Kaspersky Endpoint Security and Management

Часть III. Контроль

kaspersky

Учебный курс

Содержание

	1.	Общие сведения	3
	1.1	Назначение компонентов контроля	3
	1.2	Лицензии и типы установки	4
	1.3	Установка компонентов контроля	5
	2.	Контроль программ	7
	2.1	Как работает контроль программ	7
		Приниип работы	7
		Как настроить Контроль программ	8
	2.2	Как задать категории программ	9
		Категория, созданная и обновляемая вручную	. 11
		Автоматически наполняемая категория на базе папки	. 18
		Категория на базе эталонных компьютеров	.20
	2.3	Как создавать правила контроля	. 29
			20
		Гежимы работы контроля программ	. 29 . 30
	24	Как это булет работать	32
	2.1		. 02
		Пак опреселить, что именно запрещено конкретному пользователю Покальные уведомления и запросы пользователей	. 32 32
		Выборка Запросы от пользователей	. 33
		События	. 34
		Отчет о запрещенных запусках	. 35
	2.5	Режим Default Deny (запрет по умолчанию)	. 36
	3.	Контроль устройств	. 38
	3.1	Что можно заблокировать и как это сделать	. 40
		Дополнительные параметры	. 43
		Журнал доступа к флешкам	. 44
		Как задать доверенные Wi-Fi-cemu	. 45
		Что делает Анти-Бриджинг	. 46
	3.2	Как задать доверенные устройства	. 47
	3.3	Как настроить взаимодействие с пользователем	. 50
	3.4	Как настроить временный доступ	. 51
		Как пользователю отправить запрос, чтобы получить доступ к заблокированно	ому
		устроиству?	. 52
		Как открыть временный доступ	. 53
	3.5	Мониторинг контроля устройств	. 54
	4.	Веб-Контроль	. 56
	4.1	Критерии блокирования	. 58
	4.2	Настройка исключений и доверенных серверов	. 61
	4.3	диагностика и тестирование	. 62
kaspe	ersky		1



4.4	Настройка взаимодействия с пользователем	
4.5	Статистика работы Вео-Контроля	
4.0	Отчет о работе вео-контроля	
5.	Адаптивный контроль аномалий	
E 4		00
5.1 5.2	Как настроить Адаптивный контроль аномалии	
5.3	Статистика работы Адаптивного контроля аномалий	
5.4	Отчеты о работе Адаптивного контроля аномалий	
kaenere	kv	າ
Ruspers		2



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 ММС-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

- 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

≡ m 4	OPERATIONS / T	HIRD-PARTY APPLICATIO	ONS / APPLICATION CATE	GORIES	Категории задаются сразу для всего
	+ Add × Delete	? Refresh		Q Search	Сервера администрирования
KASPERSKY SECURITY CENTER	Туре	Name	Inherited	Last updated	При модификации категорий на клиентские компьютеры по умолчани
≣ KSC ≱→					всегда проталкивается новый
▲ MONITORING & REPORTING →			No Data		комплект полностью
E DEVICES >					Можно передавать только изменения
A USERS & ROLES >					
ङ operations 🗸 🗸					Настраивается проталкивание в
LICENSING >					свойствах Сервера на закладке
THIRD-DARTY ADDITCATIONS					Категории программ
	ן				
APPLICATION CATEGORIE	J				
APPLICATIONS REGISTRY	J				
APPLICATION TAGS					

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**



2. Контроль программ

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.

- КL-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.

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

Указав исполняемые файлы

			фаилы
		Данн	ные об исполняемых файлах собирают:
O Condition criteria			Koutport prospann
Specify rule type for condition		-	— Предотвращение вторжении
From KL category Select actificate from providence		-	— Задача инвентаризации
 Specify path to application (masks supported) 			
Removable drive	 Condition criteria 		
 Hash, metadata, or certificate 	Charu only files that are sutside the as	elisation categories	
Select from list of executable files	show only mes that are obtaide the a	plication categories	
Select from list of executable files Select from applications registry	C Refresh B Assign to category		
Specify manually From file or from MSI package / archived folder	File name	File version	Туре
	EXE		
	LaunchTM exe	10.0.14393.0 (rs1_release 16071 >	> DE
	Help Exe	10.0.14393.0 (rs1_release 16071 >	> EXE
	O perfmon msc		EXE
	o aculexe	10.0.14393.0	EXE
	Sinnotrap.exe	10.0.14393.1378 (rs1_release 17_>	> EXE
	<u>fissadmin msc</u>		EXE
		10.0.14393.0 (rs1_release 16071_>	> EXE

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

	спользуя ре	естр пр	ограми	N
Condition criteria		Данные ре администр	естра программ н ирования	наполняются Агентом
Specify rule type for condition From KL category Select certificate from repository		Агент бере	эт данные из реес	тра Windows
Specify path to application (masks supported) Removable drive Hash, metadata, or certificate	Condition criteria		14	
Select from list of executable files Select from list of executable files	× Remove applications that are not installed	ign to category 2 Refresh		отсутствует информа
Select from applications registry Specify manually From file or from MSI package / archived folder	Name +	Version	Vendor	КSC, чаще всего это
	ClamWin Free Antivirus 0 99.4 AO Kaspersky Lab		alch	связано с тем, что она просто не успела дойт
	Kaspersky Endooint Security for Windows	11.6.0.394	AO Kaspersky Lab	базу КБС
	Google LLC			Задача инвентаризаци
	Google Chrome	89.0.4389.90	Google LLC	может ускорить проце
	Google Chrome	89.0.4389.114	Google LLC	этом случае
	Kaspersky			
	Exchange Mobile Device Server	13.0.0.11247	Kaspersky	

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 программам, но именно колоставляет сведения об установленных программам, но именно колоставляет сведения об установленных программам, но именно колоставляет 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

Задав свойства фа ме	айла: сертификат, хеш или етаданные
Condition criterie Specify rule type for condition Condition reposition Select certificate from reposition Remonated drive Hash, metodata, or certificate Select from full coll executable files Select from selectable reposition Select from selectable files Select from selectable reposition Secold Transmitty More file or introl MSJ package / archived folder:	 Основной сибите Сертификат
KL.002116-Kaspersky Endpoint Security& Management	kaspersky

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 попрежнему 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 KLкатегорий, которые как раз и определяют класс или тип программы — почтовые программы, браузеры, инструменты для разработки, электронные платежные системы и т.д. Термин KLкатегория 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 КL-категориям. Все некатегоризированные файлы автоматически относятся к KL-категории **Другие программы**.

Задав путь к файлам в явном виде

Condition criteria	
Specify rule type for condition From KL category State t catfit at from reportions	
Specify path to application (masks supported) Bemovable drive	O Condition criteria
 Hash, metadata, or certificate 	Specify the path to the folder in which running or downloading executable files, scripts, and modules will be monitored. Use regular expressions such as C\Program Files\Internet Explorer*. We do not recommend using this type of criterion because using common criteria, such as folder path, is unsafe.
	C (Wersadministrato/Downloads)*
	— Проверяется только путь
	— Поддерживаются маски — «*» и «?»

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.



Condition criteria			
Specify rule type for condition From KL category			
Select certificate from repository Specify path to application (masks supported) Removable drive	New Category Wizard		
 Hash, metadata, or certificate 	Conditions		
	× Delete + Add ≠ Properties		
	 Condition criterion 	Condition value	
	Media	Removable drive	
		сменные носители	
			u u

 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

	Указав сер	тификаты
Condition criteria Specify rule type for condition General condition		Выбрать можно любые сертификаты из хранилища Сервере администрирования
Fourie Company Specify path to application (masks supported) Removable drive Hash, metadata, or certificate	Condition criteria	(2) m x
		t≣ Filter
	Serial number	Issued to
	010731D47844570857C4C90411054525	Cheldongie Ltd., Cerdoogie Ltd., Cerdoogie Ltd., Cerdoonaania View, Secandonia, Cerdoo
	0A91F3R6841F24786Ra268D145DCA144	Cherkaspersky Lab 3CC. Oll #Kaspersky Lab. 0#Kaspersky Lab.3CC. L#Moscow. C#RLLSERIALNIIMRER#10277395
	013C6684E0F39030C05FA36B42AF33CA	CN=Kaspersky Lab JSC, O=Kaspersky Lab JSC, L=Moscow, C=RU
	OF668F80F0F0028774C7DD8D769EE581	CN=Kaspersky Lab, O=Kaspersky Lab, L=Moscow, S=Moscow City, C=RU
	OF9D91C6ABA86F4E54CB89EF57E68346	CN=Kaspersky Lab, O=Kaspersky Lab, L=Moscow, C=RU
	☑ 0C15BE4A15BB0903C901B1D6C265302F	CN=Google LLC, O=Google LLC, L=Mountain View, S=ca, C=US
	OC5396DCB2949C70FAC48AB08A07338E	CN=Mozilla Corporation, O=Mozilla Corporation, L=Mountain View, S=California, C=US
	055F937A9DF73DFD90BA9889E4C50A11	CN="Notepad++" O="Notepad++" L=Saint Cloud S=lle-de-France C=FR

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

) New Category Wizard		Исключения можно задавать только для создав:
Exclusions		вручную категорий
→ Delet > + Add / Properties		
	Condition entere Specify rule type for condition From K. Leagary Select entificate from repository Select path to application (inside supported) Removable drive Hahn. metadas. or certificate Select from tot of encodable files Select from tot of encodable files Select from splications highlight Select from splications highlight From file or from MSI package / archived tolder	

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

		папк	Ν	
New Category	Vizard		Такие категории обновляются:	
Name	New category		 — автоматически при изменении сос (добавлении или удалении) 	тава папі
Select category creation method Category win content added minutally. Data of executable files is manually added to the category. Category that includes executable files from a specific foldor: Executable files of applications copied to the specified folder are automatically processed and there metaics are added to the category. Category that includes executable files from a specified foldors. There executable files are processed automatically and there metcory are added to the category.		cutable files is manually added to the category. file folder: Executable files of applications copied to the in metrics are added to the category. d devices. These executable files are processed eony.	— по расписанию	
Category w	Inclusio only unique conditio New Category Wizard	or from the Ultrard		
	Specify the folder to be used by Ad	ministration Server to search regularly for executable files, process them auton	matically, and add their metrics to the category.	
	 Include dynamic-link libraries (Include script data in this catege Calculate SHA-256 for files in the Windows and later versions) Calculate MD5 for files in this calculate MD5 for files in the file of the file of	DLL) in this category ory his category (supported by Kaspersky Endpoint Security 10 Service Pack 2 for ategory (supported by versions earlier than Kaspersky Endpoint Security 10		
Calculate MD5 for files in th Service Pack 2 for Windows				

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

		_		
Application Control attings	Kaspersky Endpoint S	ecurity		? – 🗆
Application Control settings	← Applications	from registry		
nolization Startun Control mode				
Derwist. All applications, except for the ones in the rules list, are allowed				Q. Search
Blocked applications	File	Vendor	Location	KL category
	Infrare available	Microsoft Corporation	C\Windows\bfsvc.ava	Golden Image\Opera
Allowed applications	U DIAVGENE	microsoft corporation	C.(Windows(Distclexe	Goiden image (opera
lvanced Settings	💰 hh.exe	Microsoft Corporation	C:\Windows\hh.exe	Golden Image\Opera
Control DLL modules load	HelpPane.exe	Microsoft Corporation	C:\Windows\HelpPane.exe	Golden Image\Opera
modules load control mode significantly increases the load on the system	🐂 explorer.exe	Microsoft Corporation	C:\Windows\explorer.exe	Golden Image\Opera
plications from registry	a) notepad.exe	Microsoft Corporation	C:\Windows\notepad.exe	Golden Image\Opera
of applications	→	Microsoft Corporation	C:\Windows\splwow64.exe	Golden Image\Opera
nplates	💰 regedit.exe	Microsoft Corporation	C:\Windows\regedit.exe	Golden Image\Opera
Save	Cancel	Microsoft Corporation	C\Windows\winbln32.exe	Golden Image\Operat

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 КL-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 по добавить и добавить в сети, но токое 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

m đ		-		-	
	OPERATIONS / THIRD-PARTY APPLICATIO	ONS / APPLICATIONS REG	ISTRY	— Через Реестр прог	рамм
(FT)	× Remove applications that are not installed	tegory] 😂 Refresh	Q Search		
KASPERSKY	Name I	Version	Vendor	— Из списка исполняе	мых файлов
SECURITY CENTER	Mozilla Mantenance Service	New Category Wizard			
OPERATIONS -	Mozilla Maintenance Service	Content cart goly maard			
	Mozilla Thunderbird 60.4.0 (x86 en-US)	Action on executable file r	lated to the event		
Contrast of the second s	Notepad++ Team	Add to a new applicati	in category		
THIRD-PARTY APPLICATIONS ~	Notecad++132-bit x86	Rule type	cauon calegory		
APPLICATION CATEGORIE	TeamViewer	 Rules for adding to inc 	usions		
APPLICATIONS REGISTRY	TeamViewer 13	Rules for adding to exc	lusions		
APPLICATION TAGS	Unknown Publisher	 Certificate details (or S 	IA-256 hashes for files without a certificate)		
EXECUTABLE FILES	Windows Defender for Server 2016	 Certificate details (files Ophy SMA-256 (files with 	without a certificate will be skipped)		
MONITORED APPLICATION	VMware: Inc.	 Only MD5 (discontinue 	d mode, only for Kaspersky Er		
REPOSITORIES >	VMware Tools	Category will includ	New C New C	tegory wizard	
	and a second sec	Category witt includ	only and condition		

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.

	Удобно	использо	вать	фил	њтр	
				τ		
≡ m 4	OPERATIONS / THIRD-PARTY	APPLICATIONS / EXECUTABLE FILES				
	Show only files that are outside the ap	plication categories				
KASPERSKY	2 Refresh Eg Assign to category		Q. Search		* 7	
SECURITY CENTER	File name	File version	Туре	Applic	ation name	
	EXE				Eitear	
<u> </u>	vmtoolsd.exe	10.0.9.55972	EXE	V8	Fillers	
▲ MONITORING & REPORTING →	VMConnect.exe	10.0.14393.0 (rs1_release 16071 >	> EXE	M	+ Add × Clear all	
t∎ DEVICES >	DevModeRunAsUserConfig.msc		EXE			
と USERS & ROLES 、	devmomt.msc		EXE		Property	
	VMwareAkasimport.exe	10.0.9.55972	EXE	V	Туре	
	DevModeRunAsUserConfig.msc		EXE		Condition Value	
LICENSING >	devrogmt.msc		EXE		= ~ EXE	
THIRD-PARTY APPLICATIONS	vmtoolid.exe	10.2.0.1608	EXE	10		
	VMToolsHookProc.exe	10.0.9.55972	EXE	15	Property	
	VMwareAliasImport.eve	10.2.0.1608	EXE	. W	File name	
	VMConnectexe	10.0.14393.0 (rs1_release 16071 >	> DE	M	Condition Value	
EVECTION DI COLCE					= ~ *vm*	

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

	<u> </u>		-		
H	аиденные	на компьютере			
≡ m A devices / M	ANAGED DEVICES				
Current path: KSC	Managed de 🗿 KSC				Р
KASPERSKY + Add devices × SECURITY CENTER	Delete +1 GENERAL APPLICATIONS A	CTIVE POLICIES AND POLICY PROFILES TASKS EVENTS INCIDENTS	TAGS ADVANCED		
Name	Applications registry				
	Executable files				証 Filt
▲ MONITORING & REPORTING >	Distribution points	Name	Version	Vendor	Updates
	Hardware registry	Microsoft Visual C++ 2008 Redistributable - x64 90 30729 6161	9.0.30729.6161	Microsoft Corporation	0
POLICIES & PROFILES	Available updates	Microsoft vss Writer for Sull Server 2017	17.00.11047	Microsoft Corporation	0
TASKS	Software vulnerabilities	Exchange House Device Server	14.0.1000.169	Microsoft Corporation	0
MANAGED DEVICES	Remote diagnostics	Discound Visual Case 2008 Redistributable - v86.9.0.30720.4148	9.0 30729 4149	Microsoft Corporation	0
DISTRIBUTION POINTS		Microsoft SOL Server 2017 Setup (Epolish)	14.0 1000 169	Microsoft Corporation	0
MONING PLIES		Microsoft SOL Server 2017 T-SOL Language Service	14.0.1000.169	Microsoft Corporation	0
DEVICE SELECTIONS		Microsoft SQL Server 2017 (64-bit)		Microsoft Corporation	0
THE		Kaspersky Security Center Administration Server	130011247	Kaspersky	0
TAGS		Kaspersky Security Center Web Console	13.0 10253	Kaspersky	0
HIERARCHY OF GROUPS		Microsoft Visual C++ 2015 Redistributable (x64) - 14.0.23506	14.0.23506.0	Microsoft Corporation	0
			14.0100000		

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

	Создайте задачу инвентариз	ации
= m 4	DEVICES / TASKS	Задача найдет файлы,
	Current path XSC +448 0 Bart III Proce D Resure Q. Search. 2	или нерегулярно
B KSC ► >	Taak name Application Kaspersky Endpoint Agent	Важно регулярно выполнять инвентаризацию эталонных
▲ MONITORING & REPORTING →	Databases and Module Lixities Rapersity Endpoint Agent Kaspersity Endpoint Add Task Wizerd	компьютеров
POLICIES & PROFILES	Kaspersiy Security New task	Выполнять инвентаризацию всех компьютеров сети
TASKS MANAGED DEVICES	Advisionation Server Application Deventional uselites: Kaspersky Endpoint Security for Windows 111.6.01	не рекомендуется
MOVING RULES DEVICE SELECTIONS	Backs of Administ Task type Task type Kapensky Security Kapensky Security	
	End whereholders Inventory Kaspersky Security Kaspersky Security Kaspersky Security	
ABC\ADMINISTRATOR	Database Undate Specify device addresses manually or import addresses from a list	



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

	Включ	ите Контроль программ	
Kaspersky Endpoint Security for Win	dows (11.6.0)	По умолчани	ю он выключ
 High protection level. 			6
GENERAL EVENT CONFIGURATIO	ON APPLICATION SETTINGS REVISION	O Application control	
Advanced Threat Protection	Application Control	Application Control	A Enforce
Essential Threat Protection	This component monitors users' attempts to	Application Control ENABLED	
Security Controls	Davina Control	This component monitors users' attempts to start applications and controls the startup of applications by using rules.	
Detection and Response	This component allows you to control the co	Application Control Settings	A Enforce
Data Encryption		Kaspersky Endpoint Security for Windows blocks startup of applications that are blocked by Application	
Local Tasks	Web Control This component allows you to control access	Control settings. Kaspersky Endpoint Security for Windows does not block startup of applications that could be blocked by Analistical Control settings that long information about it in the renord (Ret model)	
General settings		View report	
	Adaptive Anomaly Control This component detects and blocks abnorm	Application Control Mode	
		In Denylist mode, Application Control allows all users to start any applications except for those listed in the Application Control blocking rules.	In Allowlist mode, Applicatio
ata transfer to Administration Server		Control blocks all users from starting any applications except for those listed in the Application Control allowing rules.	
About files in Backup	Ī	Allowlist	
About unprocessed files		Rules Lists Settings	
About installed devices		Denylist and Allowlist Rules Settings	
About started applications About file encryption errors			-
Report on Adaptive Anomaly Contro	ol rules state	Чтобы он не просто работал, но еще и уведомлял KSC — надо не за	быть
Report on triggered Adaptive Anom	aly Control rules	включить пересылку событий	

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»)

	A state of the sta	A Enforce
Application Control Settings Bigestation Control Settings Water Mindows blocks startup of applications that are blocked by Application Water Mindows Security for Windows does not blocks startup of applications that calle blocked by Application Control Security for Windows does not blocks startup of applications that calle blocked by Application Control Mode Application Control Addees In Demysist tools, all users to start any applications except for those listed in the Application Control allows all users to start any application except for the applications control allows in the second on Control allows all users to start any application except for the application Control allows all users to start any application except for the application Control allows all users to start any application except for the application Control allows all users to start any application except for the application Control allows all users to start any application except for the application Control allows all users to start any application except for the application Control allows all users to start any application except for the application Control allows all users to start any application except for the application Control allows all users to start any application except for the application Control allows all users to start any application except for the application Control allows all users to start any application except for the application Control allows all users to start any application except for the application Control allows all users to start any application except for the application Control allows all users to start any application except for the application Control allows all users to start any application except for the application Control allows all users to start any application except for the application Control allows all	Applications control ENABLED This component momony users unterrings to start applications and controls the starting of applications by using rules.	O Denylists and allowlists
Application Control Allows all users to start any application except for those load in the Application Control allows all users to start any application except for the applications specified in Application Control Control Allows all users to start any application except for the applications specified in Application Control Allows all users to start any application except for the applications specified in Application Control Allows all users to start any application except for the applications specified in Application Control Allows all users to start any application except for the applications specified in Application Control Allows all users to start any application except for the application Control Allows all users to start any application except for the application Control Allows all users to start any application except for the application Control Allows all users to start any application except for the application Control Allows all users to start any application except for the application Control Allows all users to start any application except for the application Control Allows all users to start any application except for the application Control Allows all users to start any application except for the application Control Allows all users to start any application except for the application Control Allows all users to start any application except for the application Control Allows all users to start any application except for the application Control Allows all users to start any application except for the application Control Allows all users to start any application except for the application Control Allows all users to start any application except for the application Control Allows all users to start any application except for the application Control Allows all users to start any application except for the application Control Allows all users to start any application except for the application control allows all users to start any application except for the application control allows all users to start	Application Control Security for Windows blocks statup of applications that are blocked by Application • Kapenyky Endpoint Security for Windows blocks statup of applications that are blocked by Application • Kapenyky Endpoint Security for Windows blocks statup of applications that are could be blocked by Applications and the security block statup of applications that could be blocked by Applications	Denylists and allowlists Denylist (sctive) Allowlist
Corylist Allowidt Name Status Test mode Allowed Blocked	Application Control Mode Application Control Allows All uses to stat any applications except for those listed in the Application Control Control block all uses from starting any applications except for those listed in the Application Control	Application Control allows all users to start any application except for the applications specified in Application Contro
Pulse Liste Satisan	Denylist Allowlist	Name Status Test mode Allowed Blocked
Decusion Allowite Rules Settings	Rules Lists Settings Denylist and Allowlist Rules Settings	Rrowsers Enabled - Even

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

Denylists and allowlists			
Denylists and allowlists	Application Control rule		Application categories
Denyist lactivel Allowist Application Control allows all users to start any application except for the application Application Control allows all users to start any application except for the application Application Control allows Test mode Allow Developmentume approximation D	Action	tion Control settings (Test mode) Control settings gory. xp to create executable files that will be allowed to	Application categories Search.
голько к категориям, но и ко всем процессам, которые будут нициированы объектами из категории	Deny for other users + Add × Delete User or group Everyone	Launch privileges	Список всех категорий на I для которых еще нет прави

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 обновления¹

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 специальная² КL-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 КL-категорию при настройке условий для категории программ нельзя

2.4 Как это будет работать

Как определить, что именно запрещено конкретному пользователю

				пол	ьзователю	
Imperies: Repeaky Endpoint S High protection level Sections General Event configuration Advanced Threat Protection	All recommended protection compor Application Control	nents are enabled. empts to start application	s and controls	the startup of	Статический анализдоступен	н только в ММС-консоли KSC
Issential Threat Protection Detection and Response learnity Controls Application Control Device Control Web Control Adaptive Anomaly Control	Application Control settings Control mode: Denylist + Add D Edit X Remov Status Rule na 1 On Browsees	Action: Test rules Action: Static and Action: Test rules Action: Test rules Action: Test rules Action: Test rules	alysis	P Blocked Veryone	×	R
was una gibini alinaral actinga Una gantinga Una gantinga Una dan hatary	Control DLL modules load (n) Managa template cettings Templates Configure 1	Name	Isa No No	Policy Kaperski findport Secz Kapersky Endport Secz Kapersky Endport Secz	Ord de "Novidade" de "Unitaria to sea a la d'al descondate fine blocked finunde de la descondate fine blocked finunde de la descondate fine blocked finance. Vers blocked fine Novidade fine	Вывести список заблокированных файл Список категорий, для которых есть запрещающие что-то этому пользователю правила

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 ММС-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

= m /t		ELECTIONS	На Сервер KSC в виде	события, в ко	отором буде	,et:
	Selection All selections	LLECTIONS	 Текст, который недово отредактировать, доб 	ольный пользов авив что-то сво	ватель может ре	Г
KASPERSKY	type + Add Properties D Reconfigure sorting and start.	× Delete	— Идентификатор его ко	мпьютера		
SECURITY CENTER	Selection name	Selection type	— Имя пользователя			
⊑KSC ≁→	User requests	Predefined selection	— Информация о файле,	который был з	аблокирован	4
▲ MONITORING & REPORTING ↓	Critical events	Predefined selection	— Почему он был заблок	ирован: катего	рия и правило	10
DASHBOARD	Result of User requests on 04/16/2021 2:53:36 pm				e = ×	
EVENT SELECTIONS	C Refresh list × Delete () Export to file () Ass	sign to category 🛛 🗃 Revision	history 🛛 🗃 Exclude from Adaptive Anomaly Control	Q Search	☆ 7	
NOTIFICATIONS	Event occurred Device Event		Description		Administration gr	
DEVERSION ANNUALEMENTS T∎ DEWCES > & USERS & ROLES >	04/16/00122337.cm T0H-U470P Apple	ation startup blockage me >>	Held Page allow me to work with the file chrome exe that has been block control inte Control inte Control interesting and the set of the control interesting and the con	d according to an Application	Managed devices	

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.

Что мож	кет сдел	ать адми	нистра	торво	ответ?
Result of User requests on 04/16/2021 2:53:36 pm				<mark>е</mark> ш х	
② Refresh list X Delete ⊕ Export to file SAss	ign to category 🗃 Revision history	🗃 Exclude from Adaptive Anomaly Control	Q Search	\$ ₹	
Event occurred	Device	Event	Description	Administration group	
	IUM-LAYIUP	-spinoton tanup bockage me>>	Press allow me to work with the file chrome end that basens locked according to a Algobian Centrol nue. The properties Chronic nue chrogens Files biolitocopie (Chrome Algobian Files biolitocopie) (Chrome Algobian Wender Coopie) LiC August 1980 1980 1980 1990 Wender	munged Devices	
Добавить файл в другую кат Например, для которой есть	егорию исключение из об	щего запрещающего і	правила		
002.11.6: Kaspersky Endpoint Security & Management					kaspersky

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

New event selection			1	
			1.	Запуск программы разрешен
General	Application name	Kaspersky Endpoint Security	~ 2.	Запуск программы запрещен
Devices	Version		3.	Запуск программы разрешен в тестов
Time	Task name			режиме
Access rights	Severity level	Info	~	(по умолчанию на КSC не пересылаето
	 Do not include general e Include selected general 	events		менять в политике Kaspersky Endpoint Security)
	Severity level	Event name	4	Запуск программы запрешен в тестов
	Info	Application startup prohibited in test mode		режиме
	Info	Application startup allowed in test mode	5	
		A page that is allowed was opened	5.	запуска программы
		File operation performed		
			Па	умолчанию выборки нет, но ее всегда
			MC	



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

Настройте реж	им Запре	тпо	умо	лчан	ию	
Application Control	•	1	Есть вст	роенные пр	авила:	
Application Control		🔒 Enforce 💽	— Опер – ста	ационная си ндартные фа	стемаие йлы ОС (п	е компонент 10 умолчанию
Application Control ENABLED This component monitors users' attempts to start applications and controls the startup of applications by using rules.			включ	чено)		
Application Control Settings		🔒 Enforce 💽	— Дове умол	ренные прогр чанию выключ	раммы об чено	оновления — г
Kaspersky Endpoint Security for Windows blocks startup of applications that are blocked by Application Control settings. Kaspersky Endpoint Security for Windows does not block startup of applications that could be blocked b Application Control settings. But logs information about it in the report (Test model.	 Denylists and allowlists 		9			
View report Application Control Mode	Denvlists and allowlists					
In Denylist mode, Application Control allows all users to start any applications except for those listed in the A Control blocks all users from starting any applications except for those listed in the Application Control allow	pp in Denylist Allowlist (active)					
Dervist Allowlist	Application Control blocks all users fro	m starting any application	ons except those sp	ecified in Application Con	trol allow rules.	
Rules Lists Settings Denylist and Allowlist Rules Settings	+ Add × Delete 1 Import	t 💱 Export				
Advanced settings	Name Status	Te	est mode	Allowed	Blocked	Trusted Updaters
Control ULL modules load (significantly increases the load on the system)	Trusted Updaters Golden Image	 Enabled Enabled 		Everyone	•	
При переходе в Белый список — другой набор правил						
principal de de la contra de la principal de l						kaspers

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 флэшнакопителей. 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.

Блокиров	ка шины устройства:
 Infrared Serial Port Parallel Port USB FireWire PCMCIA 	Но разрешения для устройств (предыдущий слайд) всегда имеют более высокий приоритет
Устройства обработки изображений шине	і (например, сканеры) можно заблокировать только по
Клавиатуры и мыши заблокировать н	ельзя в принципе
Чтобы злоумышленник не мог замаск есть специальный компонент Kaspers устанавливается отдельно	кировать флеш-накопитель под клавиатуру или мышь, sky Endpoint Security. Называется BadUSB,
KL 002.11.6: Ka spersky Endpoint Security & Management	kaspersky

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

Kaspersky Endpoint Security for Windo	wws (11.6.0)	В политике Kaspersky Endpoint Se	curity
High protection level.		Device Control	(2)
GENERAL EVENT CONFIGURATION	APPLICATION SETTINGS		
Advanced Threat Protection	Application Control	Device Control	🔒 Enforce 💽
Essential Threat Protection	This component monitors users' a	Device Control ENABLED This composed allows use to control the comparison of removable driver	
Security Controls	Device Control		
Detection and Response	This component allows you to con	Device Control Settings	🔒 Enforce 💽
Data Encryption	Web Control	Allow requests for temporary access	
Local Tasks	This component allows you to con	Access rules for devices and Wi-Fi networks Access to the types of devices	
General settings	Adaptive Anomaly Control		
	This component detects and block	Connection buses Connection bus access rules	
		Trusted devices List of devices, access to which is always allowed	
		List of devices, access to which is aways allowed	

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.



Настройте блокирован	ие по типам у	стройств
Device Control		
Device Control		
Device Control ENABLED This component allows you to control the connection of removable drives.	Types of devices	
Device Control Settings		
 Allow requests for temporary access 	Access To Storage Devices	
Access rules for devices and Wi-Fi networks	Name	Access
coes to the gpes of devices	Hard drives	Depends on connection bus
Connection buses	Removable drives	Depends on connection bus
connection bus access rules	Floppy disks	Depends on connection bus
Insted devices	CD/DVD drives	Depends on connection bus
list of devices, access to which is always allowed	Portable devices (MTP)	Depends on connection bus
повия, которые задаются тут, имеют более высокий	Access To External Devices	
иоритет , чем условия по шинам (следующий слайд)	Name	Access
я Wi-Fi сетей можно задать список доверенных и	Printers	Depends on connection bus 👻
лючить остальные по ссылке Правила доступа для	Modems	Depends on connection bus 👻

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 (МТР)
- 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 (МТР) 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.

Device Control	По ссылке Шины подключения	
Device Control		
Device Control ENABLED This component allows you to control the connection of removable drives.	По умолчанию все шины разрешены	
Device Control Settings		
 Allow requests for temporary access 	O Connection buses	
Access rules for devices and Wi-Fi networks Access to the types of devices		
	Device connection buses	Access
Connection buses Connection bus access rules	Infrared port	Allow
	Serial Port	Allow
rusted devices, ist of devices, access to which is always allowed	Parallel Port	Allow
	USB	Allow
	FireWire	Allow
	PCMCIA	Allow

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

Задайте расписание д	оступа для у	стройств
Device Control		
Device Control ENABLED		
This component allows you to control the connection of removable drives.	Types of devices	
Device Control Settings		
Allow requests for temporary access	Access To Storage Devices	
ccess rules for devices and Wi-Fi networks	> Name	Access
coss to the gipes of betwees	Hard drives	Depends on connection bus
onnection buses	Removable drives	Depends on connection bus
onnection ous access rules	Floppy disks	Depends on connection bus
usted devices	CD/DVD drives	Depends on connection bus
st or devices, access to which is always allowed	Portable devices (MTP)	Depends on connection bus
льзователям можно ограничить доступ по расписанию к:	Access To External Devices	
Жестким дискам	Name	Access
	Drinterr	Depends on connection bus
дискетам	Printers	

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.

Types of devices					
Assess To Storage Davises					
Name	Access				
Hard drives	Depends on connection	n bus	Device Access Rules		
Removable drives	Depends on connection	n bus			
CD/D Porta Device Access Rules Logging Access Configuring device access rule			Rights of the selected group o Write Read Priority 0	f users by access schedules	-
Access			Users' rights	Schedule editor	
O Block			-t Add V Delete	Name	Business hours
Mode				00 01 02 03 04 05 06 07 08 09 10 11 Mo Tu We Th	12 13 14 15 16 17 18 19 20 21 22

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 флэшнакопитель и что-то на нее скопировать, сразу после применения политики она станет недоступна и следующая операция заблокируется.

Types of devices		Device Control Settings
Access To Storage Devices		Device Access Rules Logging
Name Hatd drives Benrouted adves CD/DVD dress Bostable devices IMTE Access To External Devices Name	Access Depends on connection bus Access	Logging Logging ENABLED The function like your monitor information about operations on files located on removable drives. File operations elete Write Filter on file formats Al formats M formats
Printers Moderns и же, нажав Запись собь	Depends on connection bus Depends on connection bus TITILIB B ЖУРНАЛ	Text files Video files Audio files Graphic files Executable files Trice files

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

Device Control	1. Прокрутить спис	ок до самого конца и кликнуть на W
Device Control ENABLED This component allows you to control the connection of removable drives.		
Device Control Settings		
Allow requests for temporary access		
ccess rules for devices and Wi-Fi networks ccess to the types of devices	Bluetooth	Depends on connection bu
Connection buses connection but access rules	Cameras and scanners	Depends on connection bu
Tutted services and a functions access to which is above allowed	Access to Wi-Fi networks	
	Name	Access
	Wi-Fi	Allow
Invention has access have	Access to Wi-Fi networks Name Wi-Fi	Access Allow

Hac	тройте доверенн	ые Wi	-Fi-сети
Bluetooth	Depends on connection bus ~	и се	сылке правила доступа для устроисті тей Wi-Fi
Cameras and scanners	Depends on connection bus v	1. Г	Ірокрутить список до самого конца и ликнуть на Wi-Fi
Name Wi-Fi	Access Allow	2 E 3	Зыбрать уровень доступа (Разрешающе Запрещающее, Запретить с гсключениями)
Trusted Wi-Fi networks		З. Г	1ри необходимости добавить роверенные сети Wi-Fi
Access to Wi-Fi networks	Add Wi-Fi network Enter the settings of the trusted network for which you want to authorize connection.	-	
Allow	Network name ABC_Guest		
Block with exceptions	Authentication type WPA2-Enterprise ~		
Trusted Wi-Fi networks	Encryption type Any ~		
+ Add × Delete	Comment		
	Note: a network is only considered to be trusted when the encryption type, authentication type, and the network name		

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



– 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

Для чего нужен А	нти-Бриджинг?	
D Dewa Control	- По умолчанию Анти-Бриджинг вы	ключен
Allow requests for temporary access Access rules for devices and Wi-Fi networks Access to the types of devices Connection bases Connection ba	Анти-Бриджинг блокирует дублир через: —Сетевые адаптеры —Wi-Fi —Модемы	ующие подключени:
Lindis devices	Anti-Bridging Anti-Bridging Anti-Bridging	
подаление и пользователю будет разрешено установить	Enabling Hos Bridging lets you prevent bridge connections from being enablished. Rules for devices Select connections that cannot be established simultaneously. Only one connect	tion of this type can be active according to
олько одно соединение в каждый момент времени	Move up Move down Device type	Control
Занти-бриджинге участвуют только те типы	Network adapter	O Off
юдолочении, которым выставлен ВКЛ, остальные в таком	Vi-Fi	On
any de ne komponepyroton	Modem	

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

Зачем нужны доверенные устройства?	
Например, это может быть флешка администратора, на которой он будет х утилиты для траблшутинга	кранить
Доверенное устройство можно задать по:	
— Его персональному ID — Маске для ID — Модели устройств	
Доверенные Wi-Fi-сети мы рассмотрели раньше	
L. 0.02.1%. Kaspersky Endpoint Security & Management	aspersky

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.

Посарь	I C A	верен	пыс устройства	•	
vevice Control			Там же, в политике Казр	ersky Endr	oint Security
evice Control			Чтобы добавить устрой	ство, его н	адо:
Device Control ENABLED This component allows you to control the connection of removable drives.			1. Подключить к любой есть Kaspersky Endpo	рабочей с bint Securit	танции, где у
evice Control Settings Allow requests for temporary access coess nules for devices and Wi-Fi networks coess to the types of devices			2. Дождаться, пока на К	SC придет	событие
onnection buses onnection bus access rules	Add true	isted devices			ршх
tutted devices for which is always allowed	Step :	1. Add trusted devices by IE		5	
					‡≡ Filter
		Name	Device ID	Device type	Computer name
		Generic Flash Disk USB Device	USBSTOR\DISK&VEN_GENERIC&PROD_FLASH_DISK&REV_8.07\874318176	0 Removable drives	
		Generic Flash Disk USB Device	USBSTOR\DISK&VEN_GENERIC&PROD_FLASH_DISK&REV_8.07\83F19E80&	Removable drives	

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.

usted devices			1.	Выбрать	ь метод	
) Merge values when inheriting			2.	Заполни	ить поля фильтра	
+ Add device by ID + Add device by model + Add device by ID mask +	+ Add device by model mask 🧳	Edit X Delete	3.	Выбрать	ь устройства	
Export		Name	4.	Выбрать	ь пользователей	
Device inodet Device ID						
		Northe	5	Примен		
		1 YURT FG	5.	Примени	ить политику	
		1968 FPG	5.	Примени	ить политику	
d trusted devices		THE THE	5.	Примени elect user o	ИТЬ ПОЛИТИКУ or group	×
M trusted devices ep 1 Add trusted devices by ID		Hanna	5.	Примени elect user o	ИТЬ ПОЛИТИКУ or group	x
M trusted devices ep 1. Add trusted devices by ID en		TYPE I IN	5.	Примени elect user o tom	ить политику or group -LAPTOPIAdministrator	x Q
M trusted devices by ID en		Device type	5.	Примені elect user o tom том-	ить политику or group АРТОРИdministrator АРТОРИdministrator	Q Q
M trusted devices ep 1. Add trusted devices by ID en Name Device ID Common: Flash Disk USB Device USBSTOR/DISKMVEN_CENERICEPROD_FLAX	SH, DISK6REV, 807/8743181760	Device type Removable drives	5.	elect user o tom том- том- том-	ITE ПОЛИТИКУ or group -LAPTOP/Administrator -LAPTOP/DefaultAccount -LAPTOP/Guest	x

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.

	К	уда уйде	ет пр	оосьб	а пользова	теля?
=	m 4	MONITORING & REPORTING	EVENT SELEC	TIONS	На Сервер KSC в виде	е события, в котором будет:
	KASPERSKY	Selection All selections type + Add / Properties > Reconfigure s	▼ Orting and start ×	Delete	 Текст, которыи польз Идентификатор и опи 	зователь может редактировать исание заблокированного устройства
		Selection name User requests		Selection type Predefined selection	 Имя пользователя Компьютер Операция с устройст 	
		Recent events Critical events		Predefined selection Predefined selection	— Дата и время	
,		Result of User requests on 04/19/202 C Refresh list × Delete @ Export	1 3:40:37 pm to file 🛛 🖓 Assign to	category 🛛 🗃 Revision hist	ory 🙀 Exclude from Adaptive Anomaly Control	
	NOTIFICATIONS KASPERSKY ANNOUNCEMENTS	Event occurred Device	Event	Description		
њ. Д	DEVICES >	04/19/2021 315/40.cm TOM-LAPT	OP Device access blockage message to administrator	Helio! Please allow access to ope blocked according to the of Device parameters: Device type: Removable di Device rume: Generic Flas Modet: VEN_GENERICEP Device ID: USBSTORIDISKI	ations with the device Generic Flash Disk USB Device that has been wrice access rule. I mail USB Device DD, FJASH, DSK VDL GLABRIKCHERDOD, FJASH_DISKREV_8 07:8371988060	
KL 002.11.6: Kasper	sky Endpoint Sec urity & Managemen	t		Operation details: Computer: TOM-LAPTOP User: ABC\Tom Blocked operation type: Re Start date and time: 19-Apr	ad -21151540	kaspersky

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 ММС-консоли.

 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 .**акеу**-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 ММС-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 .**акеу**-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

New ev	nt selection		1. Устройство полключено
Genera	Application name	Kasnersky Endonint Serurity	
Events	Varian	inspecing emporie accurry	
Device:	Task name		 Подключение устройства заблокировано
Access	shts Severity level	Critical	4. Операция с устройством разрешен
	 Do not include general e Include selected general 	vents events	5. Активирован временный доступ к
	Severity level	Event name	устройству
	Critical	AMSI request was blocked	6. Операция с устройством запрещен
	Critical	Network attack detected	По умолизнию выборки событий пля
	Critical	Anglication startup prohibited	Контроля устройств нет, нужно создава
	Critical	Prohibited process was started before Kaspersky Endpoint Security startup	вручную
	Critical	Access denied (local bases)	
	Critical	Access denied (KSN)	



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.

Настройт	еб-контроль
⊙ Kaspersky Endpoint Security for Windows (116.0)	В политике Kaspersky Endpoint Security
High protection level GENERAL EVENT CONFIGURATION APPLICATION SETTINGS REVISION HISTORY POLICY PROFILE	Порядок правил имеет значение – срабатывает первое применимое
Advanced Threat Protection Esential Threat Protection Security Control Detection and Response Data Encryption Local Task General settings Advanced Threat Protection Data Encryption Local Task General settings Advanced Tables Data Security Advanced Advance	rol EMBLED wert allow you to control access to welt-insources depending on their content and location. ettings C Delete A Move Lip V Move down II: Import II: Export
авило по умолчанию может: — Разрешать все и всегда (Черный список) — Запрещать все, кроме (Белый список) умолчанию ничего не блокируется, т.к. правило	e nume State Actions al networks C Active Bock ~ Crept the rules list

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.

Состав правила Веб-контроля						
Rule						
Rule name Social networks		Types of data Addresses Addresses Apply to all addresses Apply to individual addresses and/or groups	Список адресов			
Status Ctatyc правила ● Active Active Active Действие		+ Add / Edit × Delete	No data			
Block Warn Ref type By content categories By content categories By types of data	<u>n</u>	Users Apply to all users Apply to individual users and / or groups Apply to individual users Apply to individua	Пользователи			
Content categories Types of data Addresses		User or group	No data			
Apply to all addresses Apply to individual addresses and/or groups			ание			

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 вебстраниц (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.х) 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

Web Control	(2) a x	
Web Control	🔒 Enforce 💽	Точно так же как общие правила — и поставить выше общего правила
Web Control ENABLED The component allows you to control access to web resources depending on their content and location.		выше общего правила
Web Control Settings	🛆 Enforce 💽	Тут порядок имеет значение
Rule List		
+ Add X Delete A Nove up V Nove down III Import III Export		
Rule name State Actions		
Linkedin C Active Allow V		
Social networks O Active Block -		
Default rule		
Allow all except the rules list Denv eventhing except the rules list		
Advanced settings	🗄 Linforce 🌑	
Information to the United Section of the Section of		
Termilates	A Selecte	

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 попробовать о	ткрыть запрещенный сайт:
🐼 Kaperly Endpoint Security for x + - 🗆 X	
← → C & facebook.com ☆ ⊕ :	Можно запросить доступ — запрос уйдет в виде события
The requested with page sproof the remainded	
Address: https://www.facebook.com/. The web page has been blocked by the Social networks rule.	
Reason: the web resource belongs to the Social networks content category(-les) and the Undetermined data type category(-les). This web resource is prohibited at the company, if you consider the blocking to the middake or if you need to acress the websets and	
contact the administrator of the local corporate network (Beoues)	
kaspersky	
2.11.6: Kaspersky Endpoint Security & Management	kaspers

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**.

Измените текст уведомлений				
Default rule Allow all except the rules list. Deny very thing except the rules list.	Шаблоны уведомлений доступны в политике Kaspersky Endpoint Security в настройках Веб-Контроля.			
Advanced settings				
Quarging the wetting a populate if the checkbox "spect scops" file web traffic to initiat with web pages" is checked in the Contrast Setting / Network Setting's vectors.				
warning wessage about blocking wessage to administrator Template of the message that is displayed if a not recommended web page or website is blocked. Image: Complete compl				
+ Add variable + Add link × Reset				
The requested web page cannot be provided. Address: %CANONIC_REQUEST_URL%.				
The web page has been blocked by the %RULE% rule.				
Reason: the web resource belongs to the %CONTENT_CATEGORY_LIST% content category(-ies) and the %TYPE_CATEGORY_LIST% data type category(-ies)				
This was accounted and his his of the annexes. How and do the blacking to be mittless as if you need to				



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

≡ m 4	MONITORING &	REPORTING / EVENT	SELECTIO	NS	Defer		<i></i>
	Selection All selection	ons 🗸			В общии список Запросы пользо	сооытии, в в вателей	ыоорку
KASPERSKY	+ Add / Properties	s D Reconfigure sorting and s	tart 🗙 Delet	2			
SECORITICENTER	Selection name		Sele	ction type			
⊟ KSC ≯ >	User requests		Pred	efined selection			
	Becent events		Pred	efined selection			
	Critical events	\downarrow	Pred	efined selection			
REPORTS	Eunctional failure	Result of User requests or	n 04/20/2021 :	:19:13 pm			
EVENT SELECTIONS	U Warnings						
NOTIFICATIONS	Info.events	C Refresh list × Delete	Export to	file 🛛 🖓 Assign to i	ategory 🛛 🖓 Revision history 🖓 Exclude from Adaptive Anomaly Contro	a Q	
KASPERSKY ANNOUNCEMENTS	Audit.events	Event occurred	Device	Event	Description	Administratio >>	
	Device with Netw	04/20/2021 1:18 36 pm	TOM-LAPTOR	Web page access blockage	Hellof	Managed devices	
▲ USERS & ROLES >				message to administrator	The web page https://www.facebook.com/ has been blocked by the Social networks rule because the web resource belongs to the Social networks content category(-ies) and the Undetermined data type category(-ies).		
					The requested web page has been blocked by mistake. Please grant me		
					Renards		

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

		События Веб-к	онтроля
New event selection			
General	Application name	Kaspersky Endpoint Security	 Доступ запрещен (локальные базы) Доступ запрещен (KSN)
Events Devices	Version		 Предупреждение о нежелательном содержимом (локальные базы)
Time Access rights	Task name Severity level	Warning v	 Предупреждение о нежелательном сопержимом (KSN)
Access rights	 Do not include general Include selected general 	events al events	Есть еще, но по умолчанию не
	Severity level	Event name	пересылается:
	Warning	Processing of some OS functions is disabled.	 Осуществлен доступк нежелательному
	Warning	Task settings applied successfully	содержимому после предупреждения
	Varning	Warning about undesirable content (local bases)	
	Varning	Warning about undesirable content (KSN)	
	Varning	Undesirable content was accessed after a warning	К Веб-контролю формально не
	Warning	Temporary access to the device activated	Относится (потому что это компонент
	Warning	Operation cancelled by the user	Sampinal, no ace we.
	Warning	User has opted out of the encryption policy	 Сооощение администратору о запрете поступа к веб-странице.
	Warning	Object disinfected	доступак вео странице
	Warning	Rollback completed	

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

			6								
	(Отче	т Веб	б-ко	нтро	оля	R				
≡ m 4	MONITORING & REPORTIN	IG / REPORTS		Report on V	/eb Control						
(PT)	+ Add > Open report template pro	perties D New report of	lelivery task 🛛 🕞 Export rep	4.50	G 244-1						
KASPERSKY	Name	Туре	Scope	/ Edit	Kerresh (> Export					
SECURITY CENTER	Report on most heavily infecte	Report on most hea >	> Threat statistics	Summar	y Details						
-	Report on threats	Report on threats	Threat statistics								
⊎ KSC ≯ →	Report on users of infected devices	Report on users of i >	> Threat statistics	Report o	n Web Control						
▲ MONITORING & REPORTING ↓	Other			Tuesday, Ap	ril 20. 2021 2:31:20	5 PM		note detected by Mi	ah Control	This secont is concepted for	c all around
DASHBOARD	Device Control	Report on Device C >	> Other	14	novides intornatio	14	access atten	ipis detected by w	eo control	This report is generated to	Social networks: 14
REPORTS	Report on Adaptive Anomaly C >>	Report on Adaptive >	> Other	13 - 12 - 11 -							Social networks: 2
EVENT SELECTIONS	Report on Web Control	Report on Web Control	Other	→ 10 9 8						2	
NOTIFICATIONS	Report on attacked controllers	Report on attacked >	> Other	7						Manp	
KASPERSKY ANNOUNCEMENTS	Report on blockage of access t >>	Report on blockage >	> Other	4					2		
E DEVICES >	Report on check of programma>>	Report on check of >	> Other	2-1-0							
▲ USERS & ROLES >	Report on device users	Report on device users	Other								
OPERATIONS >	Beport on effective user permissions	Report on effective >	> Other	Search							
				Result	Rule	Attempts	Accounts	Web addresses	Devices	Administration groups	First attempt
Показывает как част	го какие правила ст	абатывают	r	Blocked	Social networks	14	1	2	1	1	Tuesday, April 20,
FICKGODEGCT KGK 4001	io kakio npabina op	Jaca Bibaio		Warning	Social networks	2	1	2	1	1	Tuesday, April 20.
										ka	enorely
002.11.6: Kaspersky Endpoint Security & Man	agement									Ka	alie lade

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 какихлибо 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

Kaspersky Endpoint Security for W	indows (11.6.0)	
High protection level.		В политике Kaspersky Endpoint Security
GENERAL EVENT CONFIGURAT Advanced Threat Protection Essential Threat Protection Security Controls	ION APPLICATION SETTINGS REVISION HISTORY POULY PROFIL Andication Control This component monitors users' alternative to start applications and controls th Design Control	LES По умолчанию Контроль аномалий включен и работает в Интеллектуальном режиме евене of egiculos is use place
Detection and Response Data Encryption Local Tasks General settings	The component allows you to control the connection of removable drives. Web Accental This component allows you to control access to web resources depending Accentation access to entrol access to web resources depending Accentation access to entrol access to entrol behavior of applications	Adaptive Anomaly Control Control EH48LED CO To compound dences and blocks abnormal lehaner of applications. Reports Benord on Adaptive Anomaly Control Left state Benord on Dispersive Adaptive Anomaly Control Left state
		Rules Educations in Adly automated and does not require manual last up of the agglocations. Between, it is possible to set up the nates that comply with the company's securit project

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.

Rules Rules It is required to approve updates for the Adaptive Anomaly Control fuel list.	Из настроек у правил есть состояние Вкл/Выкл, режим работы Интеллектуальный/Блокировать/Уведомлять и исключения
✓ Edit ✓ Approve updates # Import # Export	Rules
Z Rule Status	is Ac
Activity of office applications	Rules
Use of Windows Management Instrumentation (WMI)	// Edit // Approve updates 毎 Import 毎 Export
Activity of script engines and frameworks	Rule Status Action
Abnormal program activity	□ ∨ Activity of office applications
	Start of Microsoft Register Server from office application
	Start of Microsoft HTML Application Host from office application On Block
Адаптивный контроль аномалий имеет	Start of Microsoft Console Based Script Host from office application
предустановленный насор правил, которые могут обновляться вместе с базами	Start of Microsoft Windows Based Script Host from office application O n Smart

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.

≡ m ¢	OPERATIONS / REPOS	ITORIES / TRIGO	ERING O	F RULES IN SMART TRAINING STATE		По умолианию Алаптивный
KASPERSKY	✓ Confirm + Exclude	✓ Properties ≢	E Filter	Non	Dat	контроль аномалий работает в Интеллектуальном режиме
SECURITY CENTER	Managed devices	ALEX-DESKTOP A	BC\Alex	Third-party application has a name similar to a system file name	ne 1	В этом режиме ничего не
LICENSING > THREP-PARTY APPLICATIONS > REPORTORES > EXORUP OURPAINTINE ACTIVE THEATS INSTALLATION PACKAGES HARDWARE				J.O.		обо всех срабатываниях попадает в КSC в контейнер Срабатывание правил в интеллектуальном режиме

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.

режиме					
		Интеллектуальный режим предполагает участие администратор			
✓ Confirm + Exclude		Алминистратору желательно обработать событие:			
Name Processed	Third-party application has a name similar to a system file name	— Подтвердить			
Status		— Исключить			
Virtual Administration Server					
Administration group	Managed devices				
Device name	ALEX-DESKTOP				
Detections count	1				
User name	ABC\Alex				
Source process path	c:\users\alex.abc.000\downloads\aac\untrusted_application_with_system _like_name.bat				
Source process hash	9D578AB540D5CB99AA134D80B8373032CDEDE144E65F1341DCB6B23A 2982E926				
Source object path					
Source object hash					
Target process path	C:\Users\alex.ABC.000\Downloads\AAC\winl0gon.exe				
Target process hash	CFD859A568382E359833538F35318972F735D97CE68E33E2669ECDD631 4960AB				
Target object path	object://cmdline:"C:\Users\alex.ABC.000\Downloads\AAC\\winl0gon.exe"				
Target object hash					

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.



пастроите исключения					
Extusion User or group ASC-kics Description Source process Culterstates ab CO01downloads1kac/untrusted_application_with_system_site_name bat Source process hash (90578A654005CB9AA13AD8088373032CDEDE1446591341DC86823A29825906 Source object hash Source object hash (C10sensides ABC 0001Downloads1AAC/winit0gon exe Target process hash (C10sensides ABC 0001Downloads1AAC/winit0gon exe) Target process hash (C10sensides ABC 0001Downloads1AAC/winit0gon exe) Target process hash (C10sensides SB25398353589729725097CE88E33526698CDD6334690A8 Target object (Dept36406483822596835389729725097CE88E33526698CDD6334690A8 Target object (Dept36406483822596835389729725097CE88E33526698CDD6334690A8 Target object (Dept3640648382539835389729725097CE88E33526698CDD6334690A8 Target object (Dept3640648382539835389729725097CE88E33526698CDD6334690A8 Target object (Dept3640648382539835389729725097CE88E33526698CDD6334690A8 Target object (Dept3640648 (Dept364064 (Dept3640648 (Dept364064 (Dept3640648 (Dept364064 (Dept3640648 (Dept364064 (Dept3640648 (Dept364064 (Dept3640648 (Dept364064 (Dept364064 (Dept364064 (Dept3640648 (Dept364064 (Dept3640648 (Dept364064 (Dept364064 (Dept3640648 (Dept364064 (Dept364064 (Dept3640648 (Dept364064 (D	Список исключений глобальный и распространяется на все компьютеры Основные параметры исключений: – Пользователь – Исходный процесс – Хеш исходного процесса – Целевой процесс – Хеш целевого процесса				

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

Основные параметры исключений:

- Польователь
- 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.

Как еще можно добави	ть исключения
Result of User requests on D4/21/2021 12:56:49 pm	Add to Adaptive Anomaly Control exclusions
C Refresh list X Delete @ Export to file @ Assign to category @ Revision history @ Exclude from Adaptive Anomaly Control	+ New policy
Event occurred Device Event Description	Policy / Profile
Place allow reto operform the action that was blocked in accordance with an Adaptive Access parameters for a parameters for a parameters in strons and closentabel skat system. Lifep. unorsystem_5064er_drog bat for any approximation of the strong strong strong strong strong strong strong strong strong for any approximation of the strong strong strong strong strong strong strong strong transfer strong strong strong strong strong strong strong strong strong strong strong strong strong transfer strong strong categorization strong strong categorization strong strong strong strong strong strong strong strong strong strong strong strong strong st	Исключения в Контроль аномалий можно добавлять прямо из событий

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.

(События	Адаптивног	о контроля аномалий
 Adaptive anomaly control 	ontrol event selection		
General	Application name	Kaspersky Endpoint Security	
Events	Version		типа событий:
Devices	Veracer		
Time	Task name		 Деиствие процесса пропущено
Access rights	Severity level	Critical	 Действие процесса заблокировано
 Do not include general events Include selected general events 		ts ints	Можно создать отдельную выборку на эти два
	Severity level	Event name	соовния
	Critical	Previously opened dangerous link detected	
	Critical	Process action blocked	
	Critical	Keyboard not authorized	
2284 K	2.014		kaspers

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.

v1.0.1