

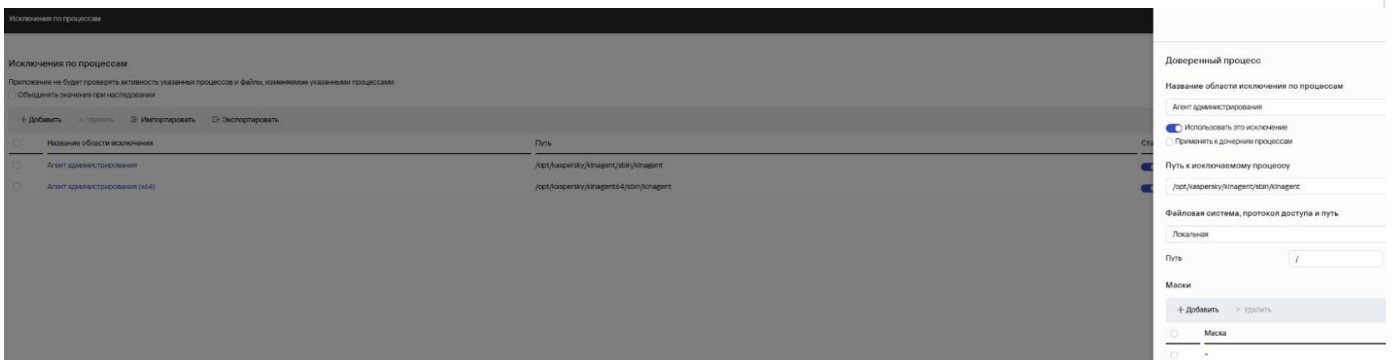
- **Исключения по маске** – KESL не будет проверять файлы с названиями, подходящими под перечисленные ниже маски. Для настройки необходимо в соответствующем разделе выбрать **Добавить** и указать необходимую маску



- **Исключения по названию угрозы** – здесь можно указать исключения по конкретным угрозам согласно [вирусной энциклопедии](#). Для настройки необходимо в соответствующем разделе выбрать **Добавить** и указать необходимую угрозу или её маску



- **Исключения по процессам** – позволяет не контролировать активность указанных процессов и файлы, которые они изменяют, а также дочерние процессы. Для настройки необходимо в соответствующем разделе выбрать **Добавить**, указать название и указать путь к процессу



Также для каждого из перечисленных типов исключения можно активировать параметр **Объединять значения при наследовании**. В таком случае исключения из

родительской политики отображаются в дочерних политиках и доступны для просмотра. Если исключения дочерней и родительской политик совпадают, то эти элементы отображаются как один элемент родительской политики.

Настройка доверенных веб-адресов

Для создания исключения компонента Защита от веб-угроз необходимо в политике KESL в компоненте Защита от веб-угроз выбрать **Добавить** в блоке **Доверенные веб-адреса** и указать необходимый адрес, возможно использование масок.

Защита от веб-угроз

Защита от веб-угроз

Защита от веб-угроз включена

Действие при обнаружении угрозы

Информировать

Блокировать

Параметры Защиты от веб-угроз

Обнаруживать вредоносные объекты

Обнаруживать фишинговые ссылки

Использовать эвристический анализ для обнаружения фишинговых ссылок

Обнаруживать рекламные приложения

Обнаруживать легальные приложения, которые злоумышленники могут использовать для нанесения вреда устройствам или данным

Доверенные веб-адреса

Защита от веб-угроз не будет проверять содержимое веб-сайтов, адреса которых перечислены в списке доверенных веб-адресов.

+ Добавить × Удалить

Веб-адрес

Веб-адрес

Введите адрес или маску адреса веб-сайта:

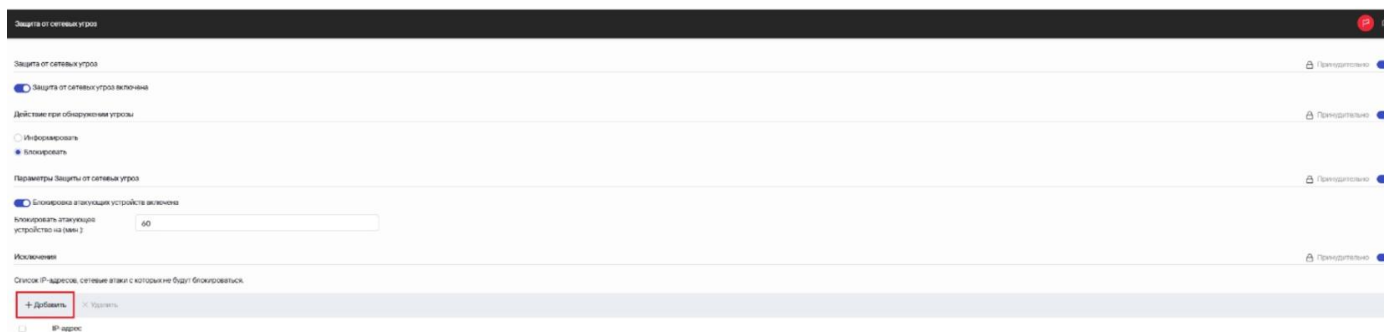
.kaspersky.

Например: *.example.com/*

На указанных веб-сайтах не будет производиться проверка их содержимого

Исключения защиты от сетевых угроз

В случае ложных срабатываний компонента **Защита от сетевых угроз** и блокировок соединений, необходимо добавить соответствующее исключение в для этого компонента в политике KESL нажав **Добавить** и указать необходимый адрес или маску сети



IP-адрес

Введите IP-адрес:

10.68.0.0/16

Например: 192.168.0.0/24 или FE80::/10

Исключения защиты от шифрования

В данном случае речь идёт о возможности исключения работы компонента **Защита от шифрования** для файловых ресурсов, расположенных в общих сетевых директориях защищаемого устройства. Для добавления исключения необходимо перейти в соответствующий компонент в политике KESL. Для обоих типов исключений работает функционал объединения значений при наследовании политик.



Возможно настроить исключение указав нужный путь. При необходимости можно использовать маски для более гибкого исключения, а также указать локальную или смонтированную файловую систему.

Название области исключения

Новая область исключения

Использовать эту область

Файловая система, протокол доступа и путь

Локальная

Путь

/

Маски

+ Добавить × Удалить

Маска

*

Также возможно настроить исключение работы данного компонента только на указанные файлы

Маска объекта

Вы можете задать шаблоны имен файлов, исключаемых из проверки. В этом случае приложение не будет проверять файлы в области проверки, которые описаны с помощью масок в формате командной оболочки, например:

*.doc
file?.*

Задайте маску объекта:

*.log

Исключения для анализа поведения

Компонент **Анализ поведения** позволяет контролировать вредоносную активность приложений в операционной системе. При обнаружении вредоносной активности Kaspersky Endpoint Security может завершать процесс приложения, осуществляющего вредоносную активность. При необходимости добавить процесс в исключение для данного компонента необходимо перейти в соответствующий компонент в политике KESL и выбрать **Настроить исключения по процессам**

Анализ поведения

Анализ поведения

Анализирует поведение приложений и обнаруживает сложные угрозы, такие как приложения-вымогатели.

Анализ поведения включен

Действие при обнаружении вредоносной активности

Информировать

Блокировать

Исключения по процессам

[Настроить исключения по процессам](#)

Исключения по процессам не заданы

В открывшемся окне можно будет добавить исключение, где будет необходимо указать путь и выбрать галочку «Исключать процесс из проверки компонентом Анализ поведения». Также можно применять исключение к дочерним процессам и исключить процесс из проверки компонентами MDR и EDR. При необходимости можно объединять значения при наследовании политик

Название области исключения по процессам

Использовать это исключение

Новая область исключения

Путь к исключаемому процессу

Путь

|

Применять к дочерним процессам

Исключать процесс из проверки компонентом Анализ поведения

Исключать процесс из проверки компонентами MDR и EDR (KATA)

Добавление доверенных устройств

Доверенные устройства – это устройства, к которым у пользователей есть полный доступ. Например, вы можете разрешить доступ к конкретным USB-устройствам или только к USB-накопителям, при этом доступ к остальным USB-устройствам будет запрещен. Кроме того, вы можете указать пользователей или группы пользователей, для которых устройства будут доверенными.

Для добавление доверенных устройств перейдите в раздел **Контроль устройств** политики KESL и выберите **Настроить доверенные устройства**

Контроль устройств

Контроль устройств включен

 Действие, выполняемое компонентом, также зависит от режима перехвата файловых операций, выбранного в разделе "Общие параметры" в подразделе "Параметры приложения".

Доверенные устройства

[Настроить доверенные устройства](#)

Доверенные устройства не заданы

В открывшемся окне будет доступно 2 способа добавления доверенных устройств:

- **Добавить по идентификатору** – позволяет указать маску идентификатора устройства (либо полностью).

Идентификатор устройства

USB*

Устройства, обнаруженные на клиентских устройствах

Название устройства ↑↓	Тип устройства ↑↓	Имя клиентского устр... >> ↑↓	Идентификатор устройства ↑
USB/IP Virtual Host Controller	Неизвестное устройство	gateway	USB\VID_1D6B&PID_0002\VK
USB/IP Virtual Host Controller	Неизвестное устройство	kscl-main-15.sales.lab	USB\VID_1D6B&PID_0002\VK
USB/IP Virtual Host Controller	Неизвестное устройство	gateway	USB\VID_1D6B&PID_0003\VK
USB/IP Virtual Host Controller	Неизвестное устройство	kscl-main-15.sales.lab	USB\VID_1D6B&PID_0003\VK

Затем будет необходимо указать пользователей или группы для которых будут доступны данные устройства (вручную, либо из списка), после этого можно будет добавить комментарий к исключению(опционально)

Пользователи и/или группы пользователей

Выберите пользователей или группы пользователей, для которых устройство будет доверено.

+ Добавить >> Удалить

- Пользователь или группа
- Everyone

Выбор пользователя или группы

Вручную

Список пользователей и групп

Поиск...

- NT AUTHORITY\SERVICE
- NT AUTHORITY\Authenticated Users

- **Выбрать существующее устройство** – позволяет указать конкретные устройства, которые уже известны KSC. Для удобства поиска можно изменить тип устройства и использовать маску идентификатора. Можно выбрать несколько устройств при необходимости.

Доверенное устройство

Устройства, обнаруженные на клиентских устройствах

Тип устройства

Жесткие диски

Маска идентификатора устройства:

SCSI*

<input checked="" type="checkbox"/>	Название устройства ↑↓	Тип устройства ↑↓	Имя клиентского устр... >> ↑↓	Идентификатор устройства ↑↓
<input checked="" type="checkbox"/>	Virtual disk	Жесткий диск	gateway	SCSI\DISK&VEN_VMWARE&PROD.
<input checked="" type="checkbox"/>	VMware Virtual disk SCSI Disk >>	Жесткий диск	KSVLA	SCSI\DISK&VEN_VMWARE&PROD.
<input checked="" type="checkbox"/>	Virtual disk	Жесткий диск	kscl-main-15.sales.lab	SCSI\DISK&VEN_VMWARE&PROD.
<input checked="" type="checkbox"/>	Virtual disk	Жесткий диск	keslla	SCSI\DISK&VEN_VMWARE&PROD.

Затем будет необходимо указать пользователей или группы для которых будут доступны данные устройства (вручную, либо из списка), после этого можно будет добавить комментарий к исключению(опционально)

The screenshot shows a configuration window titled 'Пользователи и/или группы пользователей' (Users and/or user groups). It contains a search bar and a list of users/groups. On the right, there are radio buttons for 'Вручную' (Manually) and 'Список пользователей и групп' (List of users and groups). Below these are two radio button options: 'NT AUTHORITY\SYSTEM' and 'NT AUTHORITY\Authenticated Users'.

Таким образом выбранные доверенные устройства не будут блокироваться для выбранных пользователей, что можно использовать, в том числе и для более точного и гибкого ограничения на работу с внешними носителями информации.

Revision #2

Created 26 June 2026 15:29:49 by Сергей

Updated 26 June 2026 15:46:19 by Сергей