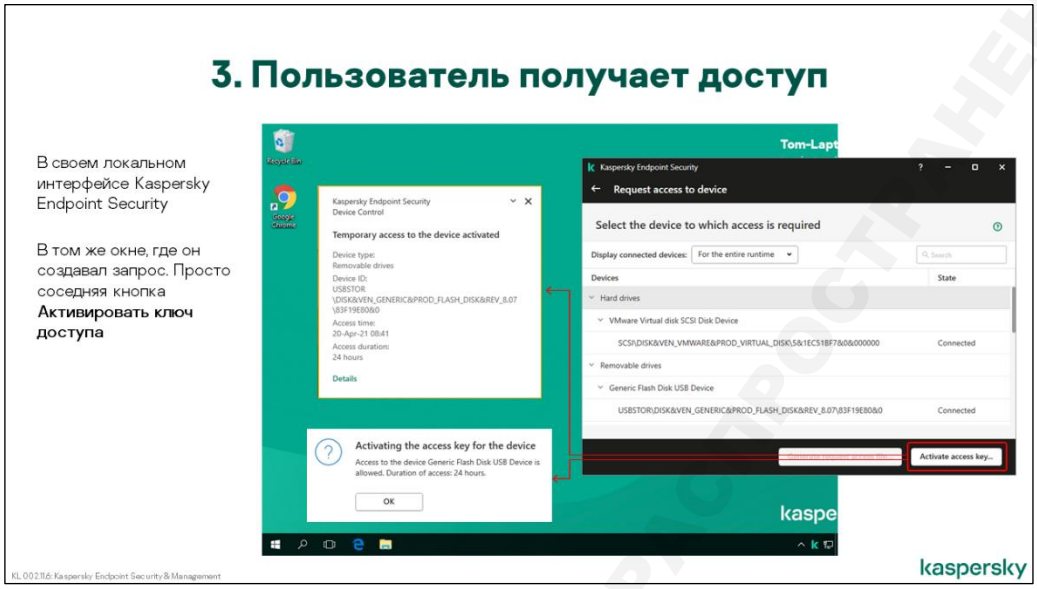
Сервер администрирования проверяет целостность файла и его соответствие выбранному компьютеру, после чего отображает информацию о запросе. При желании администратор может изменить время действия временного доступа и время активации. Они не могут быть меньше одного часа или превышать 999 часов. Значение по умолчанию для обоих периодов — 24 часа.

Затем администратору нужно сохранить сгенерированный ключ — файл с расширением .**acode** и передать его пользователю.

Таким образом, ключ генерируется для компьютера и на устройство, файл запроса к которому был получен от пользователя. Подключить другое устройство или это же устройство, но на соседнем компьютере не получится.

Кроме этого, ключ доступа привязан также к имени пользователя. Другой пользователь с этим же устройством на этом же компьютере не сможет воспользоваться ключом доступа для получения временного доступа. И если временный доступ активирован одним пользователем, другой пользователь во время разрешенного периода, устройством пользоваться не сможет.

Как открыть временный доступ

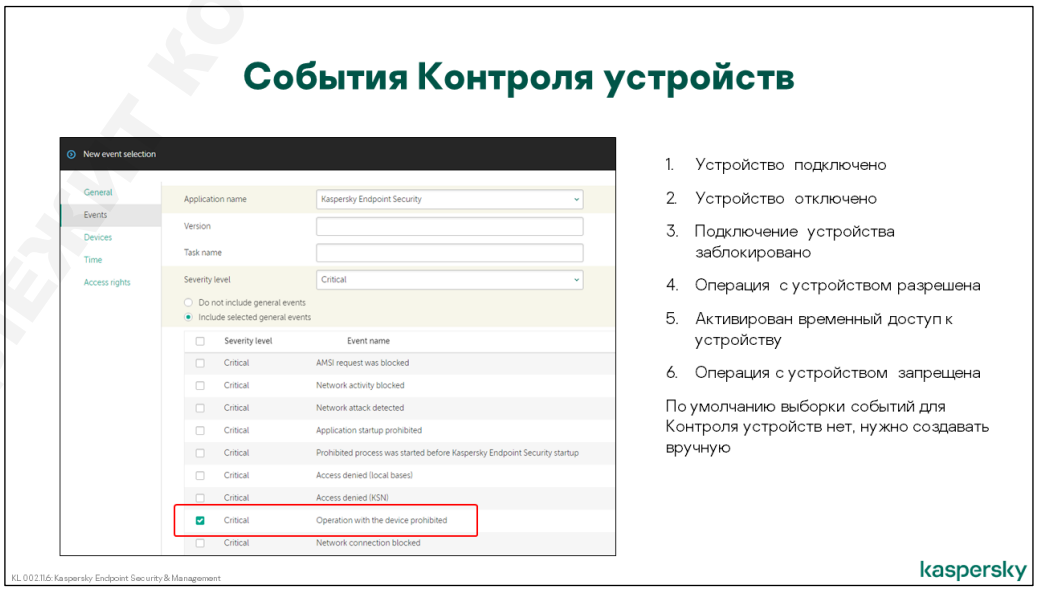


В том же окне, где генерировался ключ, пользователь выбирает соседнюю кнопку — **Активировать ключ доступа**, и вводит полученный **.acode**-файл. Устройство подключается сразу же. Ни перезагрузки, ни синхронизации с Сервером администрирования не требуется.

Активировать ключ нужно не позднее истечения срока активации, и длительность доступа отсчитывается с момента активации. Сколько раз в этот период и когда было подключено устройство, и было ли подключено вообще, роли не играет. Приостановить доступ нельзя.

При каждой активации временного доступа на Сервер администрирования отправляется уведомление-предупреждение, но в выборку запросов от пользователя оно не попадает, и в отчете о событиях Контроля устройств не отображается.

3.5 Мониторинг контроля устройств

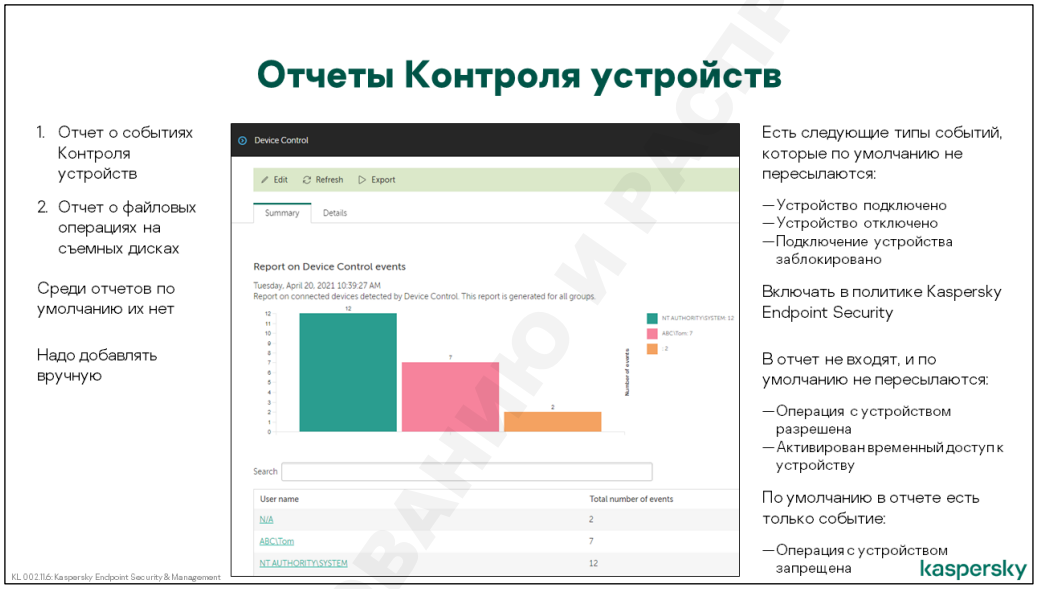


При каждой попытке пользователя подключить запрещенное устройство, на Сервер администрирования отправляется событие. В нем указываются время, имя компьютера, где была зафиксирована попытка, шина или тип устройства, его идентификатор (ID), операция и имя учетной записи, которая ее инициировала.

Событие называется *Операция с устройством запрещена*, оно относится к *Критическим* и соответственно, будет отображено в выборке **Критические события**. Если есть необходимость, администратор может сделать отдельную выборку только для заблокированных попыток доступа.

Аналогичное событие, но с уровнем важности *Информационное сообщение*, будет отправлено и при подключении незапрещенного устройства. По их количеству можно судить о частоте использования флэш-накопителей, локальных принтеров, сканеров, съемных дисков.

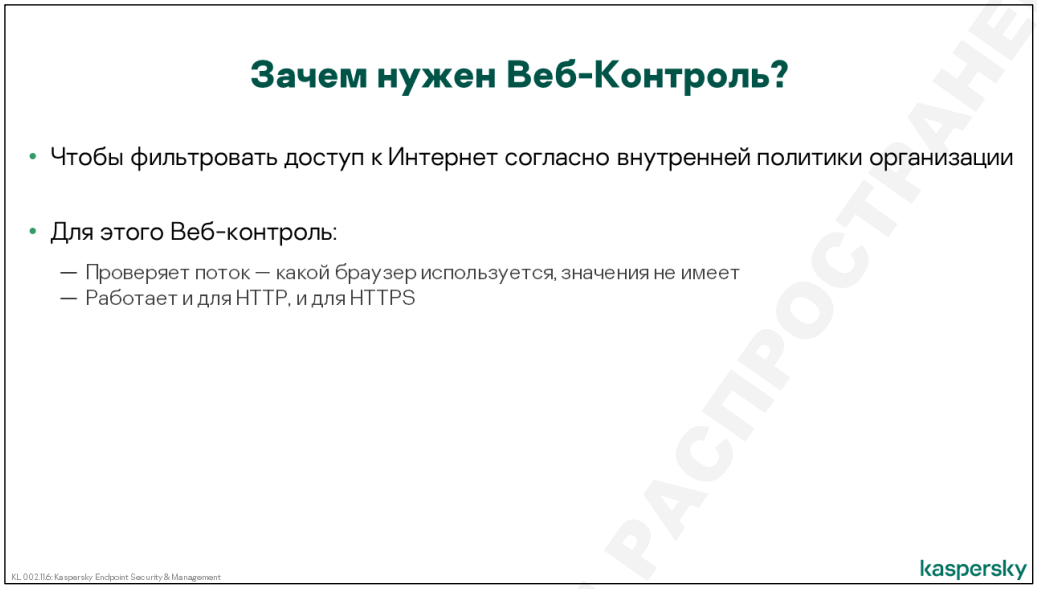
Все события, в том числе запросы пользователей, по умолчанию хранятся на сервере 30 дней.



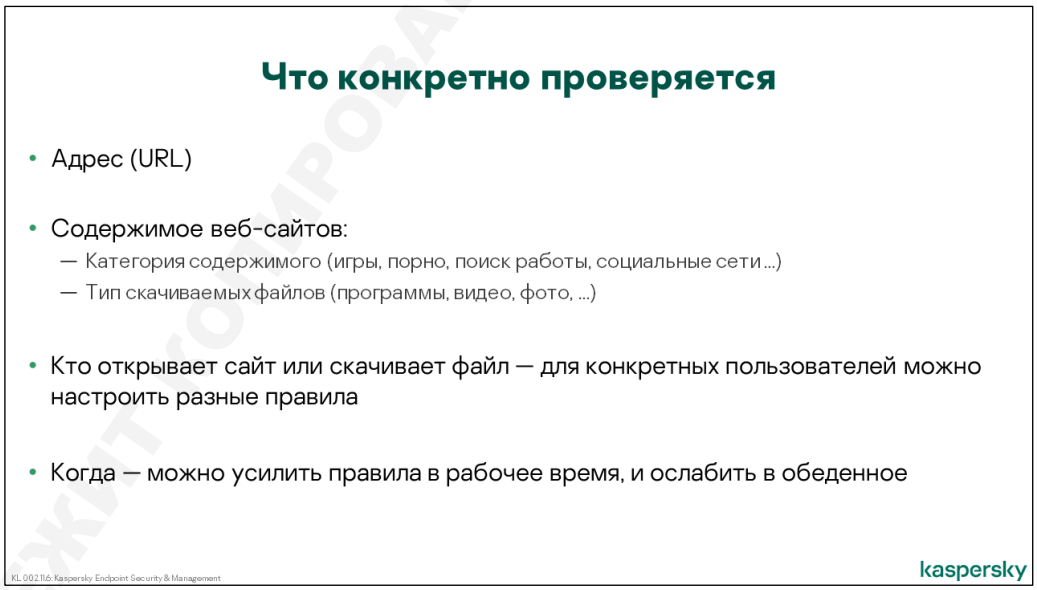
Для получения общей картины работы Контроля устройств удобно воспользоваться не выборками событий, а отчетом. Стандартный **Отчет о событиях Контроля устройств** показывает диаграмму его срабатывания в зависимости от имени пользователя. По умолчанию в отчет включаются все действия — подключение устройства, отключение и блокировка. Чтобы сгенерировать отчет исключительно о блокировках запрещенных устройств, в его свойствах на закладке **Параметры** нужно оставить отмеченным только **Подключение устройства заблокировано**.

При желании администратор может настроить ежедневную отправку по электронной почте сводной статистики о том, кто и когда пытался подключить, например, USB Flash-накопители. Для этого нужно создать задачу рассылки отчетов — как это сделать, описано в Части IV.

4. Веб-Контроль

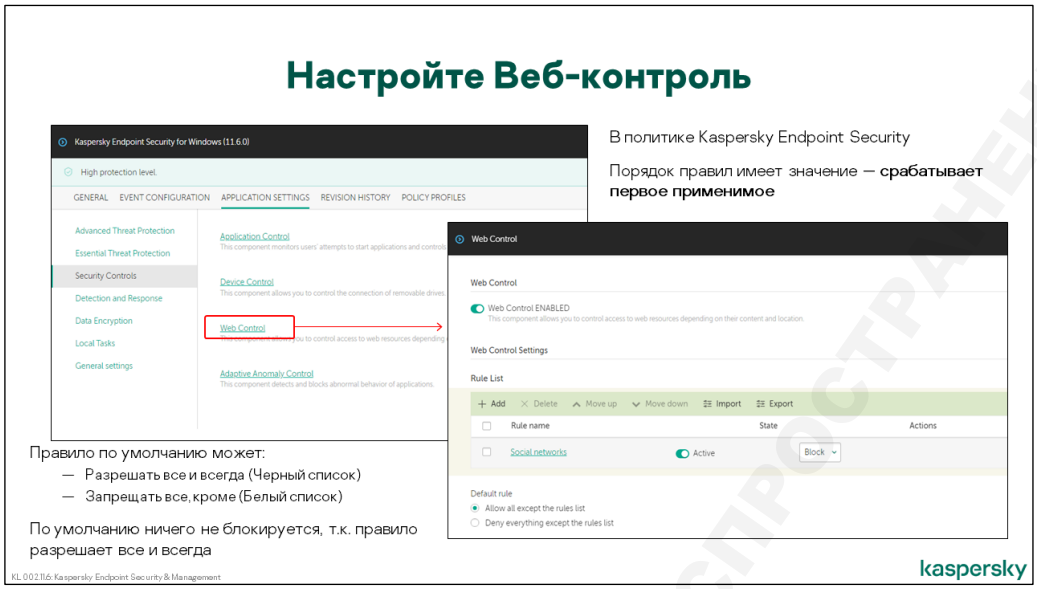


Задача Веб-контроля — фильтровать доступ пользователей к ресурсам Интернет согласно внутренней политике организации. Обычно это означает блокирование в рабочее время сайтов социальных сетей, музыки и видео, некорпоративной веб-почты, и т.п. Если пользователь захочет обратиться к такому веб-ресурсу, он получит уведомление о блокировке, или предупреждение о нежелательности доступа к нему — в зависимости от настроек политики.



Принцип работы Веб-контроля аналогичен принципу работы многих сетевых экранов. Администратор создает набор правил, которые могут быть блокирующими или разрешающими. В правилах указываются адреса или тип содержимого, пользователи, расписание и выполняемое действие.

Проверяется только HTTP и HTTPS-трафик.

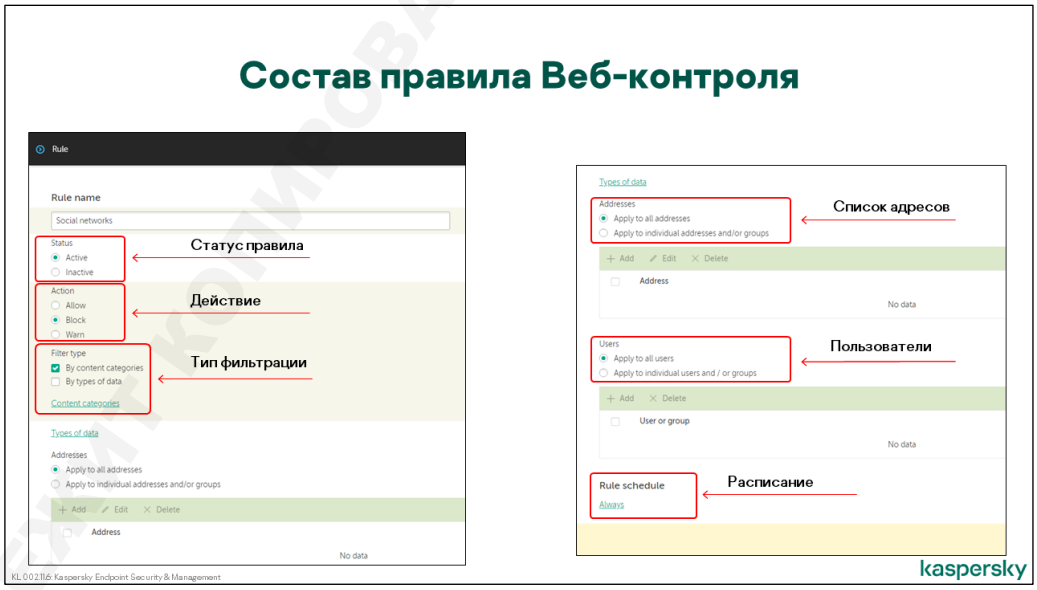


Веб-контроль настраивается в политике Kaspersky Endpoint Security. Применяются правила в заданном администратором порядке, и срабатывает первое, применимое к запрошенной странице.

Есть два правила по умолчанию, они же регулируют режим работы:

— Разрешать все, не указанное в списке правил — режим Запрещающий список
— Запрещать все, не указанное в списке правил — режим Разрешающий список

По умолчанию используется универсальное правило **Разрешать все** и всем и ничего не блокируется.

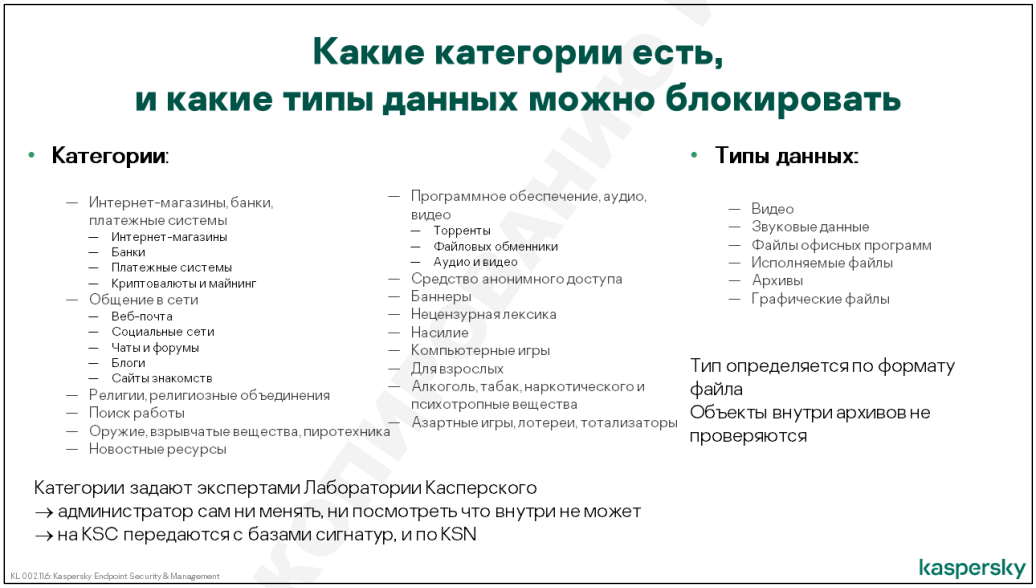


У каждого правила есть название и шесть атрибутов.

— Статус правила
  — Активно
  — Неактивно

- Действие
  - Разрешать
  - Блокировать
  - Предупреждать
- Тип фильтрации
  - По категориям содержания
  - По типам данных
- Список адресов
  - Применять ко всем адресам
  - Применять к отдельным адресам
- Пользователи
  - Применять ко всем пользователям
  - Применять к отдельным пользователям
- Расписание

4.1 Критерии блокирования



Во-первых, запрещать или разрешать доступ можно по адресу сайта. Администратор может прямо ввести набор URL, доступ к которым он хочет закрыть, или использовать универсальный символ * для блокирования всех сайтов, чьи адреса удовлетворяют маске — например, *.*fm* или **shop**.

Кроме этого, Kaspersky Endpoint Security умеет самостоятельно анализировать содержимое веб-страниц (при работе по HTTP). В результате контент может быть отнесен к одной из категорий:

- Интернет-магазины, банки, платежные системы
  - Интернет-магазины
  - Банки
  - Платежные системы
  - Криптовалюты и майнинг
- Общение в сети
  - Веб-почта

  - Социальные сети
  - Чаты и форумы
  - Блоги
  - Сайты знакомств
- Религии, религиозные объединения
- Поиск работы
- Оружие, взрывчатые вещества, пиротехника
- Новостные ресурсы
- Программное обеспечение, аудио, видео
  - Торренты
  - Файловые обменники
  - Аудио и видео
- Средства анонимного доступа
- Баннеры
- Нецензурная лексика
- Насилие
- Компьютерные игры
- Для взрослых
- Алкоголь, табак, наркотического и психотропные вещества
- Азартные игры, лотереи, тотализаторы

или определен как:

- Видео
- Звуковые данные
- Файлы офисных программ
- Исполняемые файлы
- Архивы
- Графические файлы

Администратор может ограничить показ любой из перечисленных категорий или типов данных, но редактировать их или добавлять новые нельзя.

Создавая правило, можно комбинировать фильтрацию по категориям и типам данных: например, блокировать файлы офисных программ и архивы, полученные только через веб-почту.

Для определения принадлежности к категориям используется база известных адресов (в папке с обновлениями это файлы *pc*.dat*), и эвристический анализ содержимого страниц. Кроме того, репутация страницы может быть получена из KSN.

Типы данных встроены в Kaspersky Endpoint Security и означают следующее:

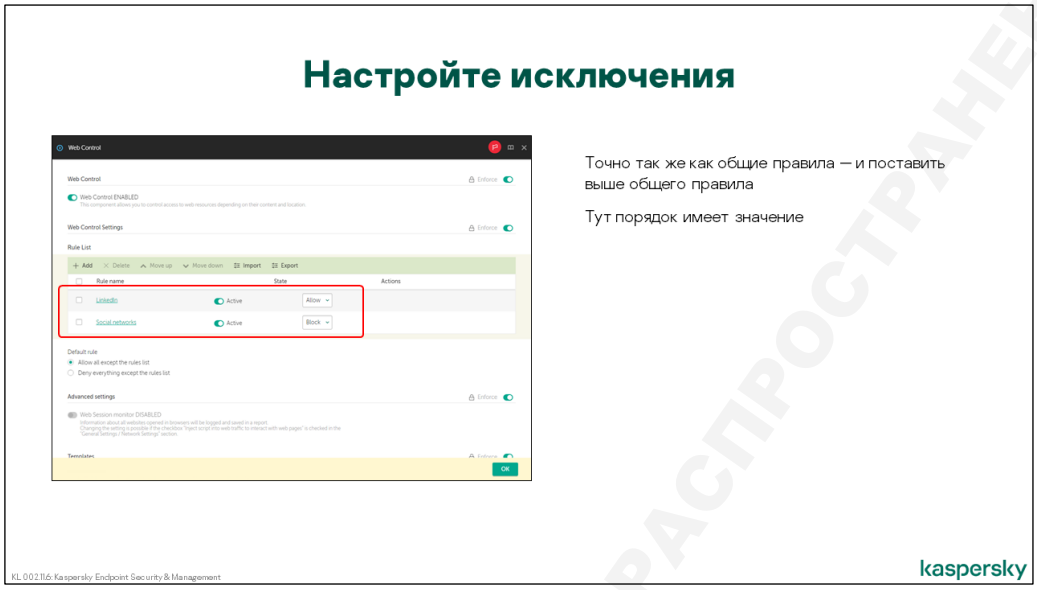
Категория	Содержание категории
Исполняемые файлы	Win32 PE — exe, dll, ocx, scr, drv, vdx, и любые другие расширения у Win32 PE файлов Microsoft Installer Archive — msi
Видео	Adobe Flash Video — flv, f4v Audio/Video Interleave — avi MPEG4 ISO format — 3gp, 3g2, 3gp2, 3p2 MPEG4 — divx, mp4, m4a Matroska — mkv Apple Quicktime — mov, qt Microsoft Container — asf, wma, wmv RealMedia CB/VB — rm, rmvb MPEG2 (DVD) format — vob VCD (MPEG 1) — dat, mpg Bink Video — bik

Звуковые данные	MPEG-1 Layer 3 — mp3 Lossless Audio — flac, ape OGG Vorbis Audio — ogg Advanced Audio Coding — aac Windows Media Audio — wma AC3 multichannel audio — ac3 Microsoft Wave — wav Matroska Audio — mka RealAudio — rm, ra, ravb MIDI — mid, midi CD digital Audio — cdr, cda
Файлы офисных программ	Open XML documents — docx, xlsx, pptx, dotx, potx, и другие Office 2007 macro enabled docs — docm, xlsm, pptm, dotm MS Office documents — doc, xls, ppt, dot, pot Adobe Acrobat — pdf
Архивы	ZIP archive — zip, g-zip 7-zip archive — 7z, 7-z RAR archive — rar ISO-9660 CD Disk — iso Windows Cabinet — cab Java (ZIP) archive — jar BZIP2 archive — bzip2, bz
Графические файлы	JPEG/JFIF — jpg, jpe, jpeg, jff GIF — gif Portable Graphics — png Windows Bitmap (DIB) — bmp Targa Image File Format — tif, tiff Windows Meta-File — emf, wmf Post-Script Format — eps Adobe Photoshop — psd Corel Draw — cdr

Отметим некоторые особенности встроенных в Kaspersky Endpoint Security типов и категорий:

- Тип определяется по формату файла, а не по расширению
- Объекты внутри архивов не проверяются — если запретить исполняемые файлы, но не запретить архивы, исполняемые файлы внутри архивов можно будет загружать
- Документы PDF относятся к файлам офисных программ. Следовательно, при блокировке этой категории некоторые сайты, использующие pdf, могут отображаться некорректно
- В старых версиях Антивируса Касперского (6.0.x) Анти-Баннер был отдельным компонентом. В Kaspersky Endpoint Security для этих целей можно использовать блокировку категории **Баннеры** в Веб-Контроле
- Заблокировать простые flash-ролики в формате SWF можно только маской по расширению; обычно это **.swf*

4.2 Настройка исключений и доверенных серверов

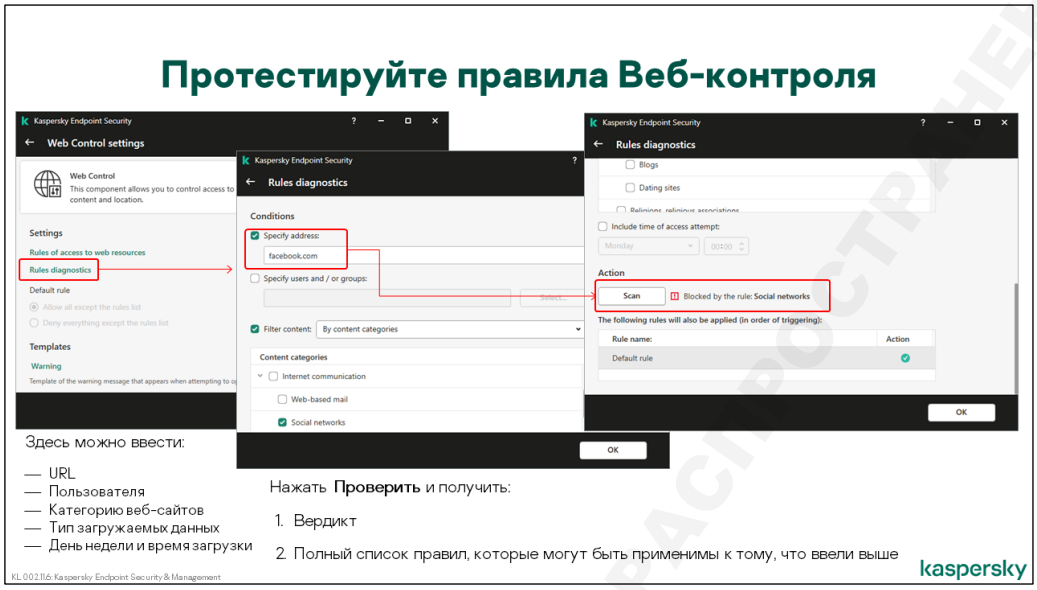


Иногда заведомо разрешенный сайт может случайно попасть под действие блокировки. Например, внутренний портал может быть распознан как социальная сеть, или онлайн-обучение отнесено к запрещенным видеоматериалам. В этом случае проще не создавать отдельную группу со своей политикой, а ввести разрешающее правило. Оно будет открывать доступ к определенным категориям или типам данных, размещенным на заданном администратором наборе серверов.

Чтобы такое правило сработало первым, его нужно поместить выше соответствующего запрещающего правила.

Как крайний случай, политика организации может совсем запрещать использование Интернет в рабочее время, разрешая только корпоративный сайт. Исключение может быть сделано только для небольшого ИТ-отдела. В этом случае администратор создает общее правило — запрещать в рабочее время все и всем. Затем добавляет выше него два разрешающих: первое будет разрешать любое содержимое для учетных записей сотрудников отдела ИТ, второе — разрешать всем доступ на корпоративный сайт.

4.3 Диагностика и тестирование



Когда правил становится достаточно много, бывает сложно отследить, какое из них сработало и почему. Поэтому в Kaspersky Endpoint Security есть функция офлайн-диагностики Веб-Контроля.

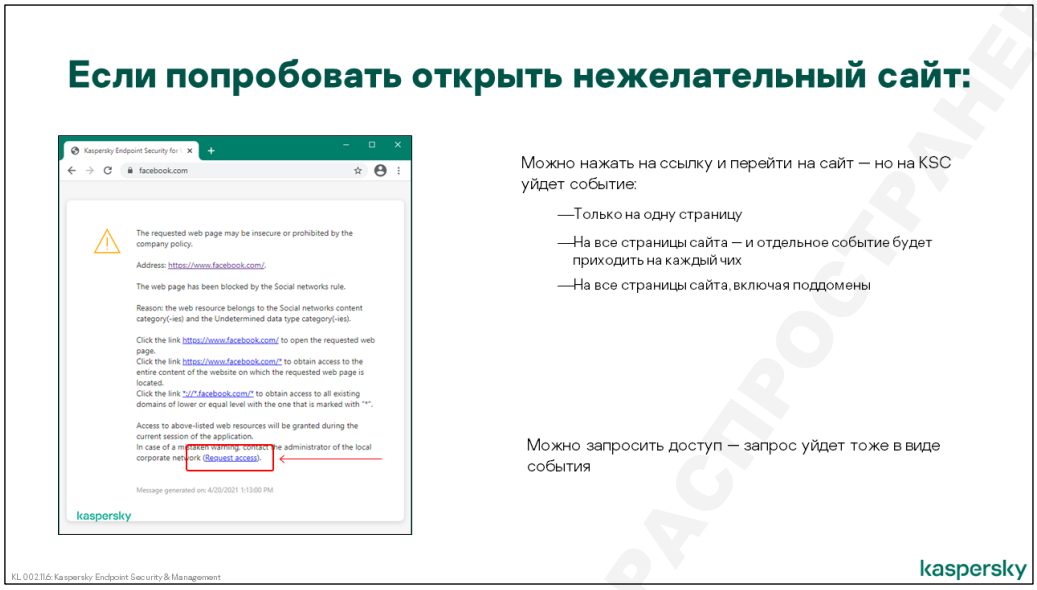
Чтобы ею воспользоваться, нужно сначала применить политику к одной из рабочих станций и открыть на ней локальный интерфейс Kaspersky Endpoint Security. Затем нужно перейти на закладку настроек, выбрать Веб-Контроль, и нажать на ссылку **Диагностика правил**. Она открывает окно, в котором можно задать любые условия предполагаемого запроса:

- отметить категории
- типы данных
- расписание
- учетные записи
- непосредственно ввести адрес сайта — можно использовать символ «*»

и в ответ получить вердикт Веб-Контроля со списком применимых к этим условиям правил.

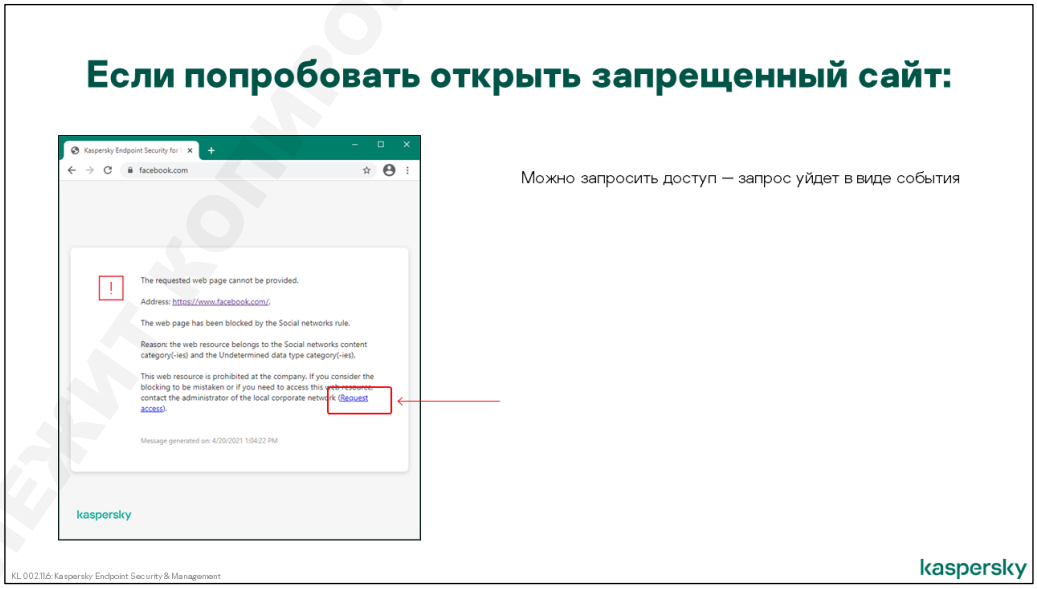
Например, администратор может проверить, будет ли доступ к домашнему почтовому серверу одного из сотрудников попадать под общий запрет веб-почты. Или если пользователи начали активно жаловаться на проблемы с доступом к некоторому явно разрешенному сайту, можно выяснить, какое именно правило работает некорректно.

4.4 Настройка взаимодействия с пользователем



Если Веб-контролем была заблокирована всего лишь часть содержимого страницы, пользователь может это и не заметить. При полном запрете он получит подмененную страницу с сообщением Веб-Контроля — предупреждением о нежелательности доступа, или сообщением о блокировке.

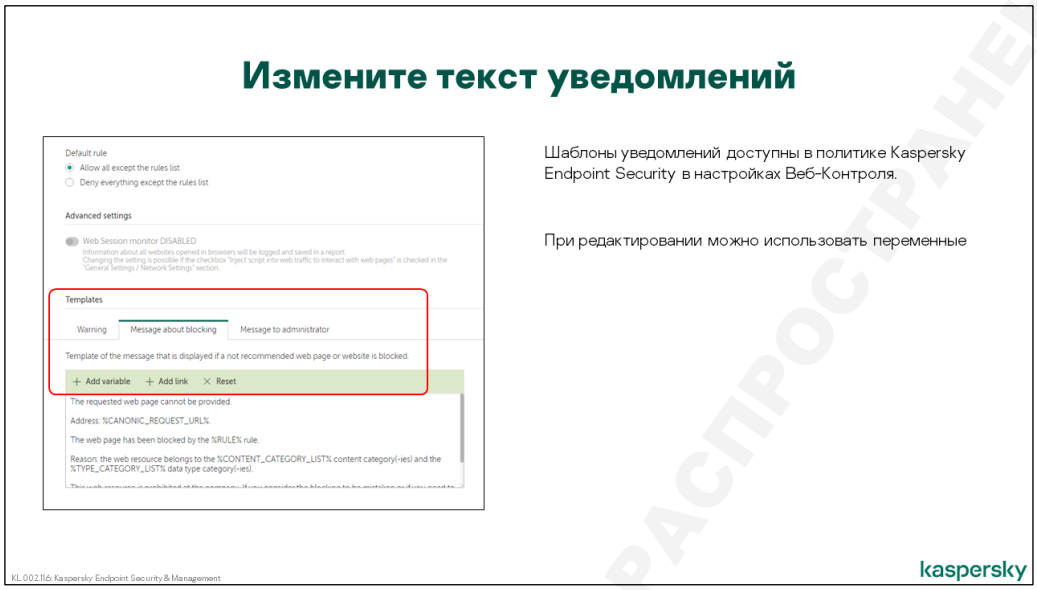
Когда доступ к сайту просто нежелателен (применяется предупреждающее правило), пользователь все же сможет его открыть — нужно будет просто перейти по одной из ссылок в предупреждающем сообщении: ссылке на страницу, которую пытались открыть, или ссылке, разрешающей доступ ко всем страницам на сайте, или ссылке, разрешающей весь сайт и его поддомены (т.е. доступ **.amazon.com/** вместо доступа к *www.amazon.com/**)

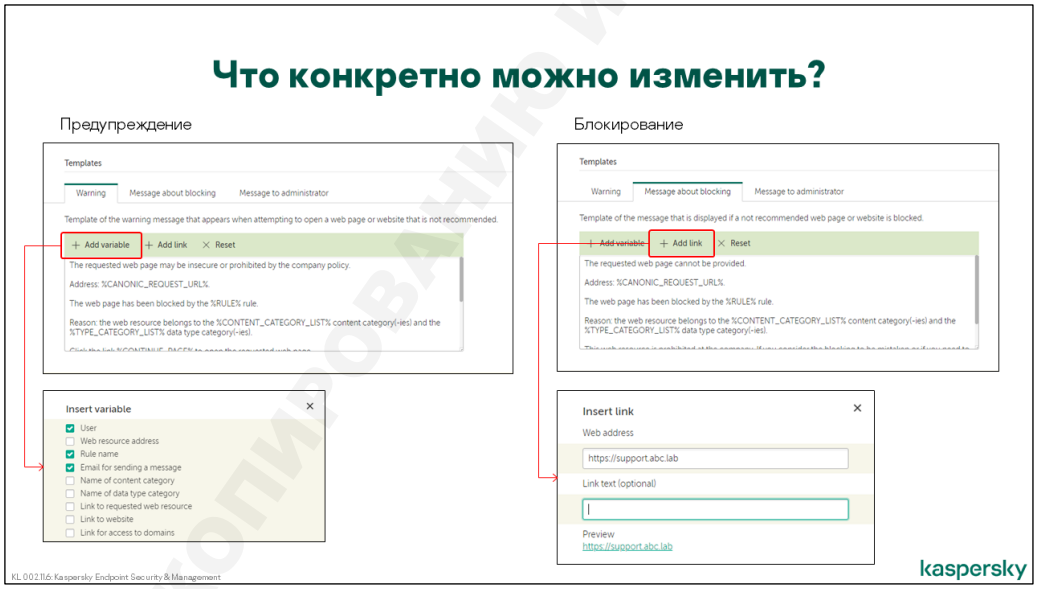


Если же сайт заблокирован Веб-контролем, доступ будет запрещен без возможности временно снять ограничение.

В сообщениях Веб-Контроля присутствует ссылка **Запросить доступ**, на случай если пользователь не согласен с политикой и желает получить беспрепятственный доступ к веб-

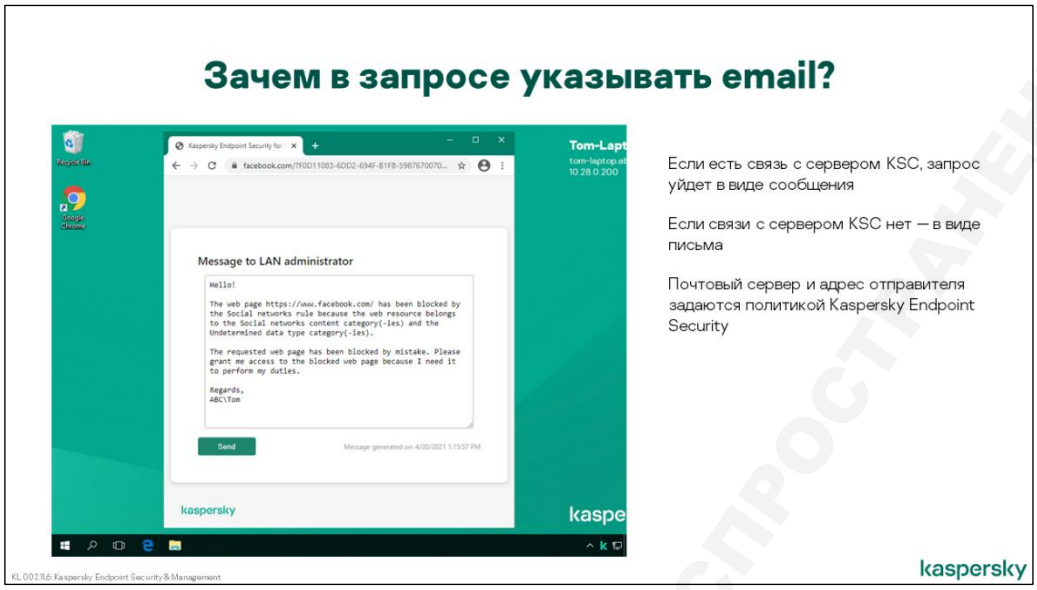
ресурсу. Запросы отправляются на Сервер администрирования в виде событий и попадают в выборку **Запросы пользователей**.



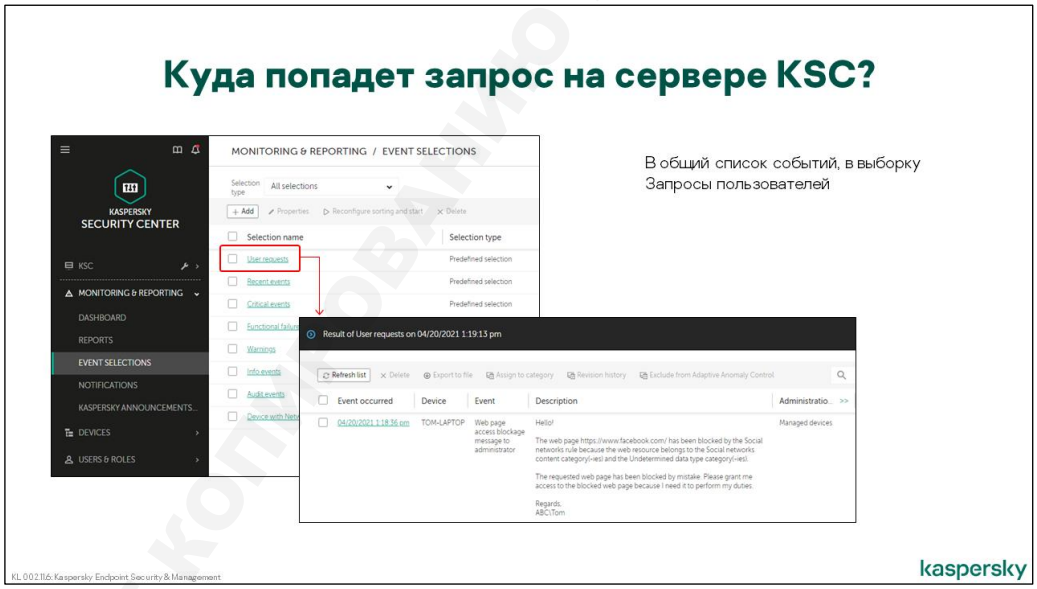


Шаблоны уведомлений доступны в политике Kaspersky Endpoint Security в настройках **Веб-Контроля**. При редактировании можно использовать переменные.

В шаблоне запроса на доступ к веб-странице есть поле **Кому (электронный адрес)**, оно нужно на случай, если нет связи с Сервером администрирования. В таком случае запрос на сервер уйдет в виде письма, а не обычного события.



4.5 Статистика работы Веб-Контроля

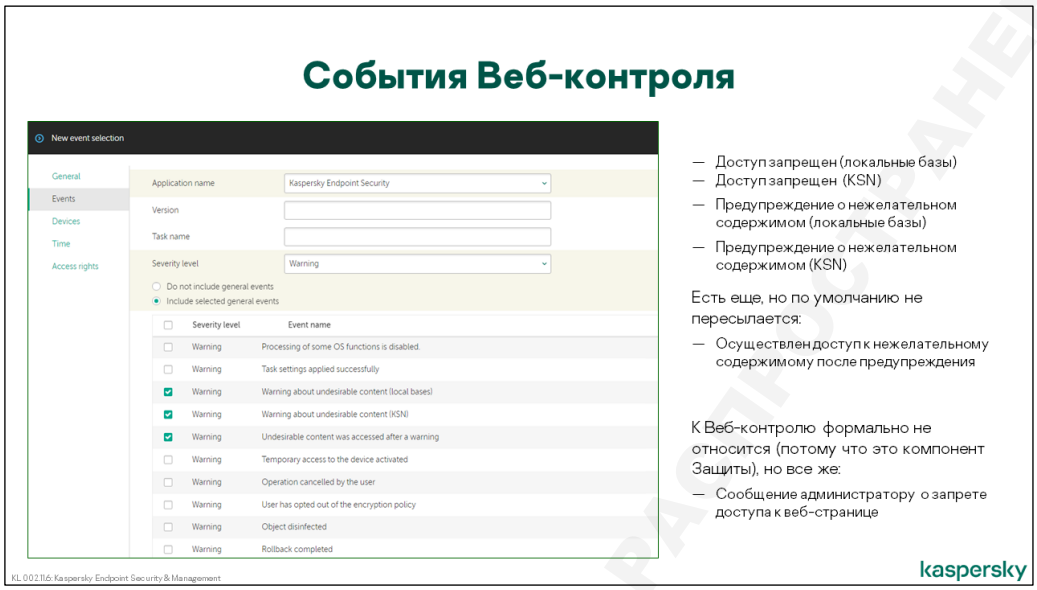


При каждом блокировании или вынесении предупреждения о нежелательности доступа Веб-Контроль одновременно отправляет на Сервер администрирования соответствующее событие. В случае блокировки это *Доступ запрещен* с уровнем важности *Критический*, для предупреждения — *Предупреждение о нежелательном содержимом* с уровнем *Предупреждение*.

В обоих случаях в событиях указываются время доступа, запрашиваемый сайт, сработавшее правило, клиентский компьютер, имя пользователя (его учетная запись) и вердикт Веб-Контроля. Если правило было задано для категории или типа данных, они тоже будут указаны.

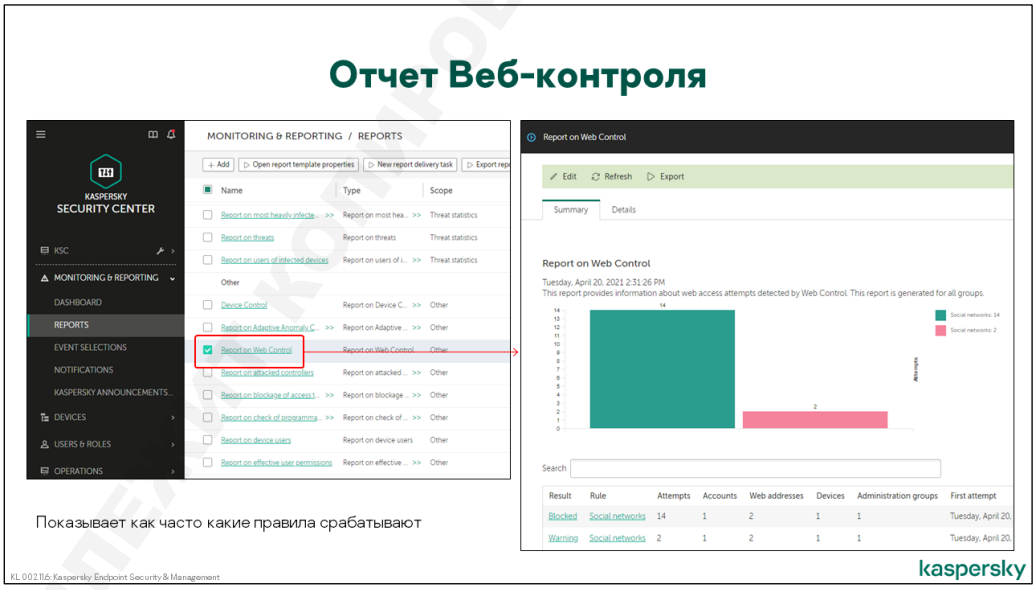
Примечание: Веб-Контроль обрабатывает каждый объект, из которых состоит сайт, независимо друг от друга. Поэтому, например, при запрете графических файлов, блокировка каждой даже самой маленькой картинки будет генерировать отдельное событие. Как следствие, одна попытка доступа к запрещенному сайту может привести к отправке сотни событий, и это вовсе не будет

означать, что пользователь день и ночь проводит в Сети. Поэтому события о блокировании доступа по умолчанию не передаются на Сервер администрирования



Если пользователь проигнорировал предупреждение о нежелательности доступа и все же зашел на сайт, на Сервер уходит событие *Осуществлен доступ к нежелательному содержимому после предупреждения*, уровень важности — *Предупреждение*.

4.6 Отчет о работе Веб-Контроля



Для регулярного контроля и получения общей картины удобно использовать отчет. В нем дается сводная статистика по количеству предупреждений и блокировок по каждому из правил. Разрешающие правила не учитываются.

5. Адаптивный контроль аномалий

Адаптивный контроль аномалий содержит набор шаблонов поведения (эвристик), которые могут обновляться вместе с антивирусными базами.

Тут собраны наиболее популярные поведения, которые характерны для вредоносных программ и могут свидетельствовать о попытках компрометации системы.

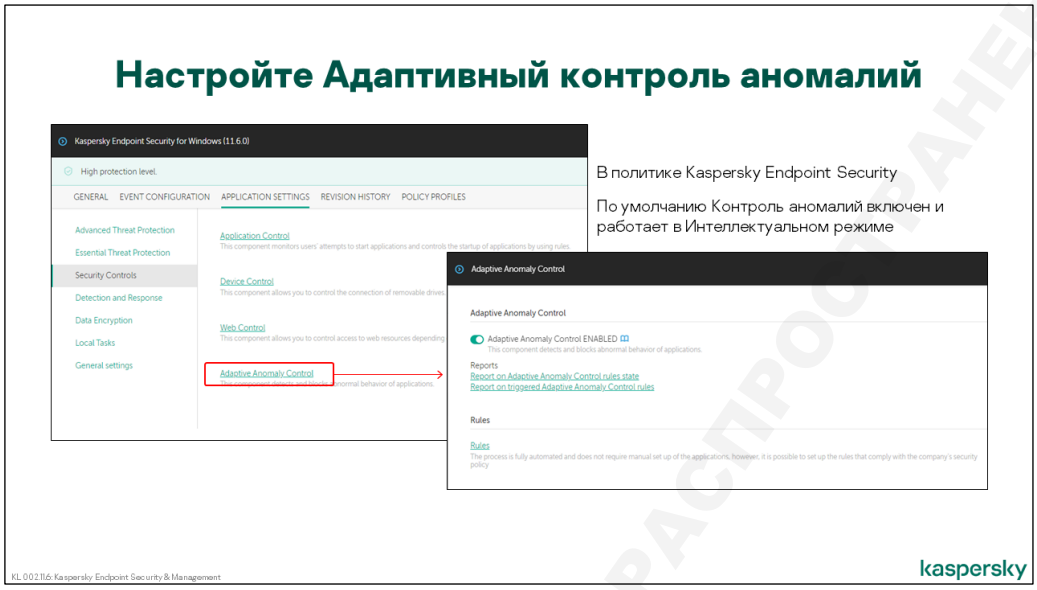
С другой стороны, некоторые действия вполне могут быть легитимными в рамках определенного компьютера или группы компьютеров. Например, запуск PowerShell из внешних программ вполне себе нормальное поведение на компьютерах администраторов или разработчиков. Или просто в компании могут использоваться обфусцированные PowerShell-скрипты для автоматизации каких-либо задач.

Задача администратора заключается в том, чтобы донести до Адаптивного контроля аномалий какая активность типичная для определенного компьютера, а какая нет, поэтому по умолчанию компонент включается в режиме двухнедельного обучения (Интеллектуальный режим), за это время он отслеживает активность, информирует об этом администратора и уже администратор, а не компонент, принимает решение характерна ли определенная активность для компьютера или нет.

Режим обучения для каждого правила на каждом компьютере происходит независимо, т.е. где-то закончится раньше, где-то позже.

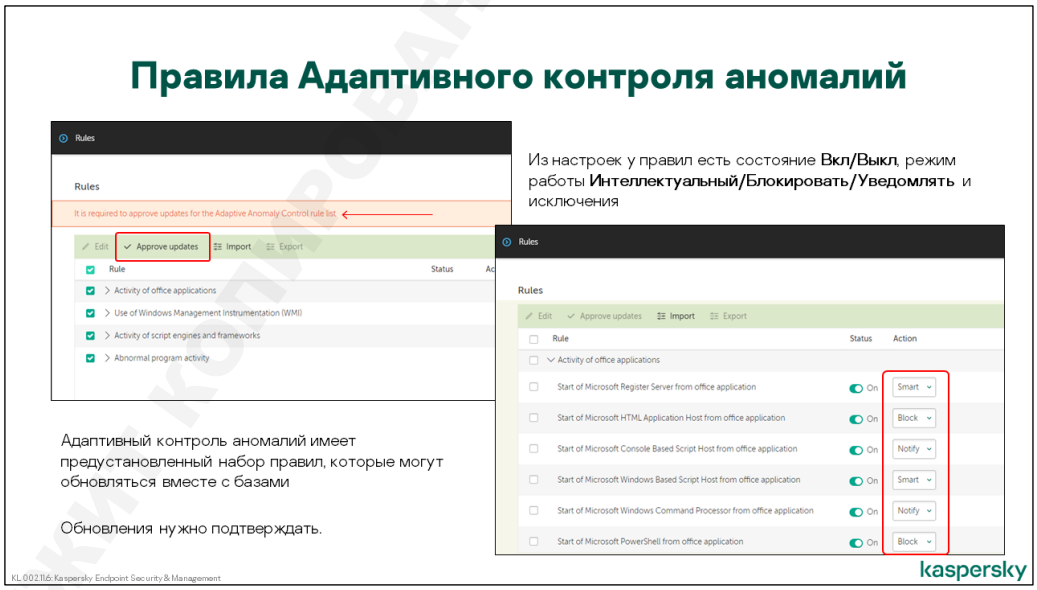
Примечание: В отличие от остальных компонентов контроля для Адаптивного контроля аномалий нужна как минимум лицензия KESB Расширенный.

5.1 Как настроить Адаптивный контроль аномалий



Компонент Адаптивный контроль аномалий по умолчанию устанавливается и включается, однако работает он в Интеллектуальном режиме (Smart).

Адаптивный контроль аномалий настраивается в политике Kaspersky Endpoint Security. Из свойств компонента можно сразу попасть в отчеты о работе компонента и список правил.



Адаптивный контроль аномалий работает на основе правил (шаблонов поведения), которые поставляются вместе с антивирусными базами, т.е. могут обновляться. Правила разделены на несколько категорий:

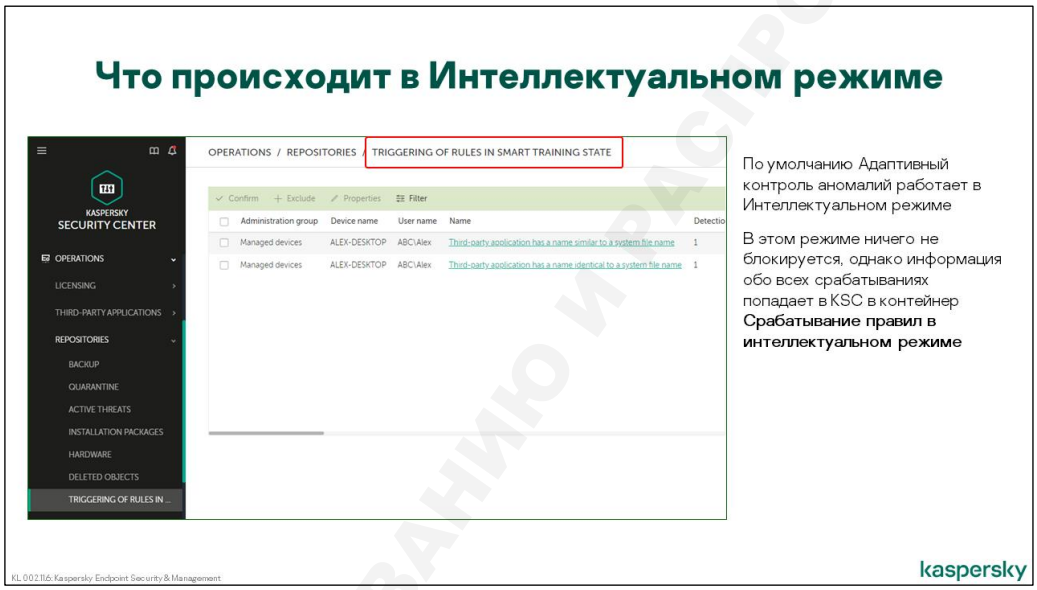
- Активность офисных программ
- Использование инструментария управления Windows (WMI)
- Активность интерпретатора скриптовых языков
- Нетипичная активность программ

Сообщение о подтверждении обновлений, которое администратор может увидеть в первый раз, с одной стороны, не влияет на работу компонента, т.е. срабатывания будут. Но если администратор захочет создать исключение в правиле, то он не сможет этого сделать до тех пор, пока не нажмет **Подтвердить обновления**.

В дальнейшем, если при обновлении баз добавится новое правило, сообщение о подтверждении обновлений появится снова, чтобы привлечь внимание администратора.

У каждого правила есть состояние **Вкл/Выкл**, режим работы **Интеллектуальный / Блокировать / Уведомлять** и исключения.

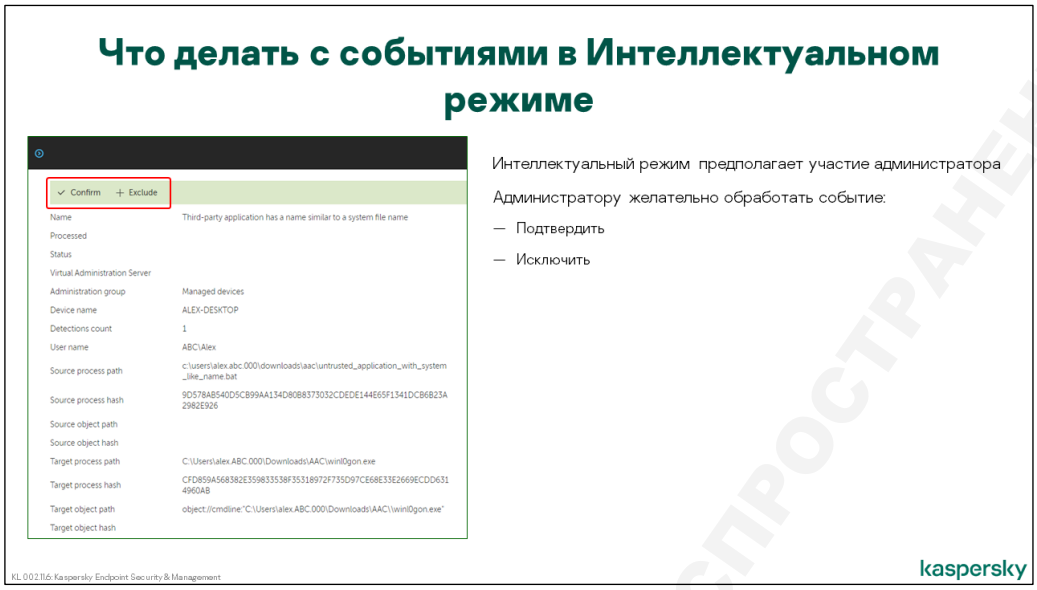
Т.е. для каждого правила можно задать режим в явном виде Блокировать или Уведомлять, однако по умолчанию включен Интеллектуальный режим.



Интеллектуальный режим тесно связан с Kaspersky Security Center и действиями администратора. Как было сказано выше, после установки компонент обучается примерно две недели, за это время ничего не блокируется, но информация о срабатываниях отправляется в Kaspersky Security Center.

В идеальной ситуации, когда за две недели не происходит никаких срабатываний, это значит, что поведение, описанное в правилах нетипично для компьютера. Адаптивный контроль аномалий переходит в режим **Интеллектуальное блокирование (Smart Block)** и при возникновении нетипичной активности она будет заблокирована.

Если же за время обучения происходят срабатывания, то они складываются в контейнер **Операции | Хранилища | Срабатывание правил в состоянии Интеллектуальное обучение** на Сервере администрирования и тут необходимо участие администратора.



Когда приходит событие, администратору нужно его обработать. Администратора может подтвердить вердикт или добавить в исключения.

- **Подтвердить** — означает, что администратор соглашается с тем, что такое поведение подозрительное и нелегитимное
- **Исключить** — означает, что администратор считает подобную активность нормальной и для нее создается исключение в соответствующем правиле

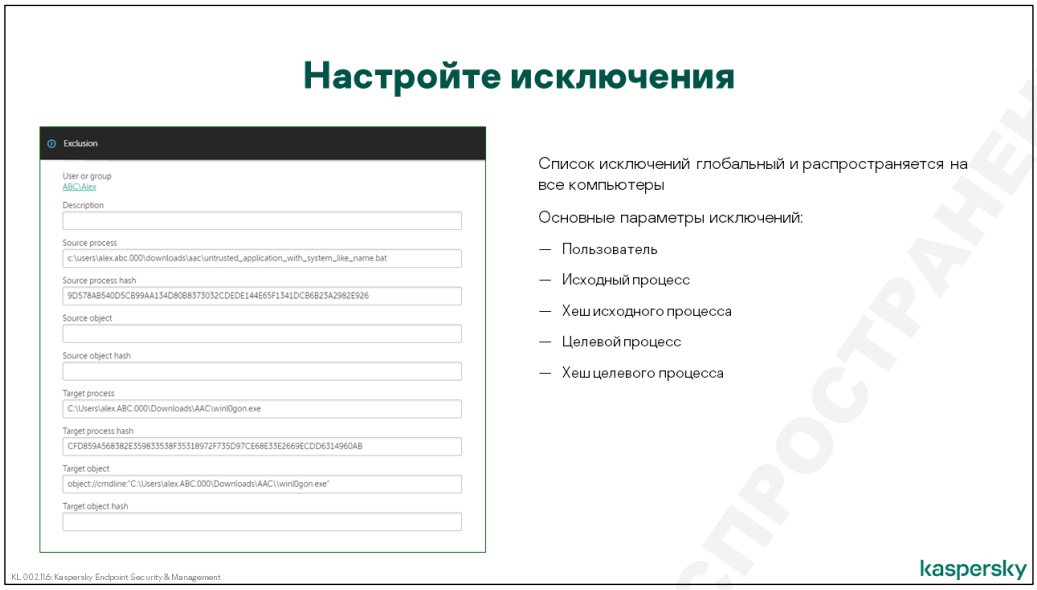
Зачем нужно обрабатывать события? Если с **Исключить** все ясно, то что будет, если администратор будет игнорировать **Подтвердить**?

Подтвердить влияет только на продолжительность режима обучения. Адаптивному контролю аномалий нужно примерно 14 (цифра может незначительно отличаться) дней, чтобы завершить обучение, и если администратор не обрабатывает события, то каждый раз по приходу нового события счетчик будет заново отсчитывать 14 дней до тех пор, пока в течение 14 дней не будет никаких срабатываний и только тогда Адаптивный контроль аномалий перейдет в режим **Интеллектуальное блокирование (Smart Block)**. Но при таком подходе возможна ситуация, когда Адаптивный контроль аномалий окажется в вечном режиме обучения, например, если срабатывание происходит регулярно (не реже 1 раза в 14 дней), но администратор его не обрабатывает.

Если же администратор будет внимательно относиться к событиям и вовремя обрабатывать их, то счетчик сбрасываться не будет и обучение завершится в течение двух недель.

Интеллектуальное обучение проходит индивидуально для каждого правила на каждом компьютере и информация о подтвержденных вердиктах во время обучения будет храниться локально на компьютерах, т.е. для каждого правила будет свой счетчик времени обучения.

Важно: Сам компонент Адаптивный контроль аномалий не может принять решение типичное или нетипичное то или иное поведение. Для Адаптивного контроля аномалий вся активность, которая попадает под действия правил нетипична, и только администратор может сказать, что такая-то подозрительная активность легитимна. Для этого нужно добавить данные об активности в исключение правила, которое детектит эту активность. Т.е. можно сказать, что Адаптивный контроль аномалий работает в режиме Default Deny, т.е. пока администратор не сделает исключение для нетипичной активности, она будет блокироваться.



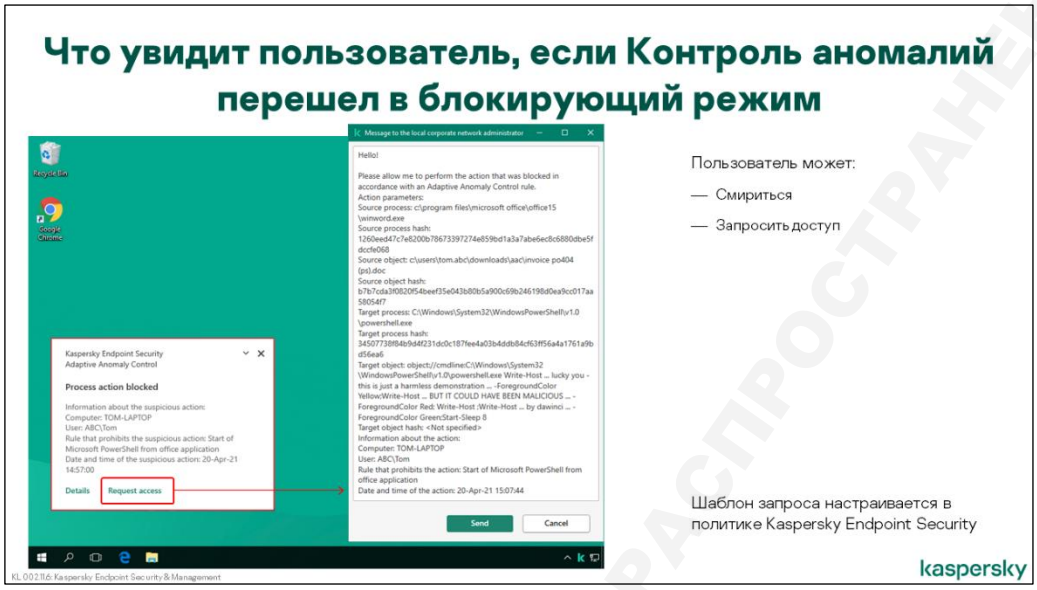
Исключения добавляются в политику Kaspersky Endpoint Security и распространяются на все компьютеры.

Основные параметры исключений:

- Пользователь
- Исходный процесс
- Хеш исходного процесса
- Целевой процесс
- Хеш целевого процесса

Тут стоит заметить, что на разных операционных системах одни и те же системные процессы будут иметь разные контрольные суммы, поэтому исключение, созданное из события на одном компьютере, может не сработать на другом. В таком случае нужно либо создавать дополнительные исключения, либо сделать менее жестким текущее, т.е. убрать контрольную сумму и оставить только путь к процессу.

5.2 Настройка взаимодействия с пользователем



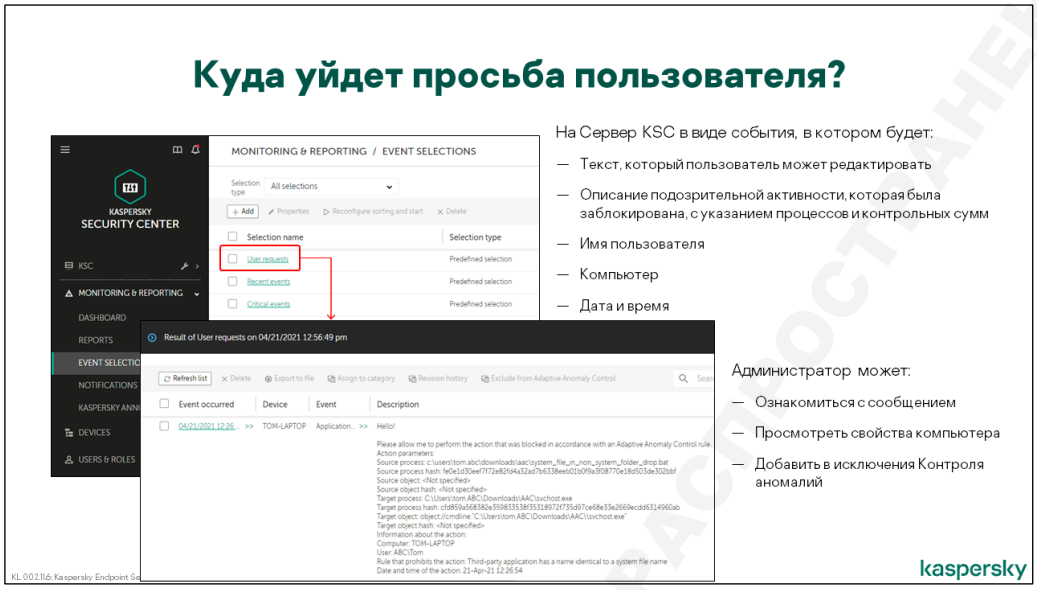
При обнаружении нетипичной активности пользователь увидит всплывающее уведомление.

Если его отключить, пользователь может ошибочно подумать, что что-то не в порядке с приложениями или операционной системой. Как следствие, обратиться к технической службе, или пытаться разобраться самому, что может быть еще хуже. Но администратор может изменить текст уведомления, указав, куда и кому звонить за помощью, написать номер телефона и адрес электронной почты.

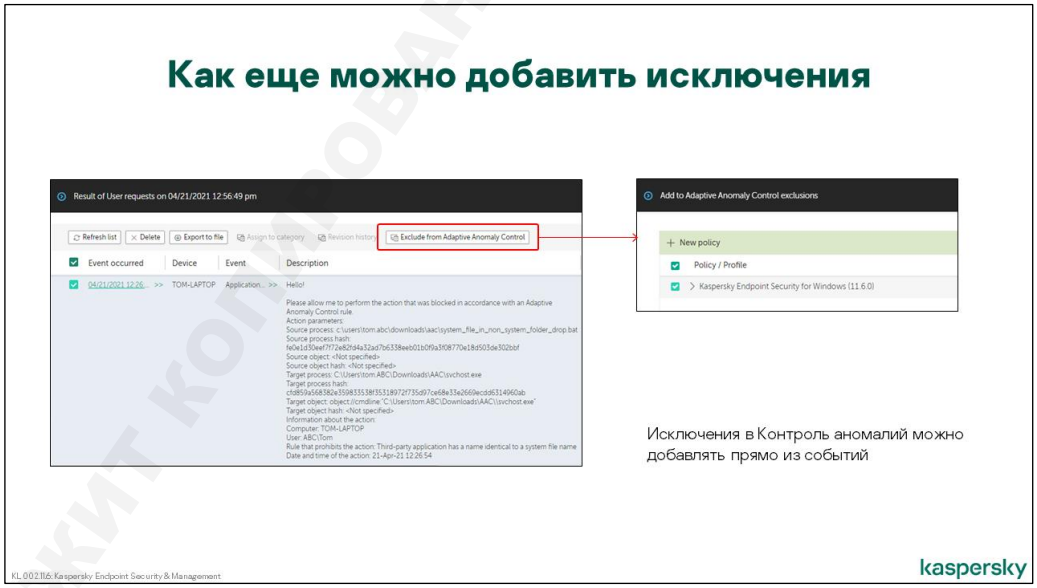
Шаблоны уведомлений доступны в политике Kaspersky Endpoint Security в настройках **Адаптивного контроля аномалий**.

Если всплывающее уведомление о блокировке включено, в нем по умолчанию будет ссылка *Запросить доступ*. Отключить или спрятать ее нельзя.

5.3 Статистика работы Адаптивного контроля аномалий



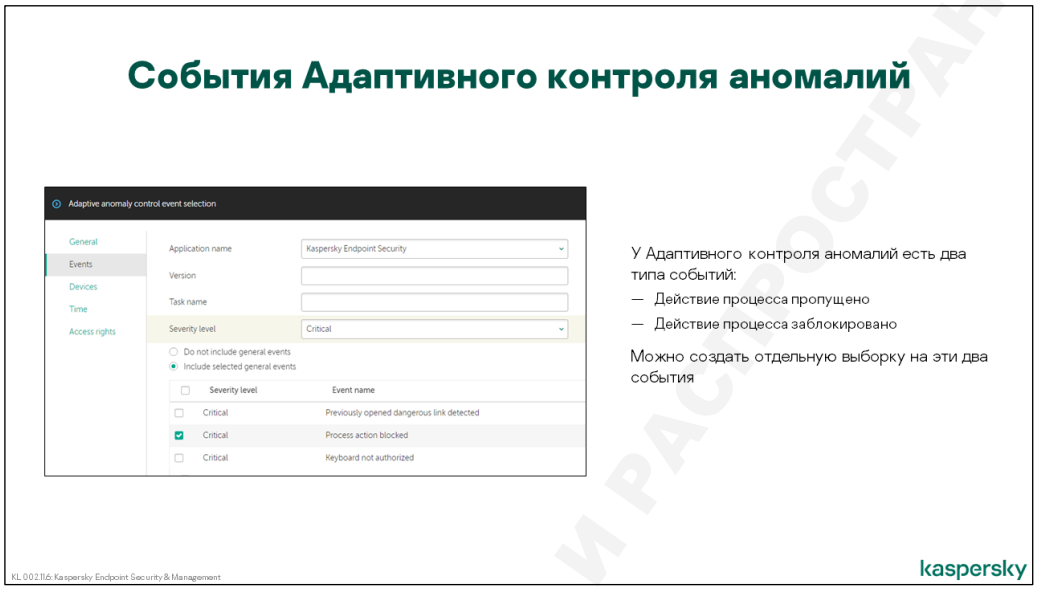
Если пользователь отправил запрос, он придет на Сервер в виде события с уровнем важности *Предупреждение*. Как и в случае других компонентов контроля, для запросов предусмотрена отдельная выборка — Запросы пользователей. Администратору не обязательно реагировать на запросы, но при желании он может, например, настроить себе уведомление по электронной почте. Это можно сделать в политике Kaspersky Endpoint Security.



При каждом срабатывании правила в режимах Блокирование, Интеллектуальное блокирование и Уведомление, Адаптивный контроль аномалий отправляет на Сервер администрирования соответствующее событие с уровнем важности *Критический или Информационный.*

В обоих случаях в событиях указывается название правила, описание подозрительной активности с указанием процессов и контрольных сумм, а также имя пользователя, имя компьютера, дата и время.

Администратор может изучить событие и если он видит, что это легитимная активность, он может сразу из события добавить исключение в политику Kaspersky Endpoint Security для компонента Адаптивный контроль аномалий. Для этого нужно выбрать событие и выполнить команду **Исключить из Адаптивного контроля аномалий**. Если политик для Kaspersky Endpoint Security несколько, мастер предложит выбрать нужную.



У Адаптивного контроля аномалий есть два типа событий:

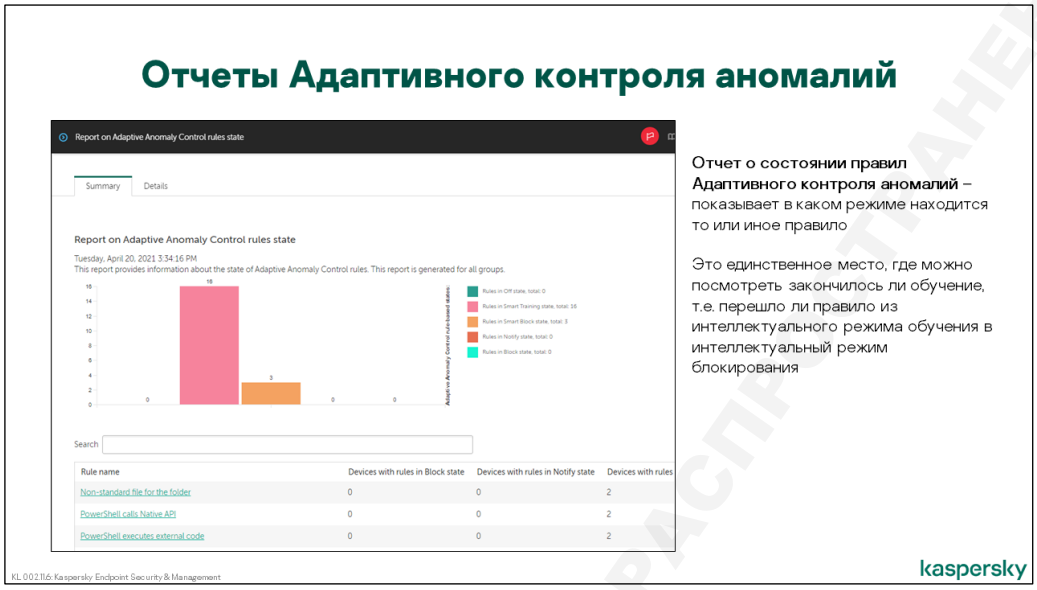
— Действие процесса пропущено — уровень важности *Информационный*
— Действие процесса заблокировано — уровень важности *Критический*

Событие первого типа генерируется, если срабатывает правило Адаптивного контроля аномалий в режиме Уведомление. Событие второго типа генерируется, если срабатывает правило Адаптивного контроля аномалий в режимах Блокирование или Интеллектуальное блокирование.

Если в сети используется Адаптивный контроль аномалий, то рекомендуем администратору сделать отдельную выборку на события от этого компонента.

Все события, в том числе запросы пользователей, по умолчанию хранятся на сервере 30 дней.

5.4 Отчеты о работе Адаптивного контроля аномалий

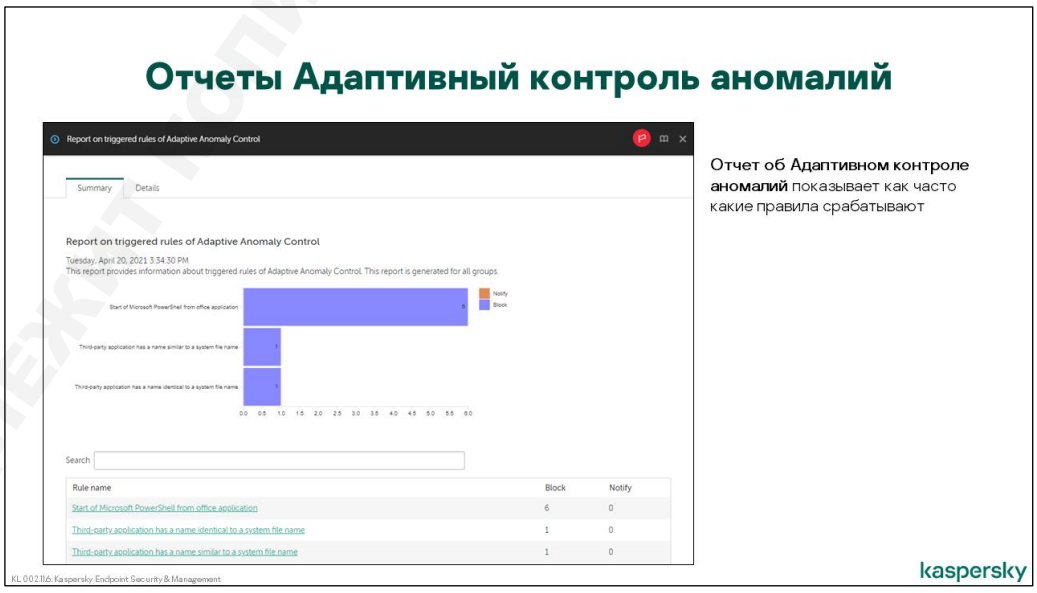


Для регулярного контроля и получения общей картины удобно использовать отчет. Для Адаптивного контроля аномалий есть два типа отчетов:

— Отчет о состоянии правил Адаптивного контроля аномалий
— Отчет об Адаптивном контроле аномалий

Первый отчет показывает в каком режиме находится то или иное правило. По умолчанию приводится суммарная диаграмма, сколько правил находится в том или ином режиме. Если переключиться на вкладку **Подробнее**, то там приводится детальная информация по состоянию правил на каждом конкретном компьютере.

Также этот отчет — единственное место, где можно увидеть какие правила перешли из Интеллектуального режима (Smart) в режим Интеллектуального блокирования (Smart Block).



Отчет об Адаптивном контроле аномалий показывает какие правила срабатывают и в каком режиме, Уведомление или Блокирование. На вкладке **Сводная информация** приводится сводная диаграмма по количеству срабатываний того или иного правила, а на вкладке **Подробнее** можно найти детальную информацию по каждому компьютеру.

Если правило перешло в режим Интеллектуального блокирования (Smart Block), то информация о блокировании попадет в отчет.